https://doi.org/10.52131/irasd-jom.2025.v7i1.2845

*i*RASD Journal of Management

Volume 7, Number 1, 2025, Pages 10 - 26

Journal Homepage:
https://journals.internationalrasd.org/index.php/jom

Smart Tech, Scared Users: A Behavioral Analysis of AI-Powered Solutions for Cyberthreat-Induced Customer Complaints in Low-Income Countries

Victor Oluwatosin Ologun[1], Ayomide Olugbade[2], Patience Farida Azuikpe[3], Michael Aderemi Adegbite[4], Olawale Abdulmumin Lawal[5], Stephen Alaba John[6]

[1] MSc. Student, Department of Information System, Le Moyne College Syracuse, New York, USA.
Email: ologunv@gmail.com
[2] MSc Student, Computer Science and Engineering, University of Fairfax, Virginia, USA.
Email: ayomideolugbade34@gmail.com
[3] PhD Student, Department of Business and Management, University of Manchester, England.
Email: patienceazuikpe@gmail.com
[4] MSc Student, Raymond A Mason Business School, College of William and Mary, USA.
Email: maadegbite@wm.edu
[5] MSc. Student, School of Advance Digital Technology, Southern Alberta Institute of Technology, Canada.
Email: ola.lawals19@gmail.com
[6] PhD. Student, Department of Accounting and Finance, Kwara State University, Malete, Nigeria.
Email: stephenalaba.j@gmail.com

ARTICLE INFO

Article History:

Received:	January	18, 2025
Revised:	March	20, 2025
Accepted:	March	22, 2025
Available Online:	March	23, 2025

Keywords:
Digital Tax Interpretation
Tax Payment System
Coretax System Implementation
Taxpayer Compliance

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

In the face of rising cyber incidents in digital banking, artificial intelligence (AI) has emerged as a critical tool for automating threat detection, enhancing response speed, and improving complaint resolution. However, the success of such technological interventions depends significantly on user behavior, perceptions, and willingness to use these systems. This study examines the behavioral determinants influencing the implementation of AI-powered solutions for cyberthreat-induced customer complaints for banks in low-income countries. Guided by the protection motivation theory (PMT), the study adopted a quantitative, cross-sectional survey design involving 350 respondents, comprising 315 bank customers and 35 frontline bank staff, across seven Nigerian banks with international authorization. PMT constructs were used to develop the Likert-based questionnaire. Data were analyzed using Ordinal Logistic Regression (OLR) model. The findings reveal that perceived severity ($\beta = 0.455$, $p < 0.05$), perceived vulnerability ($\beta = 0.387$, $p < 0.05$), response efficacy ($\beta = 0.658$, $p < 0.05$), and self-efficacy ($\beta = 0.587$, $p < 0.05$) have positive and significant effects on AI-powered solutions for cyberthreat-induced customer complaints. However, response cost ($\beta = -0.405$, $p < 0.05$) has negative and significant effects on AI-powered solutions for cyberthreat-induced customer complaints. This study contributes to the growing field of AI solutions for cyber related customer complaints in banks by offering a behaviorally grounded framework for understanding how threat appraisals and coping appraisals drive support for AI-powered cyber complaint solutions. The study recommends that banks in low-income countries should actively communicate the effectiveness and success rates of AI-powered tools such as chatbots, anomaly detection systems, and automated complaint resolution platforms to demonstrate how these systems resolve issues faster, more securely, and more accurately so as to build trust among users.

OPEN ACCESS

© 2025 The Authors, Published by iRASD. This is an Open Access article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: stephenalaba.j@gmail.com

Citation: Mahadianto, M. Y., Maulady, P., & Yani, S. (2025). Interpretation of Tax Payment Mechanism in Coretax System on Compliance (Case of KPP Pratama Cirebon). IRASD Journal of Management, 7(1), 01–09. https://doi.org/10.52131/irasd-jom.2025.v7i1.2845

1. Introduction

Understanding customer complaints is very important for businesses, regulators, and banks in today's digital age. Handling complaints well can make customers happier, reveal bigger problems in the system, help follow rules, and support better decision-making (Gonaygunta, 2023; Pio et al., 2024). Financial institutions are increasingly vulnerable to cyber threats due to the rapid digitization of banking services. Cyberattacks such as identity theft, data breaches, and account takeovers are becoming prevalent in both developed and developing economies (Eskandarany, 2024). In several countries classified as low-income economies, banks find themselves in a twofold quandary of both a lack of technological infrastructure as well as a heavy exposure to cybersecurity risks, conditions amenable to the instigation of unresolved or poorly handled customer complaints. They destroy the feeling of trust in the customer and highlight the vulnerability of the system regarding the complaints resolution systems (Gonaygunta, 2023; Wiafe et al., 2020).

Artificial Intelligence (AI) is becoming a strategically valued tool in the efforts of decision-makers to enhance cybersecurity preparedness at the same time as they also expedite the complaint-resolution process (Sharma et al., 2024; Zhang et al., 2024). With the help of AI-enabled applications including intelligent chatbots, anomaly detection machine-learning, automated complaint categorization, and predictive analytics, there is real-time capability to detect potential threats and resolve customer complaints. These technologies are capable of providing greater efficiency in operational activities, reducing the impact of human error, diminishing response time, and improving customer satisfaction when used legitimately (Al-Gasaymeh et al., 2023; AlAfnan, 2024). However, the adoption of these technologies within the low-income setting is fairly slow, limited by socio-technological, psychological and organization barriers (Roumeliotis et al., 2025). These limitations require resolution to ensure the sustainability of the banking industry and the establishment of efficient customer trust building

A critical, often underexplored dimension of this problem lies in understanding how and why customers or bank staff adopt (or resist) AI-based cyberthreat complaint systems (Abubakar et al., 2025). Traditional technology adoption models, while helpful, may not adequately capture the behavioral motivations behind users' protective actions in the face of cyber risk (Roy et al., 2024; Vairetti et al., 2024). This is where protection motivation theory (PMT), developed by Rogers (1975), becomes relevant. PMT says people are more likely to protect themselves when they see a credible threat and believe that the recommended coping response is effective and feasible.

As digital banking services expand across low-income countries, banks are facing more cybersecurity threats like identity theft, data breaches and phishing. These cyber incidents often trigger customer complaints that are either unresolved or ineffectively managed, thereby eroding trust, damaging reputations, and weakening consumer protection (Eskandarany, 2024; Gonaygunta, 2023). While Artificial Intelligence (AI) offers promising tools, such as intelligent chatbots, anomaly detection systems, and automated complaint handling platforms, for mitigating cyberthreats and resolving related customer grievances, the adoption of such AI-powered solutions in low-income countries remains limited (Almustafa et al., 2023; Hsu & Lin, 2023).

This adoption gap is not solely due to infrastructural or financial constraints but is also shaped by behavioural and psychological factors (Ashrafuzzaman et al., 2025). Despite the availability of AI tools, many customers and even bank staff may lack trust, confidence, or motivation to adopt them, especially in environments characterized by low digital literacy, poor user experience, and inadequate cybersecurity awareness (Vethachalam, 2025). Traditional technology adoption models, such as the Technology Acceptance Model (TAM) or Unified Theory of Acceptance and Use of Technology (UTAUT), fall short in explaining user behaviour when perceived threats and protective motivations are central to decision-making.

To address this gap, there is a pressing need to examine the behavioural factors influencing the adoption of AI-powered systems specifically designed to handle cyberthreat-induced complaints. PMT, which classifies behavioural motivation into two major cognitive processes: threat appraisal and coping appraisal, emphasizes how perceived severity, perceived vulnerability, perceived efficacy of the AI-powered solution system, self-efficacy, and perceived cost influence protective behaviour, offers a robust theoretical framework for this study.

However, to date, empirical studies applying PMT to AI implementation in cyber related customer complaint management in low-income countries are scarce and next to nonexistent. This limits practical guidance for banks aiming to deploy AI responsibly and effectively. Without a clear grasp of the behavioural enablers and barriers, efforts to digitize complaint systems may falter, leaving customers exposed to further harm and institutions vulnerable to reputational and financial risks. Therefore, this study seeks to examine the behavioural factors, as explained by PMT, that influence the adoption of AI-powered solutions for cyberthreat-induced customer complaints in banks operating in low-income countries.

In past years, traditional models like the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT) have long guided research on digital innovation adoption, emphasizing factors such as perceived usefulness, ease of use, and social influence. While these models are effective in explaining user behaviour in neutral or opportunity-driven contexts, they offer limited explanatory power in threat-based or risk-laden environments, particularly those involving cybersecurity vulnerabilities. In banks across low-income countries, where digital literacy is often low and cyberattacks are rising, users' decisions to adopt technologies are less about utility or performance expectations and more about psychological assessments of risk, vulnerability, and the effectiveness of protective responses, factors not well addressed by TAM or UTAUT.

This gap is especially critical in the adoption of AI-powered solution for cyberthreat-induced customer complaints. In this area of research, the choice in favor of AI-driven solutions can be explained by four interdependent drivers, including fear of attack, trust in the effectiveness of AI, individual ability, and the perceived obstacle to protection, which are collectively known as the core constructs of protection motivation theory (PMT). In spite of the significant insights that PMT has already brought to cybersecurity behaviour studies, the domain of its potential application to AI adoption, especially that in cyberthreat-related customer complaints in low-income countries, is rather unexplored. This paper hence fills that theoretical gap, using PMT to test how the threat appraisal (severity and vulnerability) and coping appraisal (response efficacy, self-efficacy and response cost) affect the application in such situations of AI-powered tools, and, in so doing, present a more comprehensive picture of protective technologic use in high-risk digital settings.

2. Literature Review

2.1. AI-Powered Solutions for Cyberthreat-Induced Customer Complaints

Artificial intelligence systems of addressing customer complaints spawned by cases of cybersecurity incursions in the banking sector define the business methodical implementation of artificial intellect potentials in identifying, regulating, and solves complaints that are associated with cybersecurity breaches that are faced by a bank. Such systems should include smart chatbots, NLP-enhanced complaint-identification systems, machine learning cancel-detection engines, and complete automation of complaint-classification or complaint-resolution processes. These tools in low-income national contexts aim to reduce response time, increase analytical accuracy and raise transparency when handling grievances caused by a cyber event- phishing attacks, unauthorized financial operations, data breaches, or identity theft. In that regard, AI acts as both a means of operational efficiency and a proactive measure in countering the digital threats against which it acts directly as a disruptor of customers trust and their overall banking experience (Alaba et al., 2025).

2.2. Threat Appraisal

The cognitive evaluation of risk that accompanies a potential cyber threat has been termed threat appraisal, and it has been suggested that this process leads to both the alteration of motivation to participate in protective behaviours and its reduction. Such process occurs in the Protection Motivation Theory (PMT) in the framework of two main constructs perceived severity and vulnerability. The combination of these dimensions dictates the level of seriousness in which a threat is taken and the perceived probability of having negative outcomes.

Perceived severity refers to the subjective assessment of the high level of possible losses caused by a cyber threat the person involved in, e.g. identity theft, unauthorized access to financial data, disappearance of funds, etc. The bank-related contexts in which the implications of expected consequences are seen as the worst, the more likely users will embrace the protective mechanisms as the use of AI-powered complaint resolution systems. On the other hand, perceived vulnerability covers the degree to which a person rates personal susceptibility towards being attacked by a cyber-attack or other financial damage, thus the subjective likelihood of these events occurring. The more there is a subjective feeling of vulnerability, the more motivated the user becomes when it comes to employing AI-based tools that aim to help avoid or act against these risks with a certain level of efficiency.

2.3. Coping Appraisal

Coping appraisal is the second mental aspect of the Protection Motivation Theory model and deals with what the person thinks he or she can do to reduce a perceived threat. This analysis involves perceptions of how well an action will work, how certain the individual will be in doing the successful action, and how expensive implementing the coping strategy will be. In the current study, coping appraisal is operationalized using three (three) distinct constructs, response efficacy, self-efficacy, and response cost.

Response efficacy refers to the idea that AI-driven systems will be an effective tool in managing or addressing complaints which emerge because of cyber incidents. As long as users believe that such tools can identify, interpret and solve cyber problems, the more the individuals will be likely to embrace them as a protective behaviour. Self-efficacy describes the confidence of the person in his or her ability to use AI-based systems, such as the abilities to interface with digital systems, navigate a complaints interface, and interpret systems feedback. High self-efficacy is associated with an increase in adoption, especially in poor circumstances where digital literacy can change extensively. Response cost denotes the barriers or efforts perceived to use and adopt AI-powered systems as well as sacrifices. These barriers may involve the cost of money, the time it takes, the technological difficulty, fear of misuse, fear of losing control of the data. Even in the case when the threat is recognized and the system being determined as effective, motivation to implement the technology can be reduced by a greater perceived response cost.

3. Theoretical Framework

The current study is based on the Protection motivation theory (PMT) initially described by Rogers (1975). PMT provides a psychological model of explaining how people get motivated to protect themselves based on perceived dangers. Although it was originally meant to explain health-related behaviour, the model has been applied by researchers and practitioners in a variety of different fields, most notably, cybersecurity, risk communication, and digital safety, to study the way in which users react to online threats like fraud, phishing, and account takeover.

In the context of PMT, the main idea is that two main cognitive processes threat appraisal and coping appraisal form the motivation to perform a protective behaviour. Threat appraisal is the process of assessing how dangerous something is but also assessing how vulnerable one is to it. Coping appraisal is the process of evaluating how effective the various courses of action options- or coping strategies that may prove to reduce the threat are. In the current study, these processes were operationalized by self-report measures

indicating the perceived severity of the threat (level of threat), and the perceived vulnerability, and the perceived efficacy of veritable coping strategies available. In a cybersecurity context, this means how serious a customer believes a cyberattack is (e.g., account takeover, fraudulent transactions) and how likely they think they are to be affected by it. If a customer believes that a threat is both severe and personally relevant, they are more likely to take action—such as reporting the issue or being cautious online.

Coping appraisal, on the other hand, evaluates the effectiveness of the protective response (response efficacy), the individual's ability to perform the behaviour (self-efficacy), and the perceived costs of the action. In the case of banks using AI to manage cyberthreat-induced complaints, coping appraisal explains whether customers believe reporting a cyber incident using an AI-powered system (e.g., chatbots, automated complaint handling platforms, anomaly detection systems, machine learning-based) will actually help them, whether they feel capable of using that system, and whether there are any barriers (e.g., complex steps, lack of trust, fear of being ignored).

The relevance of PMT in this study lies in its ability to explain why customers in low-income countries may or may not report cyberthreat-induced complaints, especially through AI-based channels. If a customer perceives that using AI tools is ineffective or difficult (low response efficacy or self-efficacy), or if they do not believe the threat is serious, they may not act. Conversely, effective awareness campaigns and well-designed, user-friendly AI tools can strengthen coping appraisal and encourage protective behaviour.

3.1. Related Studies

Chen et al. (2021) studied how AI chatbots affect customer experience and satisfaction in online shopping. They used a survey of 425 people and analyzed the data with SPSS and SmartPLS. The results showed that chatbot usability improved practical parts of the customer experience, while chatbot responsiveness improved emotional aspects. A better online experience led to higher customer satisfaction, and a customer's personality affected how chatbot usability influenced their experience.

The study by Tulcanaza-Prieto et al. (2023) explored the impact of the public attitude towards the increased usage of AI among banks that operate in Ecuador. An online survey with 226 participants provided temporal information on five dimensions namely ease of use, personalization, trust, loyalty, and satisfaction. There are two types of AI experience that respondents described: the enjoyability of the service and its understanding of what they needed. All the individual dimension and their total scores had a strongly positive impact on both measures of the experiences as estimated by the regression analysis.

To determine the role of artificial intelligence (AI) in mediating customer loyalty and overall experience and whether, in particular, personalization mediates such an effect, Ifekanandu et al. (2023) utilized a questionnaire-based study. The study utilized 636 survey answers of an online survey and used IBM AMOS structural equation modeling (SEM) to analyze the data. The findings prove that AI alone makes personalization, loyalty, and experience a lot better on aggregate.

Tula et al. (2024) reviewed the existing literature and examples of practical application to explain how AI has become a focal point of customer-based corporate strategy, as it is frequently viewed as an emerging technology. According to their argument, AI has revamped their relationship between companies and consumers by simultaneously enhancing support, forecasting requests, and providing customized solutions. However, innovation presents problems that relate to privacy of data, ethical responsibility and inadequacy of talent. The authors hence conclude that AI should be used with diligence in organizational planning.

Juipa et al. (2024) developed a chatbot capable of settling complaints in the telecommunication sector that uses sentiment-analysis to do so. The empirical results demonstrate that use of GPT-3.5 in emotional interpretation increased customer satisfaction and performance of complaints resolution and an 86% customer satisfaction level was obtained with reference to the existing baseline in the industry and highlights the ability of AI chatbots in improving complaint handling.

Kumar et al. (2024) conducted a systematic study of the problems of customer complaints focusing on emotions, and the severity of the customer issues reported in the online retail over multilingual environment. Their deep-learning mechanism, the word and sentence embeddings, learned trained is stronger than rival approaches. The study validated the hypothesis that perception of respondents to emotion and seriousness goes a long way toward solving complaints.

Vairetti et al. (2024) present a convenience-based strategy, which is deep learning (DL)-assisted and multi-criteria decision-making (MCDM) approach to prioritizing customer complaints. The model can address various aspects of dissatisfaction and satisfaction to improve satisfaction and prevent customer turnover. The authors take advantage of modern pretrained language models and reveal that the BETO architecture, which is modified based on BERT, achieves 92.1 % accuracy in the classification task.

Seok et al. (2024), propose a deep learning-based system that uses explainable AI (XAI) for real-time monitoring customer complaints. Based on the BERT-based models, the methodology processes online reviews to derive sentiment and semantic information to identify new patterns. This dynamic tracking dashboard is an addition that would allow constant monitoring of the complaints on companies with seasonal traits.

Correia et al. (2024) introduce the extension of the generative AI offering to the consumer complaint management and incorporate the integration capabilities into classification, summarization, and generation of responses. The resulting system provides 88 % classification accuracy and proves that AI can be applied to modern customer-service tasks.

Changalreddy and Vashishtha (2024) explore the application of predictive analytics in detecting the customers who are likely to churn. The authors use transactional information, behavioral tendencies, demographics and service experiences to create ensemble models predominantly logistic regression, decision trees and random forests that, using this information, determine the likelihood of churn with high precision. These models assist in guiding the banks to high-risk clients and thus help in early intervention and resource alignment.

Eskandarany (2024) evaluates the importance of bank boards in enabling the implementation of AI and machine-learning programs to prevent cyber threats. The results suggest that AI and ML reinforce regulatory compliance, identify risk, hinder fraud and simplify operational work; however, there are still several obstacles, including poor technological infrastructures, unclear strategic goals, and bias and data privacy issues. The board plays a critical role in the formulation of strategy, obtaining funds and in partnership with external vendors. The analysis is based on a stable well-regulated environment, therefore, jurisdictions with weaker institutional systems namely, Nigeria, might face greater challenges not covered under this study.

Jada and Mayayise (2024) conducted a systematic review of available sources in order to determine the actual level of influence of artificial-intelligence (AI) solutions on modern cybersecurity and assess their comparative effectiveness against conventional approaches. The authors used the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram and obtained 73 articles published in 2018-2023 using major databases, 24 of which were discarded after the screening of abstracts. Full-text examination of the 49 remaining studies followed, whereby 11 studies were eliminated. The corpus of study, with a total of 38 papers, was used for analysis. These findings showed that AI does not only automate standard operational tasks but also complement threat intelligence generation and make defenses stronger. However, AI also faces problems like attacks against it and the need for good-quality data, which can affect how well it works. Overall, the study shows AI has a positive impact on making cybersecurity more effective and stronger.

Metha (2025) studied how AI can spot possible fraud by creating a risk score based on account activity. If the score goes above 80 out of 100, security actions happen automatically. The score looks at four main signs of fraud: logging in from new devices,

changing contact info, adding new Zelle contacts or payees, and making transactions over $1,000 within 48 hours. The model uses machine learning to analyze past behaviour, patterns, and current data to calculate the score. Accounts with scores over 80 are temporarily blocked, and extra checks are done to keep them safe while trying to avoid causing problems for customers. This study doesn't fully apply to Nigeria because of uneven data handling and weak cybersecurity.

Ashrafuzzaman et al. (2025) carefully reviewed research on how AI helps personalize digital banking. They focused on how smart algorithms and customer behaviour analysis improve engagement, satisfaction, loyalty, and trust. Using the PRISMA 2020 method, they looked at 111 articles published from 2014 to 2024 to find main ideas, methods, innovations, and gaps. The study found that AI personalization not only makes banking operations better and improves service but also increases customers' long-term value and emotional loyalty.

Abubakar et al. (2025) examined the intersection of artificial intelligence (AI) and customer experience (CX), using ANOVA, which confirmed the overall model's validity. Findings revealed that AI powered customer service, relationship commitment, perceived convenience, data security, and customer satisfaction significantly impacted the dependent variable, customer loyalty. Data Security is statistically significant (with $p < 0.05$) which indicates that there is a substantial contribution from data security to customer loyalty.

MUHAMMAD and STUKALINA (2025) explored the application of AI chatbots to be used in e-commerce to improve customer satisfaction levels, using systematic literature review involve the peer-reviewed literature published between 2021 and 2024 from Scopus and PubMed. After applying some exclusion criteria. The PRISMA approach was utilized to synthesize the findings. Cross-study compatibility, validity, and reliability of sources were validated and assessed to derive more accurate data-analysis results. The results of the research support chatbots as stewards of business and customer service operations to achieve global sustainability and citizenship objectives, including inclusive interactions for all users.

Chien et al. (2025) examined the impact of AI-powered service quality on customer satisfaction on B2C e-commerce platforms in Vietnam. Additionally, it explores the mediating role of perceived value. The study surveyed 398 individuals who had experienced AI-powered services while shopping on major e-commerce platforms in Vietnam, including Shopee, Tiki, Lazada, and TikTok Shop. The findings provide new insights into the application of AI in e-commerce services, emphasizing the importance of AI adoption and customer experience optimization in enhancing customer satisfaction in e commerce.

Roumeliotis et al. (2025) tested 14 smart AI models, like DeepSeek, Gemini, Claude, and GPT-4, to see how well they sort consumer complaints from the Consumer Financial Protection Bureau into five financial groups. Reasoning models, which are trained to think and make decisions better than regular models, showed new abilities in classifying text. They checked how well each model worked by looking at accuracy and other scores and used heatmaps to find patterns. The paper focused on how different reasoning models perform when subjected to financial passages. The results of it highlighted the advantages and the weaknesses of both methods. It is especially interesting that, applied to customer complaints, these models allowed firms to solve problems independently which, in its turn, led to the improvement of the overall quality of the service.

4. Methodology

This study adopts a quantitative, cross-sectional survey design to examine the behavioural determinants of implementing AI-powered solutions for cyberthreat-induced customer complaints in banks. The protection motivation theory (PMT) provided theoretical foundation, and Ordinal Logistic Regression (OLR) model was used to test the relationships among the variables. The choice of a quantitative approach is appropriate given the need to measure latent psychological constructs and statistically assess the relationships between threat/coping appraisals and AI-powered solution implementation.

Primary data were collected using structured questionnaire based on PMT constructs and Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5). The questionnaire helps to generate data for behavioural constructs in the protection motivation theory such as perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost influencing AI-powered solutions for cyberthreat-induced customer complaints. The target population comprises bank customers and frontline bank staff, including customer service officers, IT helpdesk agents, in low-income countries who have access to digital banking services and frontline bank staff who handle cyber-related customer complaints or manage digital banking platforms (e.g., mobile banking apps, internet banking portals, USSD platforms). A stratified random sampling technique was used to select a total of 315 bank customers and 35 bank staff across seven (7) banks with International Authorization, which was chosen as the focal country based on its classification among low-income economies by the World Bank.

The study specifically required input from individuals who serve as end users of digital banking and operational intermediaries of AI-powered systems designed to resolve cyberthreat-induced complaints. To ensure feasibility and institutional readiness, the research focused on banks with sufficient capacity in terms of total assets, customer base, and market capitalization to support the deployment of AI-powered solution systems such as chatbots, automated complaint handling platforms, anomaly detection systems, machine learning-based.

The current study has ensured the collection of data seven (7) banks that have International Authorization; these are Access Bank, Fidelity Bank, Guaranty Trust Bank, First Bank of Nigeria Limited, United Bank of Africa, First City Monument Bank (FCMB) Plc, and Zenith bank. These considerations are significant, and they justify such a deliberate sampling strategy: institutional preparedness, competence in terms of technology, facing the threat of cyber-related challenges, and strategic significance to a general study. The case studies are representative samples of the largest and technologically advanced organizations within the banking sector in Africa within the low-income countries. These banks are also compelled to maintain high risk management, cybersecurity and customer-service technologies through their international licensing by the Central Bank of Nigeria (CBN). They have made significant investments in digital transformation and artificial intelligence, making them early adopters of tools such as chatbots, anomaly detection platforms, fraud detection systems, and automated complaint handling interfaces. For example, GTBank's chatbot "Habari" and Access Bank's "Tamara" are real-world examples of AI-enabled customer support systems.

Their established track record in implementing AI technologies ensures that study participants, both customers and staff, have direct experience with or meaningful exposure to the technologies under investigation. These banks serve as benchmarks for digital innovation and customer engagement in low-income African countries. Choosing international banks enhances the strategic and policy relevance of this study. As such, they represent ideal case environments for studying the adoption of AI-powered solutions in handling cyberthreat-induced customer complaints.

4.1. Method of Data Analysis

Following Alaba et al. (2025), Ordinal Logistic Regression (OLR) model was used to analyze the data. OLR works well when the outcome is an ordered category (such as levels of AI-powered solutions for cyberthreat-related customer complaints) and there are one or more factors influencing it (like perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost). The functional model is stated as:

$$\text{CICC} = f(\text{PSEV}, \text{PVUL}, \text{RESP}, \text{SELF}, \text{COST}) \quad (1)$$

The functional model is stated in econometric form as:

$$logit\big(P(Y=j)\big) = \alpha_j + \beta_1 \text{PSEV} + \beta_2 PVUL + \beta_3 RESP + \beta_4 SELF + \beta_5 COST \quad (2)$$

Where; $P(Y = j)$ is the cumulative probability of the response variable *Y* (AI-powered solutions for cyberthreat-induced customer complaints) being in category j or lower; α_j represents the cut-off points for the j-th category; $\beta_{1\text{-}5}$ are the coefficients of the explanatory variables; PSEV = perceived severity, PVUL = perceived vulnerability, RESP = response efficacy, SELF = self-efficacy, COST = response cost, respectively.

OLR was chosen because it is made to work with ordered outcomes, keeping the ranking of categories without assuming equal distances between them. The outcome in this study, AI-powered solutions for cyberthreat-related customer complaints, is measured on a 5-point scale where the order matters but the gaps between points might not be equal. The model looks at how different factors affect the chance of being in a higher category, which fits the goal of finding what influences the use of AI solutions for handling cyberthreat complaints.

5. Data Analysis and Discussion of Findings

Out of 350 surveys sent out, 311 were completed and returned. The questionnaire had two parts. Section B had questions using a 5-point Likert scale from Strongly Disagree (1) to Strongly Agree (5). Section A asked for personal information. The demographic data collected included respondents' gender, education level, familiarity with AI tools and digital banking, and how often and what types of cyber threats they have experienced.

Table 1
Distribution of Frontline Bank Staff by Functional Unit

Department / Unit	Number of Respondents	Proportion (%)
Customer Service Officers	15	42.9%
Management Staff	8	22.9%
Digital Banking Unit	9	25.7%
Risk Management Unit	3	8.6%
Total	35	100.0%

Source: Authors

A total of 35 frontline bank staff and IT helpdesk agents participated in the survey. These respondents were drawn from various units directly involved in handling customer complaints and managing digital banking operations. Specifically, 15 respondents (42.9%) were customer service officers, who engage daily with customers and handle complaints, including those related to cyber incidents. Eight respondents (22.9%) were senior management staff responsible for supervising complaint resolution procedures and coordinating cross-functional response strategies. Additionally, nine respondents (25.7%) were drawn from digital banking units, tasked with maintaining and managing platforms such as internet banking portals, mobile banking applications, and USSD services, while other three respondents (8.6%) were from the risk management units, providing insight into the organization's approach to cyberthreat mitigation and AI-based risk response mechanisms.

By gender distribution, the sample was predominantly male, with 25 respondents (71.43%) identifying as male, while 10 respondents (28.57%) identified as female. This reflects the gender composition often observed in technical and operational banking roles, particularly in customer service, digital banking, and risk management units within commercial banks in low- and middle-income settings. The years of professional experience among the frontline bank staff respondents varied across three categories. A total of 15 individuals (42.9%) reported having less than 10 years of professional experience, reflecting a relatively younger segment of the workforce likely to be more adaptable to technological innovations such as AI. Twelve respondents (34.3%) had between 10 and 20 years of experience, representing mid-level professionals with practical exposure to evolving digital banking trends. Additionally, eight respondents (22.9%) had more than 20 years of experience, contributing seasoned insights into long-term institutional practices, risk management, and customer service evolution within the banking sector.

Table 2
Distribution of Bank Customers by Customer Tenure

Bank	Account Tenure	Proportion (%)	Number of Customers
Access Bank	9	17.1%	54
Zenith Bank	8	15.2%	48
GTBank	8	15.2%	48
UBA	8	15.2%	48
First Bank	8	15.2%	48
Fidelity Bank	5	9.5%	30
FCMB	4	7.6%	24

Source: Authors

To ensure representativeness, the distribution of the 315 bank customer respondents across seven selected commercial banks in Nigeria was based on a stratified proportional approach guided by two critical factors: bank size and customer tenure, measured by the average year of account opening. This approach was adopted to ensure the sample adequately captures institutional differences in digital infrastructure, AI readiness, and the longevity of customer relationships, factors that are crucial for assessing the adoption of AI-powered systems for cyberthreat-induced complaint resolution.

Access Bank received a larger share of respondents and the highest average account tenure of 9 years due to its significant size and moderately high customer retention, boosted in part by its merger with Diamond Bank, which expanded both its digital customer base and tenure diversity. Similarly, Zenith Bank and GTBank were allocated substantial proportions of the sample owing to their leading positions in digital innovation and strong market share. However, they tend to have relatively shorter average customer tenures, reflecting their more recent aggressive growth and focus on younger, digitally inclined clientele.

In contrast, UBA and First Bank, as legacy institutions, were also assigned significant portions of the sample. These banks are among the oldest in the country, and their customer base includes long-standing account holders. This makes them particularly valuable in assessing how trust and digital engagement evolve over prolonged banking relationships and institutional familiarity. In addition, Zenith Bank, GTBank, UBA, and First Bank have comparable account tenures of 8 years. Meanwhile, Fidelity Bank and First City Monument Bank (FCMB) received smaller portions of the sample. These banks are relatively smaller in asset size and digital reach and typically have customers with shorter account histories. Although their adoption of AI-based services is emerging, it remains less mature compared to the larger banks. Nevertheless, their inclusion was essential for capturing the diversity of institutional capacities and levels of digital service maturity within the Nigerian banking sector.

5.1. Descriptive Statistics

The descriptive statistics provide an overview of the main variables used in the study, based on responses from 350 participants.

Table 3
Descriptive Statistics of Study Variables

Variable	N	Mean	St. Deviation	Minimum	Maximum
Cyberthreat-induced customer complaints	350	3.75	0.88	1	5
Perceived Severity	350	3.72	0.89	1	5
Perceived Vulnerability	350	3.45	0.92	1	5
Response Efficacy	350	3.88	0.81	1	5
Self-Efficacy	350	3.64	0.85	1	5
Response Cost	350	2.75	1.02	1	5
Respondent Age (years)	350	34.5	8.7	18	58
Customer Tenure (years)	350	7.2	3.4	1	15

Source: Authors

The dependent variable, cyberthreat-induced customer complaints (CICC), recorded a mean score of 3.75 with a standard deviation of 0.88 on a five-point Likert scale. This indicates that, on average, respondents agreed that AI-powered solutions are being used or should be used to address cyber-related complaints in banking. The relatively high mean

suggests a favorable perception of AI systems in enhancing customer service in the context of cybersecurity.

Among the Protection Motivation Theory (PMT) constructs, perceived severity had a mean of 3.72 (SD = 0.89), suggesting that respondents generally view cyberthreats as serious and capable of causing significant harm. Perceived vulnerability had a slightly lower mean of 3.45 (SD = 0.92), indicating that while cyberthreats are seen as severe, there is a moderate level of personal concern or perceived likelihood of being affected. The highest mean was recorded for response efficacy** at 3.88 (SD = 0.81), reflecting strong confidence among respondents in the effectiveness of AI-powered tools, such as chatbots, and automated complaint resolution, in mitigating cyber risks. Similarly, self-efficacy had a mean of 3.64 (SD = 0.85), showing that most participants believe they have the ability or knowledge to use such AI systems effectively.

On the other hand, response cost showed the lowest means of 2.75 (SD = 1.02), implying that respondents do not perceive significant financial, cognitive, or time-related barriers in adopting or interacting with AI-powered systems. The low perceived cost complements the high efficacy scores, strengthening the behavioural intention toward adoption. In terms of demographic characteristics, the average respondent age was 34.5 years (SD = 8.7), reflecting a relatively young but mature group of digital banking users. The average customer tenure was 7.2 years (SD = 3.4), indicating that most respondents had a long-standing relationship with their banks. This long-term engagement may contribute to well-informed opinions regarding the effectiveness and usability of AI-powered systems in handling cybersecurity-related service issues.

Table 4
Correlation Coefficient Matrix

Variable	1	2	3	4	5	6
Cyberthreat-induced customer complaints	1.000					
Perceived Severity	0.583	1.000				
Perceived Vulnerability	0.526	0.626	1.000			
Response Efficacy	0.699	0.544	0.473	1.000		
Self-Efficacy	0.662	0.498	0.448	0.654	1.000	
Response Cost	-0.455	-0.383	-0.335	-0.409	-0.317	1.000

Source: Authors Note: N = 350 respondents

The dependent variable, cyberthreat-induced customer complaints, shows moderate to strong positive correlations with all the protective motivation constructs except response cost, which is negatively related. The strongest association is with response efficacy (0.699), suggesting that individuals who believe AI-powered systems are effective are more likely to support or adopt them. Similarly, self-efficacy (0.662) is strongly correlated, indicating that users who feel capable of interacting with such systems tend to favour their use.

5.2. Validity and Reliability of the Instrument

The internal consistency of the constructs used in this study was assessed using Cronbach's Alpha (α), a standard measure of scale reliability. All five constructions derived from the Protection Motivation Theory (PMT) exhibited satisfactory reliability levels, with alpha coefficients exceeding the minimum acceptable threshold of 0.70.

Table 5
Internal Consistency Reliability

Construct	Cronbach's Alpha (α)	
Perceived Severity	0.85	Good internal consistency
Perceived Vulnerability	0.81	Good reliability
Response Efficacy	0.88	Excellent reliability
Self-Efficacy	0.83	Good internal consistency
Response Cost	0.79	Acceptable to good reliability

Source: Authors

This demonstrates the validity and internal consistency of the questionnaire items used to assess each construct.

5.3. Chi-Square Output

Chi-Square test was conducted to examine the association between threat appraisal, coping appraisal and AI-powered solutions for cyber related customer complaints.

Table 6
Chi-Square Test Results

Statistic	Value
Pearson Chi-square	15.23
Degrees of Freedom (df)	12
p-value	0.2350
Decision	Accept H_0

Source: Authors

Since 0.05, this study failed to reject the null hypothesis that the ordinal logistic regression model fits the data well. This indicates that the OLR model is appropriate and adequately represents the relationships among the behavioral predictors and the implementation of AI-powered solutions for cyberthreat-induced customer complaints.

5.4. Regression Model Results

Perceived severity (β = 0.45, p < 0.05, odds ratio = 1.57) has positive and significant impact on AI-powered customer complaint solutions. This implies that for every 1-unit increase in perceived severity, for every one-unit increase in perceived severity (i.e., the extent to which an individual believes that cyberthreats are serious and potentially damaging), the odds of a higher level of support for AI-powered customer complaint solutions increase by 57%.

Perceived vulnerability (β = 0.38, p < 0.05, odds ratio = 1.46) has positive and significant impact on AI-powered customer complaint solutions. This indicates that for every one-unit increase in perceived vulnerability (i.e., individuals who feel more personally susceptible to cyberthreats), the odds of a higher level of support for AI-powered customer complaint solutions increase by 46%.

Table 7
Ordinal Logistic Regression Results Table
Dependent Variable: AI-Powered Solutions for Cyberthreat-Induced Customer Complaints

Variable	Coefficient (β)	Odds Ratio (e^β)	p-value
Perceived Severity (PSEV)	0.4548	1.57	0.0013
Perceived Vulnerability (PVUL)	0.3867	1.46	0.0005
Response Efficacy (RESP)	0.6582	1.91	0.0001
Self-Efficacy (SELF)	0.5871	1.79	0.0002
Response Cost (COST)	-0.4045	0.67	0.0072
	Log-likelihood = -420.3619		
	Akaike Information Criterion (AIC) = 852.72		
	Pseudo R-squared = 0.6342		
	LR Chi-Square = 68.2344		
	Prob > Chi-Square = 0.0000		

Source: Authors

Response efficacy (β = 0.65, p < 0.05, odds ratio = 1.91) has positive and significant impact on AI-powered customer complaint solutions. This implies that for every unit increase in response efficacy (i.e., belief in the effectiveness of AI solutions to address cyber-related complaints), the odds of a higher category of support increase by 91%.

Self-efficacy (β = 0.58. p < 0.05, odds ratio = 1.79) has positive and significant impact on AI-powered customer complaint solutions. This implies that for each one-unit increase in self-efficacy (i.e., confidence in one's ability to effectively use AI systems), the

odds of a higher likelihood of support increase by 79%. This underscores the importance of user confidence and skill in shaping technology acceptance.

However, response Cost ($\beta = -0.40$, $p < 0.05$, odds ratio = 0.67) has negative and significant impact on the AI-powered customer complaint solutions. This means that for every one-unit increase in perceived cost (such as perceived burden, inconvenience, or resource demands), the odds of being in a higher category of supporting AI-powered solution decrease by 33%. This finding signals the deterrent effect of perceived burden or inconvenience on user acceptance of AI systems.

The log-likelihood value of -420.36 and an Akaike Information Criterion (AIC) of 852.72 indicate a well-fitting model, while the Likelihood Ratio Chi-Square of 68.23 ($p < 0.05$) confirms that the full model significantly improves upon the null model. A pseudo-R-squared value of 0.6342 suggests that approximately 63% of the variation in the dependent variable is explained by the PMT constructs, a relatively strong effect size for behavioral research involving ordinal data.

5.5. Discussion of Results

Perceived severity exerts a positive and statistically significant impact on AI-powered solutions for cyberthreat-induced customer complaints. This implies that individuals who recognize the potential damage and seriousness of cyber incidents are more likely to support the deployment of automated, intelligent systems to manage such threats. The more severe a threat is perceived to be, the greater the motivation to engage with protective technologies like AI-enabled chatbots, anomalies detection tools, or automated response platforms. This finding aligns with the protection motivation theory (PMT) which posits that the perception of a threat's severity motivates individuals to adopt coping mechanisms when effective solutions are available.

Perceived vulnerability has a positive and statistically significant impact on AI-powered solutions for addressing cyberthreat-induced customer complaints. This suggests that when customers or bank staff feel more exposed or at risk of being affected by cyber incidents such as identity theft, online fraud or unauthorized access, they are more inclined to endorse intelligent digital systems capable of detecting, reporting, and resolving such threats. The perception of vulnerability enhances the motivation to engage in protective behavior, particularly when there is trust in the availability and effectiveness of the coping mechanism, in this case, AI-enabled technologies. This finding supports the PMT, which posits that individuals are more likely to take preventive or responsive actions when they perceive themselves to be vulnerable to harm.

Response efficacy exhibits a positive and statistically significant impact on AI-powered solutions for cyberthreat-induced customer complaints. This means that when individuals, whether customers or frontline bank staff, are confident that AI tools (such as automated anomaly detection systems, chatbots, or intelligent ticket resolution platforms) can provide timely, accurate, and efficient responses to cyber incidents, they are more inclined to support or engage with these technologies. From the perspective of protection motivation theory, this finding reflects the importance of the coping appraisal process. Response efficacy enhances motivation to adopt protective behaviors when individuals believe that the proposed response (in this case, AI-powered solutions) is both relevant and capable of mitigating perceived threats.

Self-efficacy shows a positive and statistically significant impact on AI-powered solutions for cyberthreat-induced customer complaints. This result highlights the importance of users perceived competence in determining their willingness to engage with technology. Individuals who believe they can successfully navigate AI-enabled complaint resolution systems (such as virtual assistants, smart forms, or anomaly detection tools) are more likely to accept and utilize these innovations. In other words, greater confidence in one's digital capabilities translates into stronger adoption behavior. From the standpoint of PMT, self-efficacy determines whether individuals choose to take protective actions in the face of perceived threats. When users feel capable of interacting with AI systems, they are more likely to see such tools as viable and useful in managing cyber-related banking issues.

Response cost has a negative and statistically significant impact on AI-powered solutions for cyberthreat-induced customer complaints. This means that when individuals perceive that engaging with AI-powered systems is burdensome, whether due to unfamiliar technology, complex interfaces, privacy concerns, or lack of human interaction, they are less likely to support or use these solutions, regardless of how effective the systems may be. Within the framework of PMT, response cost serves as a counterweight to perceived efficacy and self-efficacy. Even if users believe that AI tools are effective and that they can use them, high perceived costs can still reduce motivation to adopt.

Table 8
Summary of Findings

Hypothesis	Description	Remark
H_{01}	Perceived severity does not significantly affect AI-powered customer complaint solutions	Reject
H_{02}	Perceived vulnerability does not significantly affect AI-powered customer complaint solutions	Reject
H_{03}	Response efficacy does not significantly affect AI-powered customer complaint solutions	Reject
H_{04}	Self-efficacy does not significantly affect AI-powered customer complaint solutions	Reject
H_{05}	Response cost does not significantly affect AI-powered customer complaint solutions	Reject

Source: Authors

5.6. Model Fitness

The log-likelihood value of -420.36 and an Akaike Information Criterion (AIC) of 852.72 indicate a well-fitting model, while the Likelihood Ratio Chi-Square of 68.23 ($p < 0.05$) confirms that the full model significantly improves upon the null model. This indicates that the inclusion of the protection motivation theory (PMT) constructs improves the predictive power of the model without leading to overfitting. As such, the independent variables, perceived severity, perceived vulnerability, response efficacy, self-efficacy and response cost, jointly contribute to explaining the variation in the ordinal dependent variable, AI-powered solutions for cyberthreat-induced customer complaints. Thus, the significant LR Chi-Square test validates the inclusion of these behavioral variables and supports the model's theoretical framework.

A Pseudo R-squared value of 0.6342 suggests that approximately 63% of the variation in the dependent variable is accounted for by the model. This indicates that the PMT-based model captures a significant portion of the underlying decision-making and psychological processes that drive the behavior in response to AI-powered customer complaints solutions. Collectively, these metrics confirm that the model is not only statistically significant but also theoretically coherent and practically meaningful for understanding the behavioral drivers of AI-powered customer complaints solutions for banks in low-income countries.

5.7. Test of Proportional Odds Assumption

Brant test is used to evaluate the proportional odds assumption, which is a key requirement for the validity of the ordinal logistic regression (OLR) model. The parallel lines assumption, or consistency assumption is postulated to specify a statistical homogeneity in the nature of the relationships between any two groups of outcomes, implying that the impact of independent variables does not vary over any level of the dependent variable.

The Brant test was used to determine the data on whether the fundamental assumption of ordinal logistic regression (OLR) model was met in terms of odds. The overall Brant test statistics (chi 2 = 6.75, $p > 0.05$) confirm that the proportional odds assumption is met at the overall level. Furthermore, all PMT variables had p-value above 0.05, meaning that none of the components were found to be in variance with proportional odds. This finding strengthens the validity of OLR estimates and it proves that the model had been specified properly. As a result, it is apposite to use OLR to investigate the impact of the PMT constructs on AI-based solutions to cyber-related customer complaints.

Table 9
Brant Test Results

Variable	Chi-Square	p-value
Perceived Severity (PSEV)	2.14	0.143
Perceived Vulnerability (PVUL)	1.89	0.169
Response Efficacy (RESP)	0.97	0.324
Self-Efficacy (SELF)	1.22	0.269
Response Cost (COST)	0.53	0.466
Overall Test	6.75	0.241

Source: Authors

6. Conclusion

This paper discussed the behavioral factors that drive AI powered solution to customer complaints due to cyber threats in banks, but in low-income countries. This study concludes that perceived severity, perceived vulnerability, response efficacy, self-efficacy, and response cost are the major behavioural determinants of AI-powered solutions for cyberthreat-induced customer complaints among low-income countries' banking sector. Therefore, this study contributes to the growing field of AI solutions for cyber related customer complaints in financial services by offering a behaviourally grounded framework for understanding how threat appraisals and coping appraisals drive support for AI-powered cyber complaint solutions.

6.1. Recommendations

This study, therefore, recommends that banks in low-income countries should actively communicate the effectiveness and success rates of AI-powered tools such as chatbots, anomaly detection systems, and automated complaint resolution platforms to demonstrate how these systems resolve issues faster, more securely, and more accurately will build trust among users. In addition, banks in low-income countries should prioritize seamless navigation through in-app guides, minimal input requirements, and multilingual or audio-visual assistance features to lower entry barriers for diverse users and improve customer and staff confidence in using digital platforms. Regulatory bodies across low-income countries should issue clear frameworks and ethical guidelines to govern the deployment of AI in customer service to ensure transparency, data protection, and accountability, thereby building public trust in AI.

6.2. Limitations and Suggestions for Future Studies

The study sampled banks with international authorization using Nigeria as the sole representation of low-income countries. This may limit the generalizability of the findings to banks in other economic environments with different regulatory classifications (e.g., national or regional banks). In addition, the sample was restricted to bank customers and frontline staff, excluding other relevant factors such as cybersecurity managers, AI system developers, or financial regulators, whose perspectives might provide a more holistic understanding of AI adoption barriers and enablers. Finally, while the protection motivation theory (PMT) offers a strong theoretical lens, the study focused only on its core constructs. Other potentially relevant behavioural or psychological variables, such as trust in technology, prior digital literacy, institutional transparency, or organizational culture, were not included.

Future research should consider expanding the geographical scope to include multiple low- and middle-income countries could enable comparative analysis across different technological, regulatory and cultural settings, so as to enhance the external validity of results. Additionally, mixed-methods or qualitative studies, such as interviews or focus groups with customers, developers, and IT personnel, can provide deeper insight into underlying motivations, barriers, and experiences that are not easily captured through surveys alone. Finally, future studies may explore how institutional environments such as data protection laws and government-led digital transformation initiatives influence the speed, implementation and success of AI cyber complaint solution.

Author Contributions

Victor Oluwatosin Ologun: Conceptualization, Methodology, Data analysis, Supervision
Ayomide Olugbade: Conceptualization, Methodology, Data analysis
Patience Farida Azuikpe: Conceptualization, Methodology, Data analysis
Michael Aderemi Adegbite: Conceptualization, Methodology, Data analysis
Olawale Abdulmumin Lawal: Conceptualization, Methodology, Data analysis
Stephen Alaba John: Conceptualization, Methodology, Data analysis, Supervision

Conflict of Interests/Disclosures

The authors declared no potential conflicts of interest w.r.t the research, authorship and/or publication of this article.

References

Abubakar, R. A., Aliyu, A. A., Yashe, Z. B., Ahmad, M. A., Abdulkadir, S., Ibrahim, M., & Ahmed, A. M. (2025). Enhanced Ai-Powered Customer Experience Model. *Science World Journal*, *20*(1), 17-21. https://doi.org/10.4314/swj.v20i1.3

Al-Gasaymeh, A., Alsmadi, A. A., Alrawashdeh, N., Alzoubi, H. M., & Alshurideh, M. (2023). Dynamic Model in Estimating the Impact of Competition on Banking Efficiency: Evidence Form Mena Countries. *Calitatea*, *24*(193), 385-394.

Alaba, J. S., Ahmed, S. J., Farida, A. P., & Oluwatosin, O. V. (2025). Adoption of Ai-Driven Fraud Detection System in the Nigerian Banking Sector: An Analysis of Cost, Compliance, and Competency. *Economic Review of Nepal*, *8*(1), 16-33. https://doi.org/https://doi.org/10.3126/ern.v8i1.80740

AlAfnan, M. A. (2024). Large Language Models as Computational Linguistics Tools: A Comparative Analysis of Chatgpt and Google Machine Translations. *Journal of Artificial Intelligence and Technology*. https://doi.org/10.37965/jait.2024.0549

Almustafa, E., Assaf, A., & Allahham, M. (2023). Implementation of Artificial Intelligence for Financial Process Innovation of Commercial Banks. *Revista de Gestão Social e Ambiental*, *17*(9), e04119. https://doi.org/10.24857/rgsa.v17n9-004

Ashrafuzzaman, M., Parveen, R., Sumiya, M. A., & Rahman, A. (2025). Ai-Powered Personalization in Digital Banking: A Review of Customer Behavior Analytics and Engagement. *American Journal of Interdisciplinary Studies*, *6*(1), 40-71.

Changalreddy, V., & Vashishtha, S. (2024). Predictive Analytics for Reducing Customer Churn in Financial Services. *International Journal for Research in Management and Pharmacy (IJRMP), 13 (12), 22. https://www. ijrmp. org*.

Chen, J.-S., Le, T.-T.-Y., & Florence, D. (2021). Usability and Responsiveness of Artificial Intelligence Chatbot on Online Customer Experience in E-Retailing. *International Journal of Retail & Distribution Management*, *49*(11), 1512-1531. https://doi.org/10.1108/IJRDM-08-2020-0312

Chien, S.-C., Yen, C.-M., Chang, Y.-H., Chen, Y.-E., Liu, C.-C., Hsiao, Y.-P.,…Lu, X.-H. (2025). Use of Artificial Intelligence, Internet of Things, and Edge Intelligence in Long-Term Care for Older People: Comprehensive Analysis through Bibliometric, Google Trends, and Content Analysis. *Journal of Medical Internet Research*, *27*, e56692. https://doi.org/https://doi.org/10.2196/56692

Correia, A.-P., Hickey, S., & Xu, F. (2024). Beyond the Virtual Classroom: Integrating Artificial Intelligence in Online Learning. *Distance Education*, *45*(3), 481-491. https://doi.org/https://doi.org/10.1080/01587919.2024.2338706

Eskandarany, A. (2024). Adoption of Artificial Intelligence and Machine Learning in Banking Systems: A Qualitative Survey of Board of Directors. *Frontiers in Artificial Intelligence*, *7*, 1440051. https://doi.org/10.3389/frai.2024.1440051

Gonaygunta, H. (2023). Machine Learning Algorithms for Detection of Cyber Threats Using Logistic Regression. *International Journal of Smart Sensor and Adhoc Network.*, 36-42. https://doi.org/10.47893/IJSSAN.2023.1229

Hsu, C.-L., & Lin, J. C.-C. (2023). Understanding the User Satisfaction and Loyalty of Customer Service Chatbots. *Journal of Retailing and Consumer Services*, *71*, 103211. https://doi.org/10.1016/j.jretconser.2022.103211

Ifekanandu, C. C., Anene, J. N., Iloka, C. B., & Ewuzie, C. O. (2023). Influence of Artificial Intelligence (Ai) on Customer Experience and Loyalty: Mediating Role of Personalization. *Journal of Data Acquisition and Processing*, *38*(3), 1936. https://doi.org/https://doi.org/10.5281/zenodo.98549423

Jada, I., & Mayayise, T. O. (2024). The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome of a Systematic Literature Review. *Data and Information Management*, *8*(2), 100063. https://doi.org/10.1016/j.dim.2023.100063

Juipa, A., Guzman, L., & Diaz, E. (2024, 2024). Sentiment Analysis-Based Chatbot System to Enhance Customer Satisfaction in Technical Support Complaints Service for Telecommunications Companies:. 21st International Conference on Smart Business Technologies,

Kumar, P., Singh, A., & Saha, S. (2024). Navigating the Indian Code-Mixed Terrain: Multitasking Analysis of Complaints, Sentiment, Emotion, and Severity. https://doi.org/10.2139/ssrn.4827145

Metha, S. (2025). Ai-Driven Fraud Detection: A Risk Scoring Model for Enhanced Security in Banking. *Journal of Engineering Research and Reports*, *27*(3), 23-34. https://doi.org/10.9734/jerr/2025/v27i31415

MUHAMMAD, T., & STUKALINA, Y. (2025). The Role of Ai-Powered Chatbots in Enhancing Customer Experience: Systematic Literature Review. https://doi.org/https://doi.org/10.3846/bm.2025.1482

Pio, P. G. C., Sigahi, T., Rampasso, I. S., Satolo, E. G., Serafim, M. P., Quelhas, O. L. G.,…Anholon, R. (2024). Complaint Management: Comparison between Traditional and Digital Banks and the Benefits of Using Management Systems for Improvement. *International Journal of Productivity and Performance Management*, *73*(4), 1050-1070. https://doi.org/10.1108/IJPPM-08-2022-0430

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The journal of psychology*, *91*(1), 93-114. https://doi.org/https://doi.org/10.1080/00223980.1975.9915803

Roumeliotis, K. I., Tselikas, N. D., & Nasiopoulos, D. K. (2025). Think before You Classify: The Rise of Reasoning Large Language Models for Consumer Complaint Detection and Classification. *Electronics*, *14*(6), 1070. https://doi.org/10.3390/electronics14061070

Roy, T. S., Vasukidevi, G., Malleswari, T. N., Ushasukhanya, S., & Namratha, N. (2024). Automatic Classification of Railway Complaints Using Machine Learning. E3S Web of Conferences,

Seok, J.-s., Kim, C.-y., Kim, S.-y., & Kim, Y.-M. (2024). Deep-Learning-Based Customer Complaints Monitoring System Using Online Review. https://doi.org/10.2139/ssrn.4795530

Sharma, S., Vashisht, M., & Kumar, V. (2024, 2024-2-24). Enhanced Customer Insights: Multimodal Nlp Feedback System. 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS),

Tula, S. T., Kess-Momoh, A. J., Omotoye, G. B., Bello, B. G., & Daraojimba, A. I. (2024). Ai-Enabled Customer Experience Enhancement in Business. *Computer Science & IT Research Journal*, *5*(2), 365-389.

Tulcanaza-Prieto, A. B., Cortez-Ordoñez, A., & Lee, C. W. (2023). Influence of Customer Perception Factors on Ai-Enabled Customer Experience in the Ecuadorian Banking Environment. *Sustainability*, *15*(16), 12441. https://doi.org/https://doi.org/10.3390/su151612441

Vairetti, C., Aránguiz, I., Maldonado, S., Karmy, J. P., & Leal, A. (2024). Analytics-Driven Complaint Prioritisation Via Deep Learning and Multicriteria Decision-Making. *European Journal of Operational Research*, *312*(3), 1108-1118. https://doi.org/10.1016/j.ejor.2023.08.027

Vethachalam, S. (2025). Cybersecurity Automation: Enhancing Incident Response and Threat Mitigation.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *Ieee Access*, *8*, 146598-146612. https://doi.org/https://doi.org/10.1109/ACCESS.2020.3013145

Zhang, K., Zhou, F., Wu, L., Xie, N., & He, Z. (2024). Semantic Understanding and Prompt Engineering for Large-Scale Traffic Data Imputation. *Information Fusion*, *102*, 102038. https://doi.org/10.1016/j.inffus.2023.102038