Issues in Information Systems
Volume 26, Issue 2, pp. 162-170, 2025

DOI: https://doi.org/10.48009/2_iis_113

The convergence of AI, cybersecurity, e-commerce, and supply chain management: A study on intelligent systems for digital risk mitigation and operational efficiency

Jose Vidal, *Universidad Ana G. Méndez G. Méndez, Gurabo Campus, jvidal23@email.uagm.edu*
Ángel Ojeda-Castro, *Universidad Ana G. Méndez G. Méndez Gurabo Campus,ut_aojeda@uagm.edu*
Rafael Padilla-Vega, *Universidad Ana G. Méndez G. Méndez, Gurabo Campus, padillar1@uagm.edu*
Monica Ocasio, *Universidad Ana G. Méndez G. Méndez, Cupey Campus, mocasio16@uagm.edu*

Abstract

This study presents a comprehensive literature review examining the convergence of cybersecurity, e-commerce, supply chain management, and consumer engagement in the digital economy. Drawing on ten scholarly sources, this study explores key themes such as fraud detection using machine learning, cost behavior in e-commerce firms, the impact of Internet of Things (IoT) technologies in retail, and data science applications in cybersecurity. A central focus is the role of artificial intelligence (AI) and Genetic Algorithms (GA) in enhancing the accuracy of fraud detection systems, as well as the application of collaborative algorithms to identify fake reviews in online platforms. The research also analyzes how digital transformation influences cost structures, consumer trust, and cybersecurity resilience. Findings reveal that AI and machine learning are crucial in enhancing operational efficiency and safeguarding against emerging cyber threats. However, challenges such as data quality, model interpretability, and standardization persist. The study emphasizes the importance of adopting strategic, data-driven approaches and fostering interdisciplinary collaboration to address these issues. Implications for future research include the development of real-time fraud detection models, the ethical deployment of AI, and the enhancement of public-private cybersecurity partnerships. Ultimately, the research highlights the importance of intelligent systems and adaptive strategies in developing secure, efficient, and consumer-centric digital infrastructures in an increasingly interconnected world.

Keywords: artificial intelligence, cybersecurity, e-commerce, fraud, genetic algorithms, and internet of things.

Introduction

In today's rapidly evolving digital landscape, the convergence of supply chain management, cybersecurity, e-commerce, and consumer engagement has created complex challenges and new research opportunities. This review compiles and analyzes ten scholarly publications that provide diverse perspectives on these interconnected domains. Topics such as supply chain complexity, fraud detection using machine learning, the impact of the Internet of Things (IoT) in retail, pricing strategies in e-commerce, and data science applications in cybersecurity are thoroughly examined (Ileberi et al., 2022). These studies offer a comprehensive understanding of the emerging trends and obstacles in the digital economy, addressing both technological advancements and evolving consumer behavior (Ates et al., 2020).

A central theme in this body of research is the increasing use of machine learning and artificial intelligence

to combat digital fraud, particularly in the financial services sector. Credit card fraud, fueled by the proliferation of online transactions and contactless payments, poses a persistent threat. Conventional rule-based fraud detection systems are no longer sufficient to detect increasingly sophisticated schemes. As such, machine learning algorithms, including support vector machines and neural networks, have shown promising results in pattern recognition and anomaly detection (Ileberi et al., 2022). The use of Genetic Algorithms (GA) for feature selection further enhances model efficiency, helping to isolate the most predictive attributes in large datasets and improving the accuracy of fraud detection systems.

In parallel, other sectors such as e-commerce are also undergoing digital transformation. Research by Argilés-Bosch et al. (2023) examines the differences in cost behavior between e-commerce firms and traditional retail structures, particularly in their allocation of operational and labor expenses. The adoption of digital technologies not only shifts cost dynamics but also requires businesses to develop strategic approaches to remain profitable while navigating rapidly changing market environments. Similarly, studies on social commerce highlight the role of mobile applications and advanced data clustering techniques in enhancing consumer engagement and personalizing the retail experience (Abkenar et al., 2022).

Cybersecurity remains a dominant concern across all digital sectors. Sarker et al. (2020) emphasize the need for data-driven approaches to identify and respond to threats in real time, particularly as conventional security frameworks become obsolete. Furthermore, research on cybersecurity awareness (Chaudhary et al., 2022) and the integrity of online content, such as fake reviews (Zhang et al., 2023), reveals the importance of both human factors and algorithmic solutions in building resilient digital ecosystems. Finally, Luo and Choi (2020) discuss the role of governments in ensuring cybersecurity within global e-commerce supply chains, advocating for collaborative frameworks that integrate regulatory oversight with technological innovation. Together, these studies underscore the pressing need for interdisciplinary strategies to secure and optimize digital operations in an increasingly connected world.

Background and Literature Review

The literature reveals a growing reliance on artificial intelligence and statistical algorithms to combat increasingly sophisticated cyber threats, especially in the financial sector. Ileberi et al. (2022) emphasize the importance of feature selection in developing effective fraud detection models, particularly using Genetic Algorithms (GA). These algorithms enable the extraction of the most significant features from transactional data, thereby improving the accuracy and efficiency of credit card fraud detection systems. As credit card fraud continues to rise due to the widespread adoption of online commerce and contactless payments, machine learning techniques such as decision trees, neural networks, and support vector machines have demonstrated considerable potential. However, the high dimensionality of data poses challenges, which GA-based feature selection helps mitigate.

Cost behavior within the e-commerce industry is another crucial area that has been extensively explored in the literature. Argilés-Bosch et al. (2023) investigate how e-commerce firms manage operational expenses and respond to shifting market demands. The study highlights that e-commerce enterprises face distinct cost structures compared to traditional retailers, characterized by higher operational costs and lower labor costs. The dynamic nature of digital markets necessitates flexible cost management strategies to maintain profitability while adapting to external changes. The impact of technological advancement and digital innovation on cost behavior further underscores the need for continuous adaptation and data-driven decision-making.

Cybersecurity data science also emerges as a critical theme, where machine learning and data analysis are

increasingly deployed to identify and respond to threats. Sarker et al. (2020) discuss how data science methods like clustering, anomaly detection, and real-time pattern recognition play a central role in modern cybersecurity strategies. The review outlines the challenges associated with machine learning applications, including the need for high-quality labeled datasets, vulnerability to adversarial attacks, and the importance of interpretability. Despite these hurdles, the integration of advanced analytics into cybersecurity has the potential to enhance threat detection, support intelligent decision-making, and protect digital infrastructures.

In the context of digital consumer behavior, Zhang et al. (2023) examine how fake reviews affect trust in e-commerce platforms. They propose a spammer group detection algorithm based on collaborative patterns among users, which improves upon traditional models that often ignore reviewer relationships. Likewise, Ajayi et al. (2023) explore the transformative role of the Internet of Things (IoT) in enhancing retail experiences, advocating for its use in personalized marketing and customer engagement. Meanwhile, Fries and Kassemeier (2024) analyze the implications of price changes in B2B sales, and Ates et al. (2020) present a meta-analysis on the impact of supply chain complexity on firm performance. Across these diverse topics, the literature consistently supports the integration of machine learning, digital analytics, and strategic management to address emerging challenges in cybersecurity, e-commerce, and supply networks.

Research Variables

The study of cost behavior in e-commerce firms involves key operational variables, including operational costs, labor costs, cost of goods sold, and resource allocation, which are essential to understanding how companies adapt financially in a digital environment. According to Argilés-Bosch et al. (2023), these variables enable researchers to investigate how cost structures differ from those of traditional retail businesses and how companies optimize costs to strike a balance between present profitability and future growth. Regression models and statistical analysis were employed to assess the sensitivity of these cost components to changes in e-commerce operations. This methodological framework highlights how cost behavior is both dynamic and influenced by external market pressures, technological adoption, and firm strategy.

In the context of cybersecurity data science, the study focuses on variables that evaluate the role of machine learning techniques, such as classification, clustering, and anomaly detection, in improving organizational security. Key variables include threat detection rate, response time, and false positive/negative ratios, which help quantify the effectiveness of machine learning in identifying cyber threats. Sarker et al. (2020) emphasize that these indicators are crucial for assessing the contribution of data-driven models to real-time cybersecurity decision-making. Internal and external values, such as innovation capacity and security posture, also serve as dependent variables to understand the strategic impact of cybersecurity measures within digital infrastructures.

When analyzing fraudulent reviewer detection in heterogeneous networks of buyers and sellers, the study incorporates variables such as review frequency, rating patterns, review text semantics, and reviewer history. These features are utilized by the collaborative training-based spammer group algorithm to identify coordinated spammer groups and enhance the accuracy of fraud detection (Zhang et al., 2023). The algorithm benefits from behavioral and relational data within networks, identifying users with suspiciously similar activity. This approach enables the detection system to differentiate between individual dishonest reviewers and orchestrated spam campaigns, adding a layer of precision to digital trust management.

Lastly, in measuring the effectiveness of cybersecurity awareness programs, Chaudhary et al. (2022)

highlight variables such as employee knowledge levels, behavior change, training participation, and key performance indicators (KPIs). These metrics are instrumental in evaluating the success of awareness initiatives. Pre and post-survey data are compared to determine whether the program led to improved cybersecurity practices and reduced vulnerability. Similarly, in the domain of retail engagement, variables like real-time customer interaction, purchase behavior, and IoT sensor feedback are central to assessing how technological advancements influence consumer behavior (Ajayi et al., 2023). Together, these variables form a comprehensive analytical framework to investigate performance and innovation in digital business environments.

Research Contribution

The contribution of this research lies in highlighting the strategic integration of information management and statistical algorithms, including artificial intelligence (AI), as essential tools for strengthening cybersecurity and enhancing operational performance within the retail and technology sectors. By synthesizing insights from multiple studies, the research highlights how these technologies can be leveraged to detect vulnerabilities, prevent cyberattacks, personalize customer experiences, and enhance supply chain efficiency. Specifically, the use of AI enables real-time threat detection and adaptive decision-making, while data analytics support tailored marketing strategies and customer engagement, ultimately fostering trust and driving revenue growth (Ileberi et al., 2022; Argilés-Bosch et al., 2023; Sarker et al., 2020). Furthermore, the study acknowledges the current challenges, including handling large volumes of data and the shortage of skilled professionals. Still, it emphasizes that proactive investment in data-driven solutions is crucial for achieving a competitive advantage and long-term success in both cybersecurity and digital commerce domains (Zhang et al., 2023; Chaudhary et al., 2022).

Research Questions

1. *To what extent can the use of a genetic algorithm (GA) for feature selection improve the accuracy of machine learning models in detecting credit card fraud?*

2. *How do machine learning applications in cybersecurity data science influence the enhancement of external cybersecurity protocols and threat detection mechanisms?*

3. *How effective is a collaborative training-based algorithm in detecting fraudulent reviewers in heterogeneous online networks based on user behavior and review features?*

4. *What is the impact of cybersecurity awareness programs on employee knowledge and behavior, and how do these programs influence cybersecurity practices in e-commerce supply chains?*

Research Prepositions

This section outlines thematic propositions derived from the synthesized literature review. These are intended to reflect grounded assumptions based on existing academic findings rather than speculative claims.

1. Machine learning-based approaches contribute significantly to enhancing internal organizational capabilities, such as innovation capacity and operational efficiency, particularly in the context of fraud detection and cybersecurity systems (Ileberi et al., 2022; Sarker et al., 2020).

2. The adoption of artificial intelligence and data-driven models has a positive influence on external organizational value, improving consumer trust, customer engagement, and responsiveness to digital threats in e-commerce and supply chain environments (Zhang et al., 2023; Ajayi et al., 2023; Argilés-Bosch et al., 2023).

3. Cybersecurity data science, through the integration of anomaly detection, pattern recognition, and real-time threat mitigation, enhances internal network innovation and security posture within digitally connected organizations (Sarker et al., 2020; Chaudhary et al., 2022).

4. The application of intelligent systems and collaborative algorithms fosters external resilience by supporting adaptive cybersecurity frameworks, reducing exposure to fraud, and strengthening digital trust across consumer platforms (Zhang et al., 2023; Luo & Choi, 2020).

Methodology

This study employs a qualitative research design, incorporating an extensive review of scholarly literature to explore the evolving roles of artificial intelligence (AI), data analytics, and computational models in cybersecurity and market sectors. The literature was systematically gathered from academic databases including JSTOR, ScienceDirect, SpringerLink, and Google Scholar, using keywords such as "AI in cybersecurity," "fraud detection machine learning," "IoT in retail," "e-commerce cost behavior," and "collaborative filtering fake reviews." Studies were included based on recency (published between 2020 and 2024), peer-reviewed status, citation impact, and relevance to the four stated research questions. Out of an initial pool of 50 articles, ten were selected for in-depth analysis based on these criteria.

The selection of authors, including Ileberi, Sarker, Ajayi, Abkenar, Luo, and Choi, was based on the significance of their contributions to the field, as evidenced by high citation counts, pioneering methodological frameworks, or recent influential findings in high-impact journals. These authors represent diverse perspectives on machine learning, genetic algorithms, cybersecurity strategy, and digital consumer behavior analytics. The participants and context of the study are indirectly represented through the literature, focusing on key stakeholders including cybersecurity professionals, businesses in the financial and e-commerce sectors, and technology-driven retail enterprises. Special attention is given to how these entities are integrating AI-based solutions to enhance fraud recognition systems and to improve customer interaction in dynamic digital environments (Sarker et al., 2020; Ajayi et al., 2023). In particular, the study examines how mobile applications, interconnected devices (IoT), and consumer data are utilized to predict behavioral patterns and optimize service delivery in the retail industry (Abkenar et al., 2022). The methodology provides a structured framework for synthesizing insights across disciplines, supporting the development of more resilient and data-informed business strategies.

Findings

The reviewed studies reveal that machine learning and data science are playing increasingly vital roles in enhancing digital security and operational efficiency across industries. Ileberi et al. (2022) demonstrate that Genetic Algorithms improve the accuracy of credit card fraud detection by selecting optimal features for machine learning models. In e-commerce, Argilés-Bosch et al. (2023) identify cost variability and operational inefficiencies as critical factors influencing financial performance, offering insights for strategic cost management. Sarker et al. (2020) highlight the growing importance of data-driven cybersecurity models but caution against persistent challenges, such as adversarial attacks, and emphasize the need for

high-quality data. Zhang et al. (2023) address the issue of fraudulent reviews in e-commerce through a collaborative training-based algorithm, improving detection accuracy and consumer trust.

Additional findings emphasize the importance of targeted cybersecurity education and emerging technologies in shaping digital strategies. Chaudhary et al. (2022) emphasize the importance of standardized metrics for evaluating cybersecurity awareness programs effectively. Ajayi et al. (2023) demonstrate how IoT technologies are transforming retail by enabling real-time customer engagement, although gaps remain in understanding the mechanisms of consumer behavior. In the realm of pricing, Fries and Kassemeier (2024) call for more empirical research on B2B price increases and their financial impacts. A meta-analysis by Ates et al. (2020) confirms that unmanaged supply chain complexity hinders firm performance, while Abkenar et al. (2022) propose hybrid analytical methods to enhance social commerce applications. Finally, Luo and Choi (2020) argue for stronger public-private collaboration to address cybersecurity threats in e-commerce supply chains, underscoring the government's strategic role in safeguarding digital infrastructure.

Discussion of Findings

The discussion of findings across the reviewed literature highlights how emerging technologies, particularly machine learning and data science, are being leveraged to address modern digital and operational challenges. For instance, Ileberi et al. (2022) demonstrate how Genetic Algorithms can enhance credit card fraud detection by selecting the most relevant features, improving the precision of machine learning classifiers used by financial institutions. Similarly, Argilés-Bosch et al. (2023) provide a valuable framework for understanding cost behavior in e-commerce firms, revealing how cost variability and inefficiencies can be mitigated through better strategic management. The studies by Sarker et al. (2020) and Zhang et al. (2023) both underscore the importance of AI-based approaches: the former in strengthening cybersecurity resilience through data-driven models, and the latter in boosting trust in online reviews by detecting coordinated spammer groups using collaborative training algorithms.

Other findings stress the growing influence of digital transformation in areas such as, consumer engagement, cybersecurity training, and pricing strategies. Chaudhary et al. (2022) argue that cybersecurity awareness efforts require standardized metrics to evaluate program effectiveness and foster meaningful behavioral change. Ajayi et al. (2023) demonstrate how IoT technologies enhance customer experiences in retail, while Fries and Kassemeier (2024) examine the impact of price increases on global B2B profitability and competitiveness. Ates et al. (2020) contribute insights into how supply chain complexity impacts firm performance, advocating for integrated management strategies. Abkenar et al. (2022) propose a hybrid analytical model that enables businesses to refine their social commerce applications. Finally, Luo and Choi (2020) emphasize the importance of government collaboration in enhancing cybersecurity across e-commerce supply chains, underscoring the crucial role of policy in ensuring digital resilience.

Implications for Research

This research underscores the pressing need for ongoing interdisciplinary investigation into the intersection of artificial intelligence, data analytics, cybersecurity, and digital commerce. As the digital economy evolves, future studies should explore how machine learning algorithms, such as Genetic Algorithms for fraud detection or collaborative training models for identifying fake reviews, can be scaled and integrated across sectors to enhance operational efficiency and consumer protection (Ileberi et al., 2022; Zhang et al., 2023). Additionally, given the dynamic cost structures observed in e-commerce firms, there is an

opportunity further to investigate adaptive financial modeling in response to digital transformation (Argilés-Bosch et al., 2023). In cybersecurity, the demand for robust, real-time threat detection models calls for research into explainable AI and the ethical implications of algorithmic decision-making (Sarker et al., 2020). Similarly, the impact of IoT on consumer behavior, as well as the effectiveness of awareness programs, suggests that research should expand to include longitudinal studies and cross-cultural analyses (Ajayi et al., 2023; Chaudhary et al., 2022). Lastly, the role of governance and public-private partnerships in securing global digital infrastructures warrants a deeper empirical examination, particularly in light of the rising cyber threats and the need for coordinated international policy responses (Luo & Choi, 2020).

Limitations

Despite offering valuable insights across cybersecurity, e-commerce, and supply chain management, this research is constrained by several notable limitations. First, as a literature-based qualitative review, the study relies on secondary data from previously published works, which may introduce publication bias and limit the generalizability of the findings to current or emerging real-time industry scenarios. Additionally, many of the reviewed studies focus on conceptual frameworks or theoretical models, with limited empirical validation across diverse geographic or organizational contexts. For example, the impact of AI algorithms, such as Genetic Algorithms and collaborative training models, may vary across industries and data environments; however, this variability is not fully captured. Furthermore, the lack of access to proprietary datasets, particularly in cybersecurity and financial fraud detection, restricts the ability to evaluate algorithm performance in live operational settings. Lastly, some studies highlight unresolved challenges, such as the shortage of high-quality labeled data for machine learning models, ethical concerns related to consumer privacy, and the limited availability of standardized metrics for cybersecurity awareness programs, which signal the need for further empirical investigation and cross-sector collaboration.

Conclusions

This review reaffirms the pivotal role of artificial intelligence (AI), machine learning, and data analytics in shaping resilient, efficient, and secure digital infrastructures. The synthesis of ten peer-reviewed studies across cybersecurity, e-commerce, and supply chain domains directly addresses the four research questions and underscores the value of interdisciplinary, data-driven strategies.

Figure1 illustrates how machine learning genetic algorithms (GA) contribute to fraud detection and innovation, both internally (P1) and externally (P2), which in turn strengthens cybersecurity within organizations (P3, P4). This aligns with the broader findings that machine learning and AI-based approaches enhance organizational outcomes by improving innovation capacity, operational efficiency, and security through techniques like anomaly detection and real-time threat mitigation. At the same time, these technologies foster external value by building consumer trust, supporting engagement, and reinforcing resilience across e-commerce and supply chain networks. Together, the framework emphasizes that intelligent systems and collaborative algorithms not only reduce fraud exposure but also create adaptive cybersecurity structures that sustain digital trust.

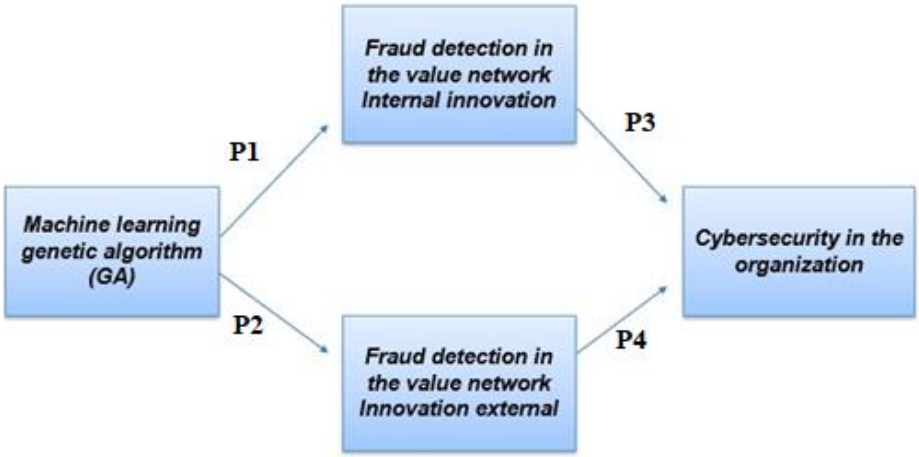

Figure1. Illustration of findings.

In response to Research Question 1—on the impact of Genetic Algorithms (GA) for feature selection in fraud detection—findings from Ileberi et al. (2022) confirm that GA significantly improves the precision and efficiency of machine learning classifiers by isolating the most predictive features in transactional datasets. This enhancement in fraud detection accuracy supports the argument for GA's strategic integration in financial cybersecurity systems. Regarding Research Question 2, which investigates the effect of machine learning applications on external cybersecurity mechanisms, Sarker et al. (2020) demonstrate that data science techniques such as clustering and anomaly detection bolster threat identification and real-time response capabilities. These applications are instrumental in reinforcing organizational security posture and adapting to dynamic threat landscapes.

Addressing Research Question 3, Zhang et al. (2023) provide compelling evidence that collaborative training-based algorithms are effective in detecting fraudulent reviewers on e-commerce platforms. Their algorithm outperforms traditional models by leveraging behavioral relationships among users, directly contributing to improved digital trust and fraud mitigation in consumer networks. For Research Question 4, Chaudhary et al. (2022) demonstrate that structured cybersecurity awareness programs, when evaluated using standardized metrics, result in measurable improvements in employee knowledge and behavior. These behavioral changes have a cascading impact on the security culture within e-commerce supply chains, underscoring the importance of human-centered approaches in enhancing cyber resilience.

In summary, this study demonstrates that intelligent systems, when guided by rigorous feature selection, real-time analytics, and collaborative frameworks, provide substantial benefits across operational, financial, and security domains. Future research should continue to explore scalable applications of these technologies, integrate ethical and interpretability considerations, and foster public-private partnerships to navigate the complex realities of digital transformation.

Future Research

Future research should further explore the integration of machine learning algorithms with real-time fraud detection systems, particularly focusing on dynamic environments where data evolves rapidly and adversarial threats adapt over time. Expanding studies on the use of Genetic Algorithms in large-scale, real-world financial systems would provide deeper insights into model scalability and generalizability. In the context of e-commerce, future investigations could examine the impact of digital cost structures across different geographical markets and assess how automation technologies affect long-term profitability.

Additionally, research on the Internet of Things (IoT) in retail should focus on consumer privacy, data ethics, and the accuracy of behavioral predictions. In cybersecurity, future studies must address the interpretability of AI models, explore methods to counter adversarial attacks, and develop standardized frameworks for evaluating cybersecurity awareness programs. Lastly, a multidisciplinary approach that includes government policy analysis, technological innovation, and organizational behavior will be crucial in developing resilient, transparent, and secure digital ecosystems.

References

Abkenar, S. P., Vanani, I. R., & Sohrabi, B. (2022). Social Commerce Mobile Application Enhancement: a hybrid text clustering - topic modeling business model analysis. *Electronic Commerce Research*, 1-40.

Ajayi, S., Correia Loureiro, S. M., & Langaro, D. (2023). Internet of things and consumer engagement on retail: *state-of-t*, 18(3), 397-423.

Argilés-Bosch, J. M., Blandón, J. G., & Ravenda, D. (2023). Cost behavior in e-commerce firms. *Electronic Commerce Research,* 23, 2101-2134.

Ates, M. A., Suurmond, R., Luzzini, D., & Krause, D. (2020). Order from chaos: A meta-analysis of supply chain complexity and firm performance. *Journal of Supply Chain Management*, 3-30.

Chaudhary, S., Gkioulos, V. y Katsikas, S. (2022). Desarrollar métricas para evaluar la eficacia del programa de concientización sobre ciberseguridad. *Revista de ciberseguridad*, 1-19.

Fries, M., & Kassemeier, R. (2024). Price Increases and Their Financial Consequences in International Business-to Business Selling. *Journal of International Marketing*, 32(1), 92-111.

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, 9(24), 1-17.

Luo, S., & Choi, T. M. (2020). E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Production and Operations Management Society*, 31(5), 2107-2126.

Sarker, I. H., M. Kayes, A. S., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data, 7(41), 1-29.*

Zhang, Q., Liang, Z., Ji, S., Xing, B. and Chiu, D. K. (2023). Detección de revisores falsos en redes heterogéneas de compradores y vendedores: un algoritmo colaborativo de grupo de spammers basado en capacitación. *Ciberseguridad,* 6(26), 1-24.