International Journal of Innovative Research and Scientific Studies, 8(7) 2025, pages: 896-907

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Security in cloud-based E-commerce: Review with a literature landscape analysis of emerging challenges and solutions

Yin Lei Yee Myint[1], Rajermani Thinakaran[2*], Hushalictmy Paliyanny[3], Kaung Khant Yan Naing[4], J. Somasekar[5]

[1]*Faculty of Business and Communication, INTI International University, Nilai, Malaysia.*
[2]*Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia.*
[3]*Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia.*
[4]*Department of Electronic Engineering, Yangon Technological University, Yangon, Myanmar.*
[5]*Department of Computer Science and Engineering, Jain (Deemed–to-be University), Bangalore, Karnataka, India.*

Corresponding author: Rajermani Thinakaran (*Email: rajermani.thina@newinti.edu.my*)

Abstract

This study systematically reviews security challenges and emerging solutions for cloud-based e-commerce platforms, providing a comprehensive analysis of recent literature. Using Scopus as the primary database, 19 articles published between 2020 and 2025 were selected through predefined criteria. PRISMA was used for a systematic literature review and bibliometric analysis, with VOSviewer mapping research trends and keyword co-occurrences. The review identifies key security challenges, including misconfigurations, insecure APIs, credential theft, insider threats, and supply chain vulnerabilities. In response, emerging solutions such as blockchain technology, AI-driven threat detection, zero-trust architectures, and fog computing frameworks show significant potential for mitigating these risks. Results also indicate a growing academic interest in cloud security for e-commerce over the study period. The findings offer actionable insights for researchers, practitioners, and policymakers to strengthen cloud security practices. The study proposes a Data-Adaptive Threat Intelligence (DATI) Framework as a practical approach for organizations to implement robust security, recommending future empirical validation in diverse e-commerce settings.

Keywords: Cloud computing, E-commerce, Process innovation, Security, Security.

DOI: 10.53894/ijirss.v8i7.11042
Funding: This study received no specific financial support.
History: Received: 22 August 2025 / **Revised:** 23 September 2025 / **Accepted:** 26 September 2025 / **Published:** 6 October 2025
Copyright: © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Cloud technology brings fundamental changes to modern e-commerce operations because it improves business management and cost reduction and delivers optimal customer experiences [1, 2]. The cloud system enables e-commerce solutions to handle massive transactional information while providing real-time services along with flexible resource allocation based on market requirements [3]. Businesses currently handle customer data and operational processes through cloud-based online retail operations, which face increasing security challenges that endanger their assets [4]. Cloud systems operate in diverse distributed networks that introduce security dangers through improper setups, as well as faulty APIs (Application Programming Interfaces) and insecure authorization methods [5]. The threat actors adapt their tactics in response to evolving cybercriminal tactics, which use various cloud infrastructure entry points to covertly attack systems while demanding ransom payments for the data [6]. Security in cloud-based e-commerce has become an absolute business priority because organizations need to defend their systems and keep customer trust strong [7].

The security problems affecting cloud-based e-commerce systems originate from different types of cloud infrastructure combinations, such as public cloud, private cloud, hybrid cloud, and multi-cloud [8]. These cloud computing architectures contain particular security threats that businesses must address using proper protective measures [9]. The distribution of operations caused by edge computing, together with containerized applications, presents challenges to traditional security measures for modern threats [10]. The adoption of non-human identities (NHIs) in cloud environments increases steadily as their total number surpasses that of human users [11]. The NHIs serve as common targets for unauthorized intruders who try to reach sensitive resources [12] thus requiring enhanced IAM (Identity and Access Management) solutions.

As the entire industry relies on third-party integrations and APIs for payment processing, inventory management, and customer relationship management, e-commerce platforms are highly prone to cyberattacks [13]. Supply chain attacks on these integrations have become more common, leading to cascading risks across interconnected systems [14]. Misconfigured systems have been a leading cause of breaches in cloud environments, supplying an attack vector to gain access to critical infrastructure [15]. Credential theft continues to be a common danger in e-business frameworks due to phishing efforts, malware attacks, poor secret key behavior, and social engineering attacks [16]. When IAM practices are insufficient, threat vectors such as insider threats and misuse of privileges multiply, increasing the organization's exposure surface [17].

Innovative technologies are changing how e-commerce platforms secure their cloud environments to combat these challenges. The Zero Trust Security Model has been adopted as the de facto way to continuously verify users and devices before granting access to resources [18]. Zero Trust inhibits the lateral movement of attackers across cloud networks by employing micro-segmentation techniques and the principle of least privilege [19]. Zero Trust models include such passwordless authorization methods, which use biometric or cryptographic keys, to remove the weaknesses tied to traditional passwords [20].

Moreover, AI-powered threat detection systems are bolstering real-time surveillance systems by scrutinizing large datasets for irregularities that may suggest possible breaches [21]. Technologies, such as blockchain or confidential computing, are also revolutionizing security practices in cloud-based e-commerce [22]. Blockchain ensures that transactions and inter-cloud data exchanges through a decentralized ledger enable a tamper-proof record for access, allowing improved transparency and data integrity in supply chains [23]. These developments solve fundamental pain points like data loss and leakage, and data privacy violations.

This systematic review specifically concentrates on security difficulties concerned with the protection of cloud e-commerce platforms, focusing on new trends and innovative techniques to enhance the protection of data and the resiliency of operational infrastructure. Specifically, this study seeks to: (i) illustrate the trends and connections in research on security in cloud-based e-commerce, by delivering a comprehensive landscape analysis of the scientific literature; (ii) examine the dominant security implications of cloud-based e-commerce environments; and (iii) identify emerging solutions to overcome the security implications of cloud-based e-commerce environments; and (iv) propose a framework on directions for future research to focus on ensuring the security of cloud computing in the context of e-commerce. Furthermore, synthesizing the available literature on the subject matter, this study aims to provide insights for researchers, practitioners, and policymakers looking to promote better cloud security practices in the fast-moving e-commerce environment.

The paper is organized as follows. Section 2 provides the methodology employed in the systematic review. Section 3 discusses the results and analysis of the literature review landscape. Section 4 provides a discussion of the findings by proposing a framework, and Section 5 notes limitations and avenues for future inquiry. Finally, the concluding section synthesizes the overall contributions and emphasizes the study's relevance to researchers and practitioners seeking to harmonize security and cloud computing in the e-commerce industry.

2. Methods

This study investigates the emerging security challenges and solutions in cloud computing spanning 2020 to 2025 through a systematic literature review (SLR). The systematic review offers a combined analysis of current security challenges and solutions over time [24-26]. This methodology is especially suitable for the research since it enables the collection and evaluation of extensive datasets, facilitating the overview of the literature related to security concerns and solutions in cloud computing [27].

The SLR protocol is adopted to analyze how e-commerce platforms secure data in their cloud. The research adheres to accepted protocols for conducting SLRs in technology and information systems research [28, 29] and follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework for transparent reporting [30]. It forms a comprehensive and substantive overview for policymakers and future scholars. According to the purpose of this review, the following research questions (RQs) were identified:

RQ1 - What does the literature landscape reveal about the trends and connections in research on security in cloud-based e-commerce?

RQ2 - What are the primary security challenges of cloud-based e-commerce environments? and

RQ3 - What emerging solutions and technologies are being adopted to enhance cloud security in e-commerce?

2.1. Data Collection

SCOPUS was used as the main source of data because its database contains a huge number of papers and citations [31, 32]. SCOPUS is the best choice for this large-scale and general bibliometric study. The study mostly looked at papers that had "security," "cloud computing," and "e-commerce" in the title, keywords, or abstracts. The data set accurately showed how these two important groups came together by focusing on keywords. The analysis only looked at stories from 2020 to 2025. The data was first collected in March 2025 using the search term "security" AND "cloud computing" AND "e-commerce", and articles were selected from 254 journal publications and conference proceedings pertinent to the study's topic. This time frame was picked to give a modern look at the subject, considering the most recent developments and debates.

2.2. Study Selection and Eligibility Criteria

The papers are selected from the most relevant sources in conference proceedings and journal articles. However, books, chapters, dissertations, and reports have been excluded so that the results in each database are readable and can be filtered in a short time. Moreover, the eligibility criteria were independently applied to all reports as a way of minimizing the risk of selection bias, as described in Table 1. Finally, a total of 19 articles were included in the final review of this study. Each of the selected articles was then read in detail to extract the relevant data to answer the research questions. The synthesized findings were then the answer to each research question. The PRISMA flow diagram for the systematic review and results is shown in Figure 1.

Table 1.
Inclusion and Exclusion Criteria for Literature Review.

Inclusion Criteria	Exclusion Criteria
Articles must be written in English.	Articles are written in other languages.
Articles published from 2020 to 2024.	Articles were published before 2020 and after 2024.
Articles published in conferences and journals.	Articles are published on news websites, magazines, and other unreliable sources.
Articles focus on the e-commerce industry.	Articles focus on FMCG, Healthcare, Tourism, and other industries.
Articles dedicated to challenges and solutions related to the security of cloud-based e-commerce.	Articles dedicated to consumer behavior, customer trust, digital marketing, and platform features of e-commerce.

The data was downloaded in CSV format from Scopus and imported into a master Excel file. The Excel file was utilized to create a descriptive analysis to record the cloud security concerns and emerging solutions in the context of e-commerce. Data from the Excel file were imported into VOSviewer to perform a bibliometric analysis. The VOSviewer software's bibliometric method, "keyword co-occurrence analysis," was employed to show the keywords with the highest co-occurrence and their related themes, which can help determine the direction of future study.

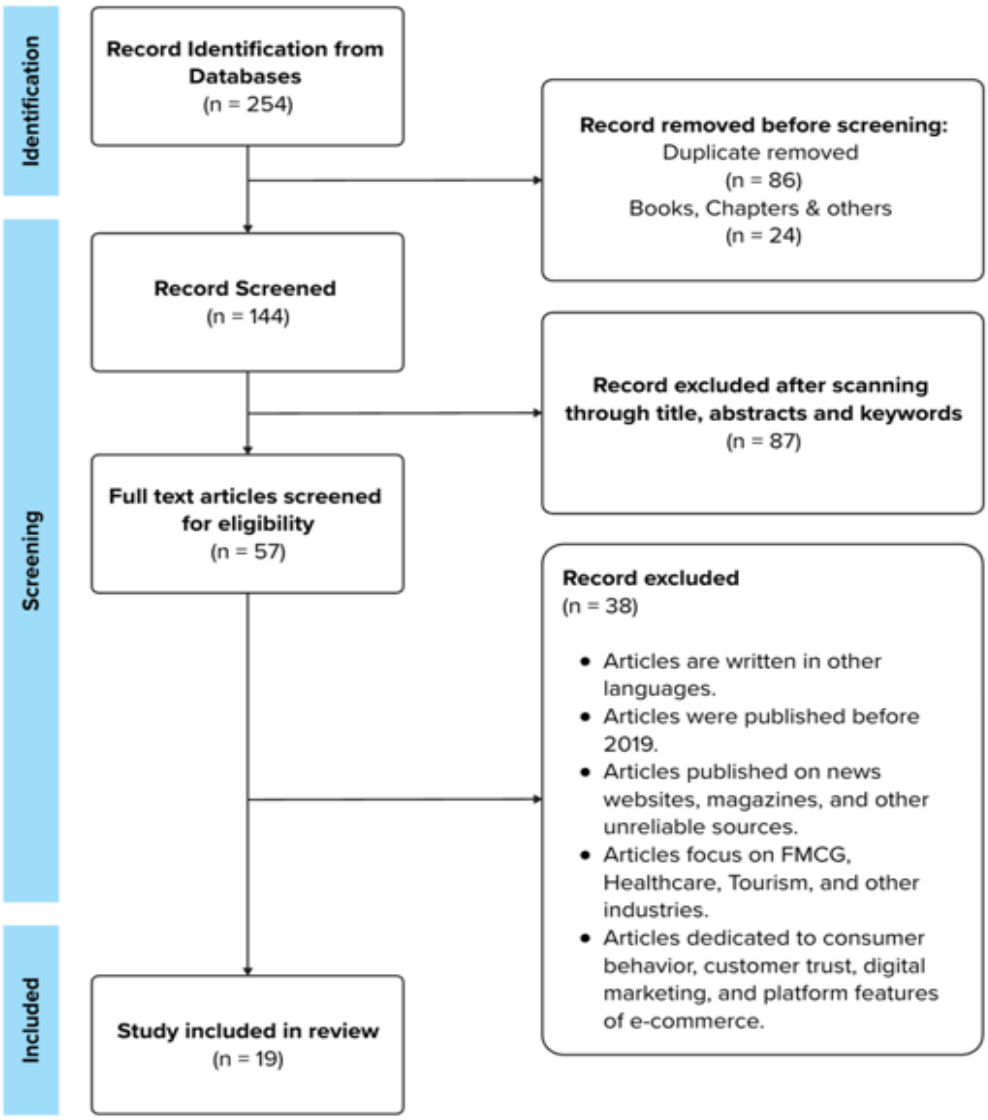

Figure 1.
PRISMA Flow Diagram for SLR.

3. Results

The purpose of this systematic review was to record and summarize emerging challenges and solutions related to the security of cloud-based e-commerce. The review looked at 19 Scopus-indexed publications from the last five years using scientific mapping to answer the first research question, RQ1. Table 2 provides a summary illustration of the eligible research based on two main components: security challenges and solutions, with the type of publication.

Table 2.
Summary of Eligible Studies From SLR.

Type of Publication	Research	Security	
		Challenges	Solutions
Conference Paper	Megerdichian, et al. [33]	Yes	Yes
	Mohamad, et al. [34]	No	Yes
Journal Article	Hongmei [35]	No	Yes
	Vinoth, et al. [36]	Yes	No
	Wang [37]	Yes	No
	Alfadli [38]	Yes	Yes
	Walia, et al. [39]	Yes	Yes
	Wang and Li [40]	No	Yes
	Zeng, et al. [41]	Yes	No
	Alfadli [42]	Yes	Yes
	Al-Moghrabi and Al-Ghonmein [43]	No	Yes
	Arif, et al. [44]	Yes	Yes
	Hou and Zhou [45]	Yes	Yes
	Ludbe, et al. [46]	No	Yes
	Mutemi and Bacao [47]	Yes	No
	Savithi and Suttidee [48]	Yes	Yes
	Shili and Anwar [49]	Yes	Yes
	Xin and Radzi [50]	No	Yes
	Yanyan and Althabhawi [51]	Yes	No

The review identified a small collection of 19 Scopus-indexed documents related to the security of cloud-based e-commerce published between 2020 and 2025. The information provided in this review, as seen in the development rate, indicates that a growing number of researchers are becoming interested in the security of cloud-based e-commerce. Figure 2 reveals a fluctuating, yet growing over time, suggesting increased interest in the literature in this area.

In 2020, there were no published papers, indicating that cloud security in e-commerce appears to have been overlooked during the early years of the timeline. However, there was a 5-fold increase in 2021 compared to an average of one article per year before that. This spike probably represents the growing use of cloud computing technologies in e-commerce and the need to address new security challenges, such as data breaches and fraud prevention.

In 2022, the publication rate slightly decreased compared to the previous year, with 4 articles, suggesting a stabilization of the research output. It indicates a period that was more of a phase of cementing top-level studies and ensuring technology-based security solutions, such as the integration of blockchain technology and AI-driven threat detection systems etc.

A significant drop is observed in 2023, with only one article published. This decline may be due to changes in research priorities or limitations of resources in the field. Despite this decline, research activity surged to its highest level during the study period in 2024, with nine articles published. This sharp increase highlights renewed interest and urgency in addressing security checks originating from advanced cyber threats and the ongoing rapid prospects for cloud-based e-commerce platforms.

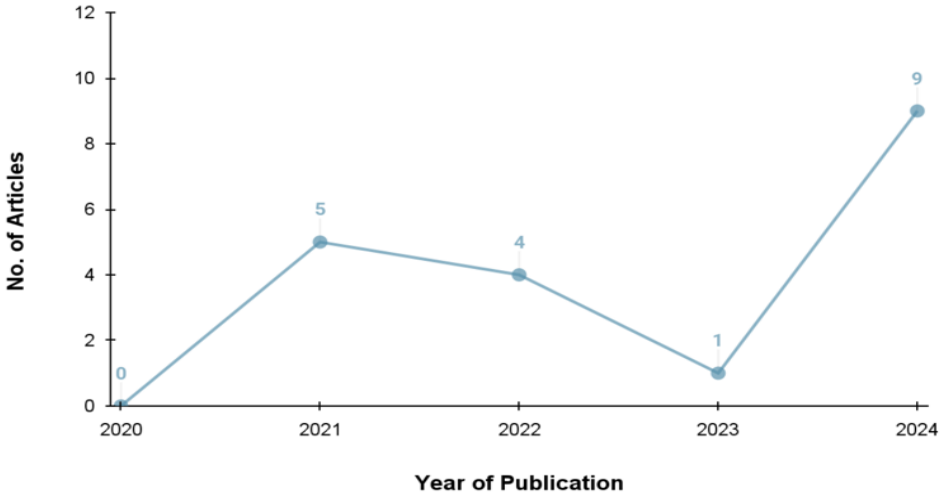

Figure 2.
Development Rate of the Literature on Cloud Security in E-Commerce.

Figure 3 illustrates the distribution of total citations across various publication sources in the domain of cloud security in e-commerce, highlighting the prominence and influence of specific platforms in shaping the research landscape. Among the sources, Science Direct is the most cited source with 102 mentioned sources. This dominance is an indication of Science Direct being a premier platform for accessing high-impact research articles and successfully attracting studies that explore ongoing and emerging issues in cloud security.

Second is WILEY with 40 citations, indicating its overall input towards knowledge generation for the field. WILEY's publications seek interdisciplinary approaches demonstrating either technical solutions, such as blockchain and AI-based threat detection, or practical applications within e-commerce operations. With a focus on engineering and technology-driven solutions like fog computing frameworks and machine learning algorithms for fraud detection, IEEE Explore occupied the third position with 25 citations.

Other contribution sources include SCIENCE Publications with 3 citations, Springer, Research Gate, and RGSA with 1 citation each.

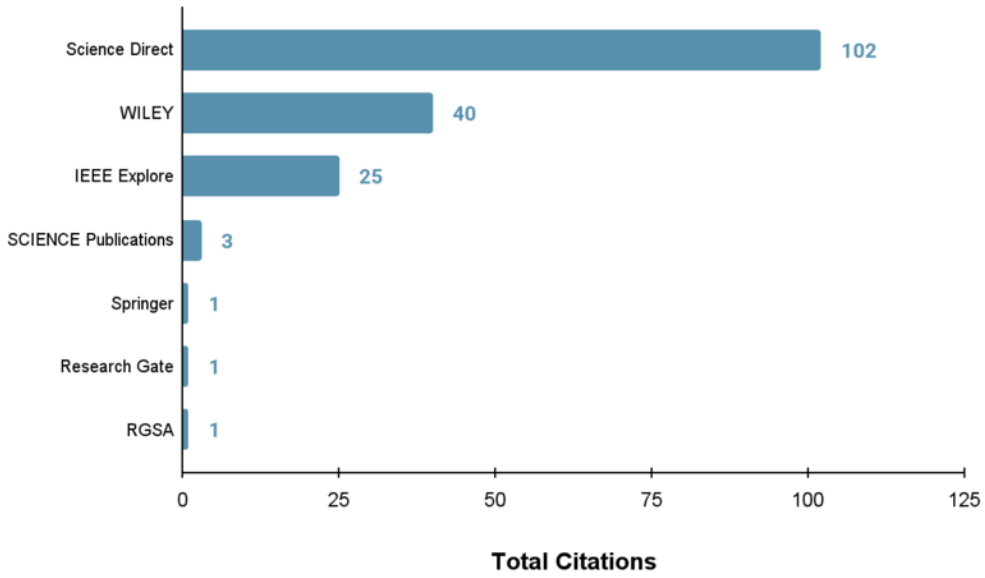

Figure 3.
Sources by Total Citations.

Figure 4, the visualization of the co-occurring keyword network generated by VOSviewer, presents a profuse network for the cloud technology-based e-commerce security domain, with the major co-occurring keywords being "electronic commerce", "cloud computing", and "e-commerce". Such keywords correlate with network security, data security, risk assessment, and much more, recommending the need to secure sensitive data at the core of cloud-based e-commerce operations. Access control and effective solutions are there, demonstrating the attention to governance and technology, and the focus on laying down how to control vulnerabilities.

Specifically, unique clusters form around blockchain and big data, as these are becoming increasingly important in the context of solving the problems faced by e-commerce. Blockchain, associated with transparency, trust, and NFTs (Non-

Fungible Tokens), highlights the capability of blockchain to improve the integrity of transactions, enable decentralized businesses, and inspire new applications.

Along these lines, the cluster around big data and network security mirrors, to a certain extent, the convergence of AI-enabled analytics, such as BP neural networks and data mining methods, for real-time threat identification and predictive modeling. The latter classification envelopes smaller clusters like fog computing and agent-based models, indicating recently developed frameworks aiming at solving some of these challenges related to scalability, operational efficiency, and secure decision-making in environments with defined distribution characteristics.

This analysis highlights the interrelationship of research topics in this area of cloud-based e-commerce security with a high concentration on the dual use of state-of-the-art technologies to combat ever-changing threats, ensuring transparency, efficiency, and trustworthiness, and providing motivation for further research.

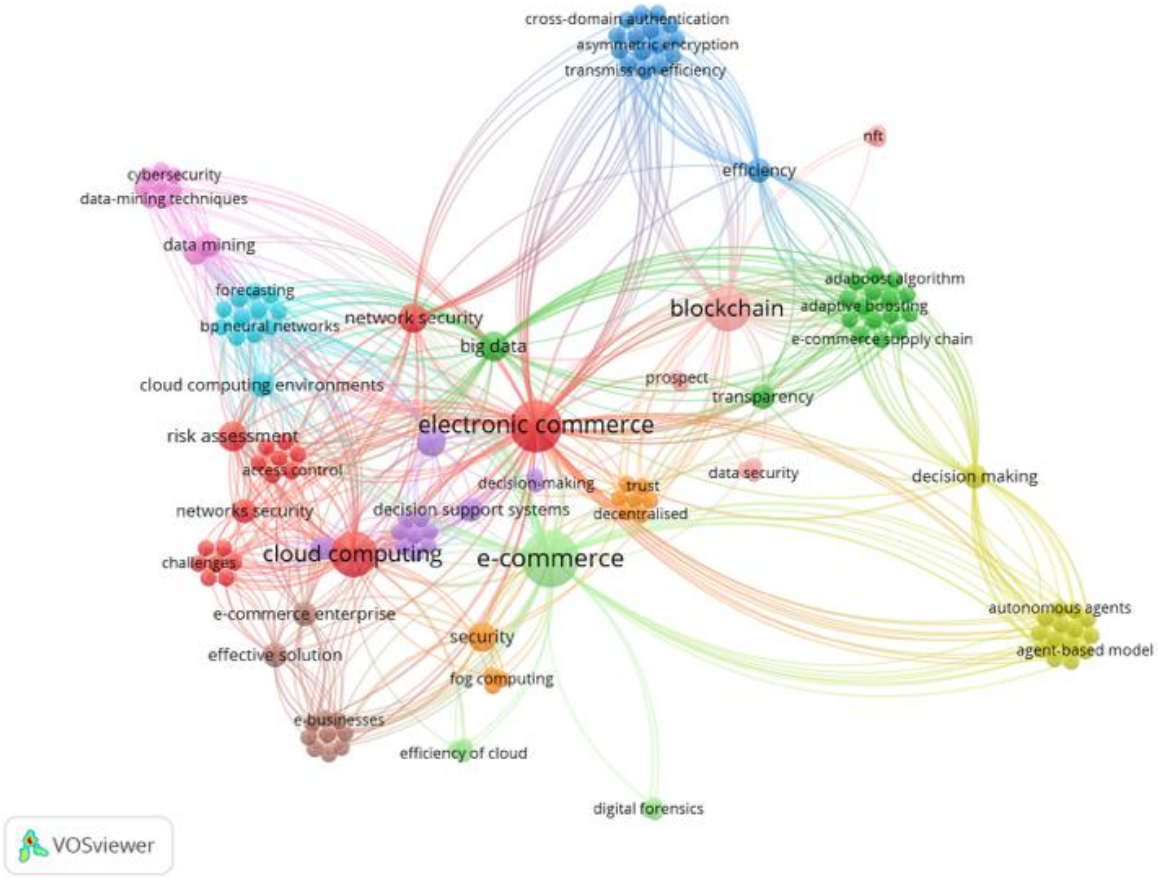

Figure 4.
Co-occurrence of Keywords Network Visualization.

4. Discussion

The session examines security challenges and approaches that resolve security concerns in cloud-based e-commerce to answer the two remaining research questions, RQ2 and RQ3. The discussion introduces the DATI (Data-Adaptive Threat Intelligence) Framework as the last component. The session utilizes earlier findings on the research questions to construct a comprehensive knowledge framework that explains e-commerce system operations between cloud computing and security compliance to enhance customer experience.

4.1. Primary Security Challenges in Cloud-based E-commerce

Security threats are diverse, and cloud-based e-commerce platforms significant risk to protecting sensitive information of the customers, such as payment data, personal details, and transaction records. Among the biggest challenges are fraud and cyberattack risks. Mutemi and Bacao [47] also state that the level is getting complex with instances of e-commerce fraud, including phishing, identity theft, and credit card fraud, and cloud-based systems are vulnerable to these high-level frauds. These attacks are fueled by poor authentication and insufficient monitoring systems.

Another major concern is misconfigurations in cloud environments, which continue to be a primary cause of data breaches. Inappropriate access controls and insecure storage configurations allow for sensitive data to be exposed to unauthorized access [36]. This is due to the decentralized nature of cloud environments, which increases the chances of encountering misconfiguration and therefore emphasizes the need for adopting robust governance frameworks [41].

Third-party integrations and APIs (Application Programming Interfaces) are prone to vulnerabilities. If not properly secured, APIs used for payment processing, inventory management, or customer relationship management can be entry points for attackers [41]. Cross-border e-commerce operations' serious security vulnerabilities are intractable problems; no

country can solve the problem of security. Particularly, the regulatory system is inconsistent, and people will have a greater impact in the new situation [35].

Cloud apps like e-commerce platforms also face some high risks, such as insider threats and the misuse of privileges. According to the study [38] poor Identity and Access Management (IAM) practices provide opportunities for employees or contractors to misuse their privileges either knowingly or unknowingly, causing data breaches or disruptions to systems.

The quick uptake rate of mobile payment systems has also opened new attack vectors. Mobile payment systems in cloud environments are prone to attacks, including but not limited to capital loss and privacy violation, owing to unsafe network connections and incomplete encryption protocols [37].

Lastly, e-commerce platforms face distinctive challenges when it comes to cross-border transactions. As stated by Hongmei [35] traditional centralized models have problems such as inconsistent credit rating, lack of traceability of logistics, vulnerabilities in payment, and so on. These challenges are compounded by cross-country differences as a result of different regulatory compliance requirements between countries.

4.2. Emerging Solutions and Technologies for Cloud Security in E-Commerce

To address these security challenges, various technologies and solutions are available that are developed specifically for cloud-based e-commerce. The most widespread approach is the implementation of blockchain technology, which has been adopted by companies to improve e-commerce operations by making them more secure, traceable, and transparent. This approach also tackles the issue of the security of transactions on foreign networks and eliminates the need for mutual trust between systems [35]. Similarly, a secure migration of an e-commerce system can be built on the basis of blockchain, where the system design records all transactions and inter-cloud data exchanges, and these records are tamper-proof [44]. For instance, in supply chain logistics management, the blockchain facilitates real-time tracking of the goods, preserving the integrity of data [45].

Another key innovation is artificial intelligence (AI)-driven threat detection systems. For example, multidimensional time-series data can be used to establish BP neural networks and predict mobile payment risk [37]. These AI models provide the ability to proactively mitigate risks by spotting anomalies that indicate potential breaches before they become serious threats.

Zero Trust architectures have emerged as a powerful approach for securing cloud-based e-commerce environments. Zero Trust demands ongoing verification of users and devices before they can be granted access to resources [41]. Utilizing micro-segmentation techniques and the principle of least privilege, Zero Trust significantly reduces the potential for lateral movement by an attacker once inside a cloud network.

Fog-based cloud computing frameworks can be considered a hybrid paradigm that addresses latency issues and enhances security with edge-level detection. The study [39] presents a fog-enabled architecture to physically integrate edge nodes and a centralized cloud system for more efficient communication while still ensuring encryption at all tiers.

Passwordless authentication is an example of protection through unlinkable credentials, like biometrics or cryptographic keys. These techniques increase user convenience while dramatically lowering the risk of credential theft [42].

Apart from technical solutions, designing a website efficiency to clarify information has proven to be the most critical factor for customers to trust your business. Savithi and Suttidee [48] state that efficient cloud computing practice with reliable information presentation improves customer confidence in e-commerce platforms.

Lastly, utilizing agent-based modeling and integration of IoT is proposed as a method for improving the operational efficiency of e-commerce platforms, along with addressing security issues. According to the study [49]. Internet of Things (IoT) units coupled with agent-based dissemination might enhance inventory management processes by guaranteeing secure data transmission.

4.3. Proposing the Data-Adaptive Threat Intelligence (DATI) Framework

The DATI Framework establishes an approach that handles cloud-based e-commerce security needs through innovative methods to defend data, as well as capture threat information and oversee identities, and streamline compliance tasks. The framework implements a layered method to deliver a thorough defense over vital e-commerce operational aspects. The study describes the four DATI Framework frameworks, enabling better security practices while reducing vulnerabilities at each stage.

The Data Integrity and Privacy Layer commences the architecture by shielding sensitive transactions and personal information with blockchain security and confidential computing, and dynamic data masking protection. Through the implementation of these integrated technologies, this layer provides an effective solution to the current data breach threats and the need to follow GDPR and PCI-DSS regulations, as well as repairing consumer trust in privacy protection.

The Adaptive Threat Defense Layer safeguards organizations by implementing AI threat detection and neural networks combined with machine learning, along with zero-trust micro-segmentation to isolate threats and automated self-healing systems for vulnerability auto-patching. The Adaptive Threat Defense Layer addresses multiple threats like phishing attacks, malware infection, and supply chain threats alongside insider threats, which require pre-emptive defense and solutions to be deployed at this stage of the stack.

Identity and Access Governance Layer guarantees protected authentication and authorization functionalities through decentralized identity management and behavioral biometrics detection of compromised accounts and Role-Based Access Control (RBAC) with adaptive authentication. The third model layer creates a security system against credential theft, combined with privileged escalation protection and internal threat defense, which achieves easier user operations.

The Compliance and Audit Automation Layer is employed to achieve convenient regulatory compliance management and automate report generation for accountability purposes. The system executes settlements through regulation-adherent smart contracts and relies on blockchain for permanent data logging alongside artificial intelligence that provides instant risk evaluation. The solution addresses three key problems arising from enterprises' improper use of customer data in cross-border e-commerce: regulatory violations, inefficient audits, and associated legal risks.

This DATI Framework fills crucial gaps in existing frameworks. It combines high-tech components such as blockchain, AI-driven analytics, zero-trust architectures, and automated compliance into its system, specifically designed for e-commerce security needs.

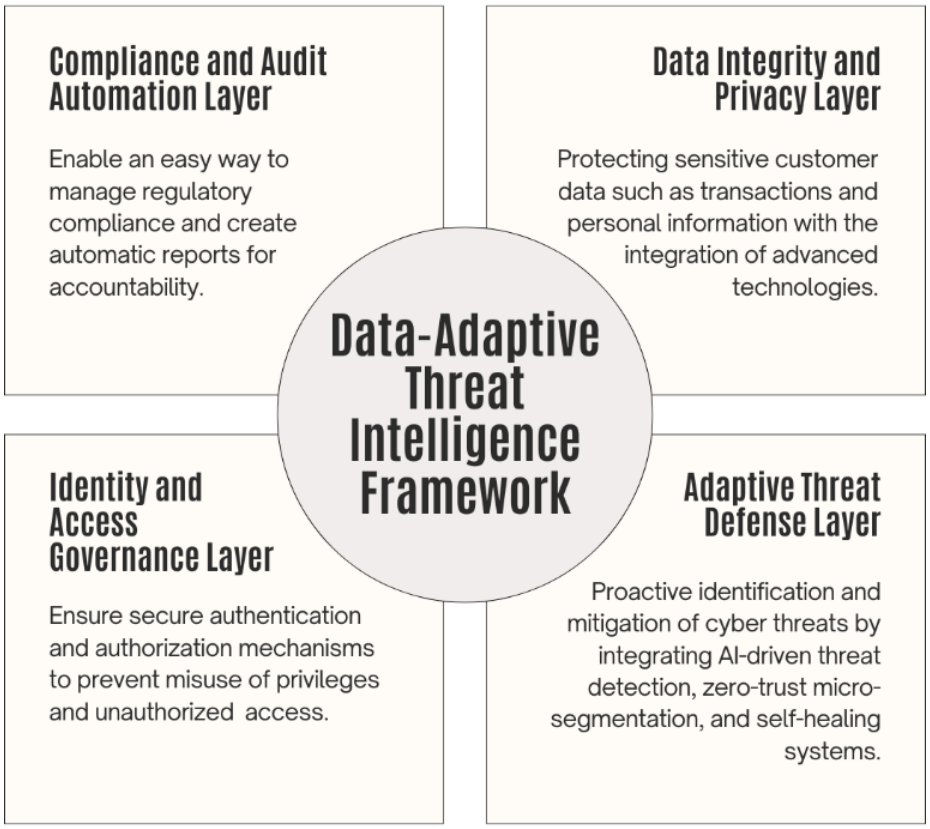

Figure 5.
Proposed Framework of Data-Adaptive Threat Intelligence (DATI).

5. Limitations and Future Study Recommendations

The limitations of the review and recommendations for future studies were emphasized in this section.

5.1. Limitations of the Review

This study provides valuable insights into the security issues and solutions developed around cloud-based e-commerce, yet several limitations should be recognized. First, the study is based solely on Scopus-indexed publications, which, although extensive, might overlook pertinent articles listed in other databases or grey literature. Such a restriction can result in more limited insight into the research landscape. Second, the analysis is time-limited, 2020-2025 inclusive, so that it may miss out on foundational studies published before the cut-off date or frontier advances after the data collection period.

Third, one limitation of this study is its reliance on bibliometric analysis tools like VOSviewer, which may oversimplify complex relationships between research topics. While keyword co-occurrence analysis provides valuable insights into thematic clusters, it does not capture nuanced interdependencies between concepts such as AI-driven analytics and Zero Trust architectures. Finally, although this review integrates results from 19 articles, the limited number of articles analyzed may restrict the transferability of its implications in other contexts or sectors outside of e-commerce.

5.2. Recommendations for Future Studies

Future studies should overcome these limitations by broadening the range of data sources to incorporate other well-established databases, such as IEEE Xplore, Web of Science, and others, to present a more holistic perspective of the research landscape. Further longitudinal studies extending beyond 2025 may be beneficial to capture evolving trends and emerging technologies within the realm of cloud security for e-commerce. In particular, verifiable technology and accountable AI lend themselves well to in-depth case studies, such as blockchain or AI-powered threat detection systems. Such interdisciplinary approaches drawing from cybersecurity, business management, and legal compliance could provide

comprehensive solutions addressing issues of inconsistent regulations across jurisdictions. Additionally, research on regional security concerns for cloud-based e-commerce systems will offer insight into localized risks and compliance measures. Finally, future work could focus on developing and validating unified frameworks, such as the proposed DATI Framework, to evaluate their practical applicability and scalability in securing cloud-based e-commerce platforms.

6. Conclusion

This systematic review discussed cloud-based e-commerce security issues and new solutions while providing an extensive state-of-the-art literature review to develop a framework that improves cloud security. Insufficient security data reveals several issues, which consist of configuration errors combined with unprotected APIs, along with stolen credentials and unauthorized user actions endangering customer data and operational systems. The implementation of blockchain technology together with AI threat detection systems, zero-trust network approaches, and fog computing systems demonstrates methods to combat these security difficulties through advanced transparency and scalability and enhanced resilience. Cloud-based e-commerce security benefits from the DATI Framework, which unites these technological components into a unified security system. The research provides essential knowledge that helps experts and academics achieve security synchronization between e-commerce framework requirements and changing market demands. This review develops essential groundwork that future research will need to protect cloud-based e-commerce operations in a digital marketplace that continues to expand through connectivity.

References

[1] R. Gulia and V. Rastogi, "The role of cloud computing in scaling e-commerce businesses," *EPRA International Journal of Multidisciplinary Research*, pp. 248–256, 2024. https://doi.org/10.36713/epra19339

[2] A. A. S. Mohammad *et al.*, "Cloud computing adoption in the digital era: A bibliometric analysis and research agenda," *Artificial Intelligence, Sustainable Technologies, and Business Innovation: Opportunities and Challenges of Digital Transformation*, pp. 137-148, 2025. https://doi.org/10.1007/978-3-031-77925-1_13

[3] Y. Dong and Y. Zhang, "Implementation of distributed operation and maintenance of cross-border e-commerce platform based on cloud native architecture," *Security and Communication Networks*, vol. 2021, no. 1, p. 4254791, 2021. https://doi.org/10.1155/2021/4254791

[4] C. Pandugula and Z. Yasmeen, "Exploring advanced cybersecurity mechanisms for attack prevention in cloud-based retail ecosystems," *Journal for ReAttach Therapy and Developmental Diversities*, vol. 6, pp. 1704-1714, 2023. https://doi.org/10.53555/jrtdd.v6i10s(2).3420

[5] B. P. Manjappasetty Masagali and M. Nayak, "Empowering cloud-native security: The transformative role of artificial intelligence," *International Journal of Artificial Intelligence and Applications*, vol. 15, no. 6, pp. 1-11, 2024. https://doi.org/10.5121/ijaia.2024.15601

[6] O. M. Dopamu, "Cloud-based ransomware attack on US financial institutions: An in-depth analysis of tactics and counter measures," *International Journal of Science and Research*, vol. 13, no. 2, pp. 1872-81, 2024. https://doi.org/10.21275/sr24226020353

[7] S. Saeed, "A customer-centric view of E-commerce security and privacy," *Applied Sciences*, vol. 13, no. 2, p. 1020, 2023. https://doi.org/10.3390/app13021020

[8] N. O. Omoike, "Designing a secure and high-performing e-commerce platform for public cloud," *International Journal of Science and Research Archive*, vol. 9, no. 2, pp. 1008–1013, 2023. https://doi.org/10.30574/ijsra.2023.9.2.0525

[9] S. A. Ali, "Designing secure and robust e-commerce plaform for public cloud," *The Asian Bulletin of Big Data Management*, vol. 3, no. 1, pp. 164-189, 2023. https://doi.org/10.62019/abbdm.v3i1.56

[10] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE Access*, vol. 8, pp. 85714-85728, 2020. https://doi.org/10.1109/access.2020.2991734

[11] E. Van Der Walt and J. Eloff, "Using machine learning to detect fake identities: Bots vs humans," *IEEE Access*, vol. 6, pp. 6540-6549, 2018. https://doi.org/10.1109/access.2018.2796018

[12] K. Maidine and A. El-Yahyaoui, "Cloud identity management mechanisms and issues," in *2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, 2023, pp. 1-9.

[13] R. Gupta, "Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies," *Journal of Advanced Management Studies*, vol. 1, no. 3, pp. 1-10, 2024. https://doi.org/10.36676/jams.v1.i3.13

[14] T. Bandyopadhyay, V. Jacob, and S. Raghunathan, "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest," *Information Technology and Management*, vol. 11, no. 1, pp. 7-23, 2010. https://doi.org/10.1007/s10799-010-0066-1

[15] J. Guffey and Y. Li, "Cloud service misconfigurations: Emerging threats, enterprise data breaches and solutions," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 2023: IEEE, pp. 0806-0812.

[16] A. Rifai, A. Meliyani, P. Chyntia, and I. A. Sakti, "Penerapan metode technology threat avoidance theory terhadap tingkat kesadaran data privasi pengguna media sosial," *Journal of Information System Research*, vol. 4, no. 3, pp. 1026-1032, 2023. https://doi.org/10.47065/josh.v4i3.3081

[17] N. S. R. Mamidi, "Insider threat detection: Strengthening enterprise IAM (Identity and access management) landscape," *World Journal of Advanced Engineering Technology and Sciences*, vol. 13, no. 2, pp. 515–527, 2024. https://doi.org/10.30574/wjaets.2024.13.2.0633

[18] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," *Internet of Things*, vol. 27, p. 101227, 2024. https://doi.org/10.1016/j.iot.2024.101227

[19] N. N. Parvatha, "Securing multi-tenant cloud platforms during global crises: A zero trust approach," *International Journal of Science and Research Archive*, vol. 1, no. 1, pp. 123–132, 2020. https://doi.org/10.30574/ijsra.2020.1.1.0017

[20] J. Iggbom, "Zero-trust architecture is creating a passwordless society," *Network Security*, vol. 2022, no. 7, 2022. https://doi.org/10.12968/s1353-4858(22)70045-1

[21] S. Oduri, "AI-Powered threat detection in cloud environments," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 9, no. 12, pp. 57-62, 2021. https://doi.org/10.17762/ijritcc.v9i12.10999
[22] P. S. J. Ng, X. Zhang, L. Fu, L. Ye, and K. Y. Phan, "The inclusive innovation of blockchain in securities issuance: Reduced inequalities of investors," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 46, no. 2, pp. 188–212, 2024. https://doi.org/10.37934/araset.46.2.188212
[23] A. Park and H. Li, "The effect of blockchain technology on supply chain sustainability performances," *Sustainability*, vol. 13, no. 4, p. 1726, 2021. https://doi.org/10.3390/su13041726
[24] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333-339, 2019. https://doi.org/10.1016/j.jbusres.2019.07.039
[25] L. W. Yen, R. Thinakaran, and J. Somasekar, "Machine learning-based denoising techniques for monte carlo rendering: A literature review," *Machine Learning*, vol. 16, no. 2, 2025. https://doi.org/10.14569/IJACSA.2025.0160259
[26] N. H. Xin and R. Thinakaran, "Methods, improvement and challenges on cloth and hair animation," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 5, 2023.
[27] L.-L. Ebidor and I. G. Ikhide, "Literature review in scientific research: An overview," *East African Journal of Education Studies*, vol. 7, no. 2, pp. 179-186, 2024. https://doi.org/10.37284/eajes.7.2.1909
[28] W. Bandara and R. Syed, "The role of a protocol in a systematic literature review," *Journal of Decision Systems*, vol. 33, no. 4, pp. 583-600, 2024. https://doi.org/10.1080/12460125.2023.2217567
[29] R. I. Williams Jr, L. A. Clark, W. R. Clark, and D. M. Raffo, "Re-examining systematic literature review in management research: Additional benefits and execution protocols," *European management journal*, vol. 39, no. 4, pp. 521-533, 2021. https://doi.org/10.1016/j.emj.2020.09.007
[30] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *bmj*, vol. 372, 2021. https://doi.org/10.1136/bmj.n71
[31] J. F. Burnham, "Scopus database: a review," *Biomedical digital libraries*, vol. 3, no. 1, p. 1, 2006. https://doi.org/10.1186/1742-5581-3-1
[32] J. Baas, M. Schotten, A. Plume, G. Côté, and R. Karimi, "Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies," *Quantitative science studies*, vol. 1, no. 1, pp. 377-386, 2020. https://doi.org/10.1162/qss_a_00019
[33] N. Megerdichian, N. Abdolvand, and S. Rajaee Harandi, "The effect of blockchain on customer-to-customer electronic commerce," in *Proceedings of the International Conference on Electronic Business (ICEB '21)*, 2021.
[34] M. B. Mohamad *et al.*, "Enterprise problems and proposed solutions using the concept of E-Commerce," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 186-192). IEEE*, 2021.
[35] Z. Hongmei, "A cross-border e-commerce approach based on blockchain technology," *Mobile Information Systems*, vol. 2021, no. 1, p. 2006082, 2021. https://doi.org/10.1155/2021/2006082
[36] S. Vinoth, H. L. Vemula, B. Haralayya, P. Mamgain, M. F. Hasan, and M. Naved, "Application of cloud computing in banking and e-commerce and related security threats," *Materials Today: Proceedings*, vol. 51, pp. 2172-2175, 2022. https://doi.org/10.1016/j.matpr.2021.11.121
[37] H. Wang, "BP neural network-based mobile payment risk prediction in cloud computing environment and its impact on e-commerce operation," *International Journal of System Assurance Engineering and Management*, vol. 13, no. Suppl 3, pp. 1072-1080, 2022. https://doi.org/10.1007/s13198-021-01393-4
[38] I. Alfadli, "Integrated e-commerce security model for websites," *International Journal of Advanced and Applied Sciences*, vol. 9, no. 4, pp. 106–113, 2022. https://doi.org/10.21833/ijaas.2022.04.013
[39] S. Walia, R. Rajak, and M. Sajid, "E-commerce with fog-enabled cloud computing: Framework, opportunities, and challenges," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 13, pp. 4941–4954, 2022.
[40] D. Wang and G. Li, "The best decision for e-commerce funds transfer based on cloud computing technique," *Mathematical Problems in Engineering*, vol. 2022, no. 1, p. 9432413, 2022. https://doi.org/10.1155/2022/9432413
[41] Y. Zeng, S. Ouyang, T. Zhu, and C. Li, "E-commerce network security based on big data in cloud computing environment," *Mobile Information Systems*, vol. 2022, no. 1, p. 9935244, 2022. https://doi.org/10.1155/2022/9935244
[42] I. Alfadli, "Cloud computing model for e-commerce in Saudi Arabia," *Journal of Computer Science*, vol. 19, no. 4, pp. 446-453, 2023. https://doi.org/10.3844/jcssp.2023.446.453
[43] K. G. Al-Moghrabi and A. M. Al-Ghonmein, "Harnessing the power of blockchain technology to support decision-making in e-commerce processes," *International Journal of Artificial Intelligence*, vol. 2252, no. 8938, p. 1381, 2024. https://doi.org/10.11591/ijai.v13.i2.pp1380-1387
[44] Z. Arif, N. Zulfitria, O. N. Bariyah, N. Sopa, A. Supyadillah, and D. F. Darmansyah, "Blockchain as a facilitator for secure migration: A case study of e-commerce in Indonesia," *Revista de Gestão Social e Ambiental*, vol. 18, no. 2, p. e06342, 2024. https://doi.org/10.24857/rgsa.v18n2-164
[45] D. Hou and M. Zhou, "Blockchain-based e-commerce supply chain logistics management model innovation in the context of big data analysis," *Applied Mathematics and Nonlinear Sciences*, vol. 9, no. 1, 2024. https://doi.org/10.2478/amns-2024-0729
[46] A. Ludbe, S. Pandharipande, H. Imtiyaz, and K. Wasnik, "Blockchain-based e-commerce warranty system using NFTs," *International Journal of Creative Research Thoughts*, vol. 12, no. 6, pp. b822–b827, 2024.
[47] A. Mutemi and F. Bacao, "E-commerce fraud detection based on machine learning techniques: Systematic literature review," *Big Data Mining and Analytics*, vol. 7, no. 2, pp. 419-444, 2024. https://doi.org/10.26599/BDMA.2023.9020023
[48] C. Savithi and A. Suttidee, "The impact of information reliability and cloud computing efficiency on website design and E-commerce business in Thailand," *Journal of Computer Science*, vol. 20, no. 2, p. 198, 2024. https://doi.org/10.3844/jcssp.2024.198.206
[49] M. Shili and S. Anwar, "Leveraging agent-based modeling and IoT for enhanced e-commerce strategies," *Information*, vol. 15, no. 11, p. 680, 2024. https://doi.org/10.3390/info15110680
[50] F. M. Xin and M. S. N. M. Radzi, "Application and prospect analysis of blockchain technology in intellectual property protection of e-commerce," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 10, p. Article 7113, 2024. https://doi.org/10.24294/jipd.v8i10.7113

[51] C. Yanyan and N. M. Althabhawi, "China's online dispute resolution Mechanism for Cross-Border e-commerce: challenges and solutions," *Pakistan Journal of Life & Social Sciences*, vol. 22, no. 2, 2024. https://doi.org/10.57239/pjlss-2024-22.2.00408