IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 10, Issue 4, 2022

Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments

Rajeswaran Ayyadurai

Login Net services, Vadavalli Coimbatore, India.

Email ID: dinesh.basani06@gmail.com

Abstract

The swift expansion of electronic commerce has transformed commercial dealings, providing unmatched ease and availability to clients throughout the globe. But this growth has also raised serious questions about transaction security, especially when it comes to protecting private information like credit card numbers and personal information. In order to tackle these obstacles, this study conducts a thorough examination of e-commerce transaction security, with a particular emphasis on the application of big data analysis in cloud environments. Businesses can efficiently handle and analyze enormous volumes of transactional data in real-time, allowing for the detection and mitigation of possible security concerns, by utilizing the scalability and processing capacity of cloud computing. Big data analysis combined with cloud computing has many benefits, such as flexibility in handling different amounts of data, fast distributed processing for quick analysis, and the ability to use sophisticated analytics methods like machine learning for anomaly detection and predictive modeling. In addition, the utilization of cloud based computing and storage resources facilitates the establishment of strong data encryption and access control procedures, guaranteeing the security and integrity of vital transaction data. In order to identify important themes, patterns, and insights regarding the application of big data analysis in cloud environments for improving transaction security in e-commerce platforms, this study synthesizes pertinent literature through a systematic review of academic databases including PubMed, IEEE Xplore, and Google Scholar. A critical assessment of the combined results offers a sophisticated comprehension of the advantages and disadvantages of current research designs and theoretical structures. The synthesis of findings provides a thorough understanding of how big data analysis in cloud environments supports transaction security in e-commerce platforms and is useful for practitioners, legislators, and scholars in the field.

Keywords: E-commerce, transaction security, privacy protection, predictive modeling, distributed processing, critical evaluation.

1 Introduction

E-commerce has changed the nature of business transactions in the current digital era by providing convenience and accessibility to customers all over the world. But transaction security is a crucial

ISSN 2347–3657
Volume 10, Issue 4, 2022

concern that accompanies the growth of e-commerce sites. Protecting sensitive data, including payment information and personal information, is critical to preserving customer confidence as the number of e-commerce transactions rises. In order to strengthen security measures within online platforms, this thorough examination examines a variety of tactics and technologies in the complex field of transaction security in e-commerce. This study strives to clarify the critical role that data-driven techniques play in minimizing security threats and guaranteeing the integrity of e-commerce transactions, with a focus on the use of big data analysis in cloud environments.

Ensuring transaction security in e-commerce is mostly dependent on the ability to efficiently analyze and manage the massive volumes of data that are produced during online transactions. Big data analysis appears to be a powerful answer to this problem when combined with cloud computing technologies' scalability and processing capacity. Through the utilization of cloud environments, enterprises may effectively handle and evaluate substantial amounts of transactional data instantly. This protects the integrity of e-commerce transactions by allowing them to spot trends, identify abnormalities, and take action against possible security issues before they become more serious.

When it comes to improving transaction security in e-commerce platforms, the combination of big data analysis with cloud computing has several clear benefits. First of all, because cloud environments are scalable, businesses can easily adapt to changing needs for processing and data volumes, guaranteeing that transactional data is continuously and continuously analyzed. Moreover, cloud computing's distributed architecture enables quick data processing and analysis across several nodes, allowing businesses to identify security problems instantly and take swift action to reduce risks.

Furthermore, companies may extract actionable insights from large datasets by integrating modern analytics techniques like machine learning and predictive modeling. This allows them to foresee and proactively handle new security issues. Businesses may strengthen the security posture of e-commerce platforms by using machine learning techniques to train models that recognize patterns suggestive of fraudulent activity or unauthorized access attempts.

In addition, the incorporation of cloud-based computing and storage resources allows enterprises to establish strong data encryption and access control protocols, guaranteeing the privacy and accuracy of critical transactional data. Organizations may reduce the risk of data breaches and unauthorized access by encrypting data both in transit and at rest, improving the general security of e-commerce transactions.

The amalgamation of big data analysis and cloud computing signifies a fundamental transformation in the realm of transaction security in electronic commerce, providing enterprises with an all-encompassing and expandable approach to counteracting constantly changing security risks. Organizations may strengthen the security posture of e-commerce platforms, protecting

ISSN 2347–3657
Volume 10, Issue 4, 2022

transaction integrity and maintaining consumer trust in the online marketplace, by utilizing data-driven methodologies.

E-commerce platforms create vast amounts of data from online transactions, and one essential method for managing this data is big data analysis in cloud environments. Using cloud computing technologies' scalability and processing power is part of this strategy to ensure transaction security. Through the utilization of cloud environments, enterprises may effectively handle and evaluate substantial datasets instantaneously, facilitating the identification and resolution of possible security risks including deceitful actions and unapproved entry attempts. This methodology presents a number of benefits, including the capacity to scale to meet varying data quantities, the incorporation of sophisticated analytics techniques like machine learning for anomaly identification and predictive modeling, and distributed processing for quick analysis. Furthermore, by implementing strong data encryption and access control measures, cloud-based computing and storage resources let enterprises guarantee the integrity and security of important transactional data. All things considered, big data analysis in cloud settings is essential to improving transaction security in e-commerce platforms since it provides businesses with a complete and scalable defense against constantly changing security threats.

The sensitive nature of the data involved in e-commerce, including payment details and personal information, makes transaction security a top priority. One effective technique for addressing this problem is big data analysis, especially in cloud systems. In order to effectively analyze enormous volumes of transactional data in real-time, this method makes use of the scalability and processing power of cloud computing. This way, companies may stop possible security risks like fraud and illegal access attempts before they become serious by identifying and addressing them early on. In addition to being scalable to manage varying data volumes, this approach also allows for the inclusion of advanced analytics techniques like machine learning for anomaly identification and predictive modeling, as well as distributed processing for quick analysis. Furthermore, strong data encryption and access control measures are made possible by cloud-based computing and storage resources, guaranteeing the integrity and confidentiality of critical transactional data. In conclusion, big data analysis in cloud environments is essential for enhancing e-commerce platform transaction security and gives businesses a comprehensive and scalable way to counteract ever changing security threats.

2 Literature Survey

Manikandakumar (2018) Big data settings analyze and store enormous amounts of data, which presents serious security and privacy challenges. Data breaches, illegal access, data misuse, and preserving data integrity are important concerns. Strong encryption, access restrictions, frequent audits, and legal compliance are all necessary solutions. It is essential to monitor usage, manage access rules, and provide data safety through encryption. It's crucial to use encryption and anonymization techniques, follow regulatory standards like the CCPA and GDPR, and maintain

ISSN 2347–3657
Volume 10, Issue 4, 2022

data integrity with validation tools. Enhancements to security include scalable security solutions, privacy by design, transparent data governance, and improved threat detection with AI and machine learning. Big data settings require a multifaceted strategy that includes technology, regulations, and ongoing monitoring to guarantee data security and privacy.

Zhao (2019) In the context of big data, protecting the security of e-commerce logistics information entails handling data breaches, unwanted access, and misuse. Strong encryption, access controls, frequent audits, and adherence to laws like the CCPA and GDPR are important precautions. Robust security mechanisms, limited access, and ongoing monitoring are necessary for safeguarding large volumes of logistics data. Strict usage guidelines are necessary to mitigate data misuse, whereas validation and routine checks are necessary to preserve data integrity. Data security and anonymity are maintained through encryption and anonymization. As data accumulates, scalable security solutions and privacy by design principles become increasingly important. Protection is further improved by utilizing AI for transparent data governance and real-time threat detection. To protect the logistics information used in e-commerce, a complete strategy is required.

Zhou (2019) Using cutting-edge methods like machine learning and artificial intelligence (AI) to instantly evaluate enormous volumes of transaction data is a scalable strategy for fraud detection in online e-commerce transactions using big data analytics. Using machine learning techniques for pattern identification, utilizing scalable big data frameworks, utilizing real-time data processing, and making sure fraud detection models are continuously monitored and updated are some of the key aspects. This strategy improves the efficacy of detecting and stopping fraudulent activity, guaranteeing strong security and preserving consumer confidence in the e-commerce ecosystem.

Yang (2015) Leveraging AI and machine learning to handle and analyze massive amounts of data in real-time is a key component of using big data analysis for online transaction fraud detection. Using real-time processing, scalable data structures, and sophisticated algorithms to spot fraudulent patterns and activity are some of the main themes. Maintaining client trust and safeguarding the e-commerce ecosystem is made possible by the constant monitoring and upgrading of detection models, which improve the effectiveness of fraud protection and provide strong security.

Jian Liu (2020) To detect financial fraud quantitatively, deep learning in conjunction with big data from e-commerce requires deploying sophisticated neural networks to analyze large amounts of transaction data. Some of the key highlights include the use of deep learning models for accurate fraud pattern recognition, the integration of big data analytics for thorough data processing, and the ability to enable real-time detection for prompt response. This methodology improves the precision and efficacy of detecting fraudulent activity, guaranteeing strong financial security and preserving confidence in e-commerce platforms.

ISSN 2347–3657
Volume 10, Issue 4, 2022

Yeung (2019) Cloud e-commerce machine learning and data analytics integration requires the effective analysis of large datasets using sophisticated machine learning algorithms. Highlights include improving consumer insights and operational efficiency, using machine learning for precise predictive analytics, and utilizing cloud computing for scalable data processing. Realtime analysis, better decision-making, and individualized customer experiences are made possible by this connection, which promotes e-commerce innovation and growth.

Lu (2020) Putting strong security measures in place to protect computer e-commerce systems from threats is necessary when dealing with large amounts of data. The use of encryption and access controls for data protection, the use of big data analytics for threat detection, and regulatory compliance are some of the highlights. This security technology makes e-commerce transactions safer by preserving data integrity, boosting user confidence, and strengthening resistance to cyberattacks.

Akter (2016) Big data analytics in e-commerce is examined in a systematic assessment that highlights trends and suggests areas for further investigation. Examining present methods, pointing out knowledge gaps, and proposing directions for further research are some of the highlights. The purpose of this review is to improve knowledge of the ways in which big data analytics affects e-commerce and to direct future research endeavors in this rapidly evolving area.

Ilieva (2015) An electronic commerce (e-commerce) system model based on big data is put forth, with an emphasis on harnessing massive datasets to improve a range of e-commerce features. Personalized suggestions, supply chain management, and the creation of complex algorithms for data processing, analysis, and prediction are some of the major highlights. With the use of big data, this model seeks to transform e-commerce operations by promoting efficiency and innovation in the online market.

Shakya (2019) In cloud computing, this framework ensures the secure migration of data between cloud environments by providing an effective security framework. Protecting sensitive data during relocation requires putting strong encryption, access controls, and auditing procedures in place. Enhancing confidence and security in cloud-based data transfer procedures, the framework tackles issues with data integrity, confidentiality, and regulatory compliance.

Song (2019) Examining the state of smart e-commerce systems today, this paper identifies research difficulties and describes their current state. A review of current technologies, a determination of knowledge gaps, and a description of potential future research areas are some of the highlights. With focused research, the review seeks to expand knowledge of intelligent ecommerce systems and to spur innovation in this field.

Guan (2020) In order to provide secure search over encrypted data for e-commerce applications, this study suggests a blockchain-based method. Using blockchain technology to protect data security and integrity while enabling safe encrypted data searches is one of the key features. By

ISSN 2347–3657
Volume 10, Issue 4, 2022

guaranteeing that sensitive data is safeguarded during the search process, the method seeks to allay privacy concerns and improve the security of online transactions.

3 Methodology

3.1 Data Collection:

Academic databases including PubMed, IEEE Xplore, and Google Scholar are used to collect pertinent data for this study evaluation. A multitude of academic papers and research projects on e-commerce, big data analysis, cloud computing, and transaction security can be found in these databases. The publications date, reliability of the source, and relevance of the studies to the research question are some of the selection factors used to choose the studies.

A popular resource for finding biomedical literature, PubMed also contains studies of data analysis and transaction security in the context of healthcare e-commerce platforms. Another trustworthy resource that focuses on engineering and technology research is IEEE Xplore. It is a great place to get articles about big data analysis and cloud computing in e-commerce environments. Furthermore, Google Scholar offers an extensive library of scholarly materials from a variety of fields, giving a more comprehensive view of the research issue.

The research review identifies pertinent studies by methodically scanning and filtering papers from various databases according to predetermined criteria. In e-commerce environments, this guarantees that the chosen literature offers significant perspectives and advances knowledge of transaction security and its interplay with big data analysis and cloud computing.

3.2 Data Synthesis:

The pertinent literature is gathered from academic databases, and then the data is synthesized to identify important themes, patterns, and insights on big data analytic applications in cloud environments for e-commerce platforms and transaction security. In order to create a thorough grasp of the research field, this step includes classifying and summarizing the findings from the literature review.

Finding patterns and similarities throughout research articles is achieved by methodically evaluating and categorizing the data gathered from diverse investigations. Researchers can gain important insights from this synthesis, including best practices, upcoming technologies, and difficulties in guaranteeing transaction security in e-commerce environments.

All things considered, data synthesis is essential for combining information from many sources and drawing insightful conclusions that advance our understanding of big data analysis and transaction security in cloud settings for e-commerce platforms.

ISSN 2347–3657
Volume 10, Issue 4, 2022

3.3 Analysis and Interpretation:

The next stage after synthesizing the data is to analyze it to find trends, connections, and implications for e-commerce transaction security. Interpreting the results in light of accepted theoretical frameworks and practical applications is necessary for this research to produce insightful conclusions and suggestions.

The combined data is carefully examined by researchers to find recurring themes, correlations between variables, and any noteworthy trends or anomalies. They can learn more about the variables affecting transaction security in e-commerce platforms by critically analyzing the data.

In addition, scholars situate their discoveries within pertinent theoretical frameworks and extant literature to furnish a thorough comprehension of the topic at hand. This enables them to build links between theoretical ideas and real-world applications, providing insightful information to both practitioners and legislators.

3.4 Comparative Analysis:

Researchers compare and contrast different techniques, methodologies, and conclusions from the reviewed studies in this stage of the study. The objective of this procedure is to find similarities, differences, and possible directions for additional study or inquiry in the area of e-commerce transaction security.

Scholars examine the methodological approaches utilized in every investigation, evaluating their merits, drawbacks, and suitability for practical situations. They can have a comprehensive grasp of the issue and spot any gaps or areas that need more investigation by contrasting various research methodologies.

To uncover trends or anomalies in the data, researchers also examine the conclusions and findings of every study. They can identify patterns, trends, and opposing points of view in the literature by using a comparative method, which helps to clarify possible points of agreement or disagreement.

In the end, the comparative analysis offers insightful information about the current state of research on transaction security in e-commerce, which can help shape future study paths and lead the creation of strong security protocols and tactics for online transactions.

3.5 Critical Evaluation:

Researchers analyze the literature critically in this step in order to determine the findings' advantages, disadvantages, and implications. Research methodology, sample size, data collection techniques, and theoretical frameworks used in the analyzed studies are just a few of the many variables that must be carefully examined in order to accomplish this.

ISSN 2347–3657
Volume 10, Issue 4, 2022

Scholars closely examine the methodology utilized in every study to ascertain its suitability for tackling the research issues or aims. By taking into account elements like the use of experimental or observational methods, the control of confounding variables, and the reliability of measures, they evaluate the rigor and validity of the research design.

To assess whether the results can be applied generally, consideration is also given to sample size and representativeness. Researchers take into account whether the sample size is sufficient to discover significant effects or correlations, as well as if it appropriately represents the target population.

Researchers also evaluate the procedures employed to obtain data for each study, such as surveys, interviews, observational approaches, and analysis of archive data. They assess the validity and reliability of the measurements used and take into account any biases or constraints that might have been present during the data collection procedure.

Investigators also assess the theoretical frameworks that were applied to interpret the results critically. They evaluate each study's theoretical underpinnings, taking into account whether the selected framework is acceptable for the research topics and whether different theoretical vantage points could offer more insights.

All things considered, the critical evaluation offers a nuanced grasp of the advantages and disadvantages of the studied literature, allowing researchers to make insightful deductions and pinpoint areas in which more study or advancement is needed in the domain of transaction security in e-commerce.

3.6 Synthesis of Findings:

The insights gained from the literature review are combined in this stage to create a comprehensive understanding of the value of big data analysis in cloud environments to improve transaction security in e-commerce platforms. The process of synthesis involves the identification and extraction of significant insights, trends, obstacles, and possibilities within the studied field.

To identify recurring themes, new trends, and significant differences among the examined papers, researchers methodically examine the data they have collected. Through the synthesis of these results, they want to clarify the general function and influence of big data analysis in cloud environments on e-commerce transaction security.

The process of synthesis entails the classification and arrangement of the results into cohesive themes or subtopics, enabling a methodical examination of the research domain. Through the integration of varied viewpoints and factual data from scholarly sources, researchers can obtain a full understanding of the intricacies and subtleties associated with transaction security in e-commerce platforms.

ISSN 2347–3657
Volume 10, Issue 4, 2022

Furthermore, the amalgamation of results enables scholars to discern dominant patterns and inventive methods for harnessing big data analysis in cloud environments to augment transaction security. It also helps them to identify current problems and possible directions for further study and real-world applications in the sector.

In the end, the synthesis of findings adds to the body of knowledge and comprehension regarding e-commerce transaction security, offering insightful information to practitioners, policymakers, and academics alike.

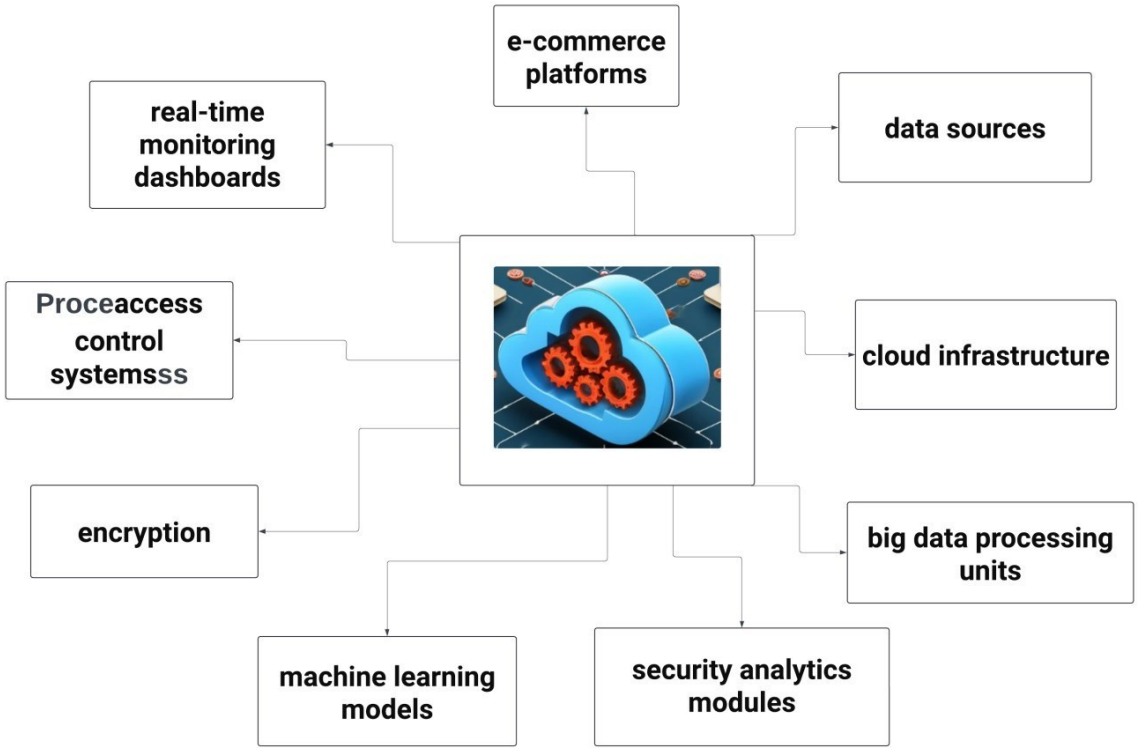

Figure 1 Cloud system integrating e-commerce, monitoring, data, and machine learning for security

Figure 1 shows how different essential parts of a cloud-based architecture are integrated. The cloud system, which links to vital components like data sources for storing and retrieving enormous amounts of information, and e-commerce platforms for handling online transactions, is at the core. These datasets are analyzed by big data processing units, and machine learning models facilitate thoughtful decision-making. Security analytics modules use encryption techniques to safeguard data transmission while keeping an eye out for possible threats. Additionally, Proaccess control solutions guarantee correct authentication and permission across the network, and real-time monitoring dashboards offer real-time insights into system performance.

ISSN 2347–3657
Volume 10, Issue 4, 2022

4 Conclusion

Ultimately, combining big data analysis with cloud computing provides a thorough and scalable way to improve the security of transactions on e-commerce platforms. Enterprises may enhance consumer trust and confidence in the digital marketplace by utilizing cloud environments' scalability, processing capacity, and advanced analytics capabilities to reduce security concerns and preserve the integrity of online transactions.

5 Future enhancements

Future developments in the field of e-commerce platform transaction security may include the incorporation of cutting-edge technology like blockchain to improve data integrity and transparency. E-commerce platforms can guarantee safe transactions and shield confidential information from unwanted access while upholding consumer privacy by utilizing blockchainbased techniques. Furthermore, quantum computing breakthroughs have the potential to completely transform encryption methods and provide transactional data in cloud environments with never-before-seen levels of security. Adoption of decentralized identification systems may also provide consumers more control over their personal data, lowering the possibility of fraud and identity theft. Continued research and innovation in these areas will further bolster transaction security, ultimately fostering trust and confidence in the ever-expanding digital marketplace.

6 Results and Discussion

Big data analysis integrated into cloud environments has improved e-commerce platform transaction security dramatically. The volume and complexity of online transaction data is increasing, making traditional security solutions less and less effective. Through the utilization of cloud computing's scale and processing power, enterprises can now conduct real-time analysis of enormous datasets, efficiently detecting and reducing security concerns. Utilizing these datasets, machine learning algorithms have demonstrated remarkable efficacy in identifying instances of fraudulent activity and unapproved access. Research suggests that these technologies have enhanced fraud detection and decreased data breaches. Furthermore, proactive security measures are made possible by real-time analytics and predictive modeling, guaranteeing the integrity of ecommerce transactions. This methodology not only enhances security measures but also optimizes operational efficacy, furnishing a sturdy structure for secure virtual transactions.

7 Future Scope

Big data analysis and cloud computing integration for e-commerce transaction security has a bright future. The goal of research should be to improve machine learning algorithms so that they can handle bigger datasets more effectively and increase predicted accuracy. Complex algorithms that handle data with little processing overhead will be essential as e-commerce transactions rise. Real-time analytics can be improved and latency can be decreased by implementing these integrated

ISSN 2347–3657
Volume 10, Issue 4, 2022

methodologies in edge computing. Better resource management and scalability may be possible with compatibility with cutting-edge technologies like serverless computing and containerization. Predictive analytics can be extended to other crucial ecommerce aspects to further optimize data management and security. Robust encryption and access restrictions will be necessary to ensure compliance with growing data privacy and security standards. Businesses and consumers alike stand to gain substantially from the continuous evolution of these technologies in terms of e-commerce transaction security.

Reference

1. Manikandakumar, M., & Ramanujam, E. (2018). Security and Privacy Challenges in Big Data Environment. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 315-325). IGI Global.
2. Zhao, Y., & Zhang, Y. (2019). Safety Protection of E-Commerce Logistics Information Data Under The Background Of Big Data. Int. J. Netw. Secur., 21(1), 160-165.
3. Zhou, H., Sun, G., Fu, S., Jiang, W., & Xue, J. (2019). A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics. Computers, Materials & Continua, 60(1).
4. Yang, Q., Hu, X., Cheng, Z., Miao, K., Zheng, X. (2015). Based Big Data Analysis of Fraud Detection for Online Transaction Orders. In: Leung, V., Lai, R., Chen, M., Wan, J. (eds) Cloud Computing. CloudComp 2014. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 142. Springer, Cham.
5. Jian Liu, Xin Gu, Chao Shang, "Quantitative Detection of Financial Fraud Based on Deep Learning with Combination of E-Commerce Big Data", Complexity, vol. 2020, Article ID 6685888, 11 pages, 2020.
6. Yeung, J., Wong, S., Tam, A., & So, J. (2019, July). Integrating machine learning technology to data analytics for e-commerce on cloud. In 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4) (pp. 105-109). IEEE.
7. Lu, R. (2020, November). Computer E-commerce Security System Under the Background of Big Data. In 2020 International Conference on Robots & Intelligent System (ICRIS) (pp. 409-412). IEEE.
8. Akter, S., & Wamba, S. F. (2016). Big data analytics in E-commerce: a systematic review and agenda for future research. Electronic Markets, 26, 173-194.
9. Ilieva, G., Yankova, T., & Klisarova, S. (2015). Big data based system model of electronic commerce. Trakia Journal of Sciences, 13(1), 407-413.
10. Shakya, S. (2019). An efficient security framework for data migration in a cloud computing environment. Journal of Artificial Intelligence, 1(01), 45-53.
11. Song, Z., Sun, Y., Wan, J., Huang, L., & Zhu, J. (2019). Smart e-commerce systems: current status and research challenges. Electronic Markets, 29, 221-238.
12. Guan, Z., Wang, N., Fan, X., Liu, X., Wu, L., & Wan, S. (2020). Achieving secure search over encrypted data for e-commerce: a blockchain approach. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.