The current issue dan full text archive of this journal is available at
https://e-journal.unair.ac.id/jraba
Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8 No. 2 (2023) 1562-1577 ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

MACHINE LEARNING FOR E-COMMERCE FRAUD DETECTION

Rahayu Damayanti [1]
Zaldy Adrianto[2]

ABSTRACT

The study examines the effectiveness, challenges, and best machine learning algorithms for detecting e-commerce fraud. This study uses a systematic literature review to evaluate the effectiveness of machine learning-based e-commerce fraud detection, identify challenges, and identify the most effective techniques. The study examinedliterature extracted from the ScienceDirect, Emeralds, Wiley, and Springer databases, identifying 29 publications from recognized journals from 2012–2022, filtered using limitations and quality assessment criteria, and assessing paper eligibility. This study reveals that machine learning significantly enhances the accuracy of detecting e-commerce fraud. Yet, there are a number of issues that need to be resolved before machine learning can be utilized to detect e-commerce fraud. Poorer-quality data distribution is the biggest challenge in detecting e-commerce fraud. In order to determine the best machine learning strategy, the model's accuracy was also evaluated, and it was discovered that random forests performed the best in terms of accuracy. This study increases theoretical contributions as a continuation of previous research relevant to the concept of machine learning in detecting fraud in e-commerce. Then, based on the random forest's greater precision, it provides practical advice to e-commerce firms as a basis for decision-makers to find a suitable machine learning technique for fraud detection.

Keyword: **Machine Learning, E-Commerce, Fraud, Detection**

ABSTRAK

Penelitian ini bertujuan untuk menganalisis efektivitas, hambatan, dan algoritma machine learning terbaik untuk mendeteksi fraud pada e-commerce. Penelitian ini menggunakan systematic literature review untuk mengevaluasi efektivitas deteksi fraud pada e-commerce berbasis machine learning, mengidentifikasi tantangan, dan mengidentifikasi teknik yang paling efektif. Penelitian ini mengkaji literatur yang diekstrak dari database ScienceDirect, Emeralds, Wiley, dan Springer, menganalisis 29 publikasi dari jurnal yang diakui dari tahun 2012-2022, disaring menggunakan batasan dan kriteria penilaian kualitas, dan menilai kelayakan makalah. Hasil penelitian ini membuktikan bahwa machine learning secara signifikan meningkatkan akurasi dalam mendeteksi fraud di e-commerce. Namun, ada beberapa masalah yang harus diselesaikan sebelum machine learning dapat digunakan untuk mendeteksi fraud pada e-commerce. Distribusi data yang kurang berkualitas merupakan tantangan terbesar dalam mendeteksi fraud di e-commerce. Untuk menentukan strategi machine learning terbaik, akurasi model juga dievaluasi, dan ditemukan bahwa random forests memiliki performa terbaik dalam hal akurasi. Penelitian ini meningkatkan pengetahuan tentang deteksi fraud pada e-commerce dengan menekankan nilai dari machine learning dan mengidentifikasi tantangan yang ada. Berdasarkan akurasi yang lebih tinggi dari random forest, penelitian ini memberikan saran praktis kepada perusahaan e-commerce sebagai dasar bagi para pengambil keputusan untuk menemukan metode machine learning yang sesuai dalam mendeteksi fraud.

Kata Kunci: **Machine Learning, Fraud, E-Commerce, Deteksi**

ARTICLE INFO

***Article History*:**

Received 09 June 2023

Accepted 14 October 2023

Available online 31 November 2023

Introduction

In recent years, the term "fourth industrial revolution" has gained popularity among Indonesians. Digital technology is driving the 21st-century industrial revolution. It all refers to the contemporary era of connectivity, advanced analytics, advanced analytics, automation, and advanced manufacturing technology that has been revolutionizing global business for years. These technologies have the potential

[1] Correspondence Author : Graduated Student at Universitas Padjajaran, Bandung, Telp. 082125359825, Email: rahayudamayanti68@gmail.com
[2] Second Author : Lecturer at Universitas Padjajaran, Bandung, Email : zaldy.adrianto@unpad.ac.id

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

to significantly impact various industies, and many companies are adopting their emerging technologies.

Artificial intelligence refers to the development of computer systems that can perform tasks that would ordinarily require human intelligence, such as visual perception, speech recognition, decision-making, and language translation (Russell and Norvig, 2021). Machine learning is one of the key elements of AI (Han et al., 2019). It has become a crucial aspect of our daily existence, as it has the potential to be integrated into claims processing, customer service, and the identification of fraudulent activity. As a result, numerous industries are allocating funds towards the development of machine learning technologies that can improve their fraud detection capabilities and one of the most interesting ones is e-commerce (Yellapantula and Ayachit, 2019). As e-commerce has become more popular, it has also led to a rise in fraudulent activities, fraudsters have become more sophisticated in their techniques.

In general, the Indonesian government is still making improvements to the realization, which has been adopting machine learning to identify and prevent fraudulent behaviors and combat e-commerce fraud. The "Safe E-Commerce" project was launched by the Ministry of Communication and Information Technology in 2021 to encourage cybersecurity awareness and protect online shoppers (Kominfo, 2021). This is further evidenced by Gupta et al., (2021) said that large e-commerce firms like Amazon and Walmart as well as banking firms like MasterCard have incorporated machine learning to monitor and process factors including transaction size, time and location, the device being used, and purchasing data. Nanduri et al., (2020) have demonstrated that machine learning algorithms are quite good at spotting fraud in e-commerce transactions.

Two modern methods, fraud islands and multi-layer machine learning models, which might effectively tackle the issue of detecting varied fraud patterns, were examined in a study published in 2020. The other topic of discussion concerns machine learning for dealing with e-commerce fraud (Saputra and Suharjito, 2019; Abdulsattar and Hammad, 2020; Hasan et al., 2022; Ruttala Sailusha et al., 2020; Korkmaz et al. 2020). Despite the efforts of e-commerce platforms to use machine learning to avoid fraud, there are still numerous examples of e-commerce fraud that occur. According to research PPATK (2022) fraud in Indonesia is gradually rising, with 9,801 fraud-related suspicious activity reports in 2019, 13,338 in 2020, and over 23,000 in 2021. As of February 2022, the most prevalent form of crime eliciting suspicious activity reports was fraud, which included e-commerce fraud and breaches of electronic transaction rules.

Considering these phenomena, there are still limitations and gaps to its effectiveness, and the potential for biased results in the fraud detection of e-commerce transactions has not been extensively researched, while ML has shown promise and has been increasingly used in e-commerce to detect and prevent fraud. Despite the rising use of machine learning for e-commerce fraud detection, there is a scarcity of comprehensive studies that particularly analyze the effectiveness, challenges, and efficiency of various machine learning algorithms in this field. Existing research frequently focuses on general fraud detection or specific types of fraud, without taking into account the distinct characteristics and requirments of e-commcerce transactions.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Based on present research issues, this study analyzes the findings of prior studies and searches for potential topics for future research. The effectiveness, types of challenges, and best machine learning techniques for detecting e-commerce fraud will all be investigated in this study. The research will be carried out with the systematic literature review approach, which assesses and determines research journal articles systematically by certain steps and phases in order to prevent subjective identification. The use of the SLR approach in machine learning research for e-commerce fraud detection has not yet been explored. This approach should be able to demonstrate the validity of some phenomena and then provide a solution through activities that include problem-solving. The facts are more conclusive, comprehensive, and balanced when they are presented in this debate after being synthesized from research findings using a systematic review method. Based from the earlier mentioned context, the formulation of the research issue is: (i) RQ1, what are the effectiveness of e-commerce fraud detection powered by machine learning? (ii) RQ2, what are the challenges of e-commerce fraud detection powered by machine learning? (iii) RQ3, what is the most efficient machine learning method for e-commerce fraud detection?

The study project has a total of three objectives in order to address the above-mentioned issue formulation. First, analyze the effectiveness of machine learning-powered e-commerce fraud detection from recognized journals from 2012 to 2022. Second, identifying the challenges related to machine learning-powered e-commerce fraud detection to solve the e-commerce fraud detection problem. Third, identify the most effective machine learning approaches for identifying e-commerce fraud to evaluate individual needs in order to choose the most successful machine learning algorithms for e-commerce. The contribution of this research results is expected to get more effective in fraud detection systems and make e-commerce safer and more secure for customers. It presents an in-depth review of the effectiveness of e-commerce fraud detection methods over a ten-year period, giving beneficial insights into the field's progress. It illustrates the present challenges and barriers in machine learning-powered e-commerce fraud detection, which may be utilized to guide future research and development efforts. On a practical level, the research has the potential to improve e-commerce security by identifying issues in current fraud detection methods, therefore protecting consumers. It also protects both both consumers and businesses from fraudulent activity, increasing trust in e-commerce platforms and reducing financial losses as a result of fraud. Eventually, this research makes essential contributions to theoretical understanding as well as practical advances in the e-commerce sector.

Literature Review

Fraud Triangle Theory

Cressey proposed the theory in 1953, and it continues to be used nowadays by auditors, fraud examiners, and other experts to figure out why people commit fraud. Maulidi (2020) supports this statement of fact. The research analyzes the fraud triangle theory and its relevance in the present society. Cressey (1953), began the research of fraud by arguing that there need to be a reason over everything people do, including to commit fraud. Then he explains that there are three keys' factors have to be present for an offense to occur such as pressure, opportunity, and rationalization.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

E-commerce Fraud Detection

The Organization for Economic Cooperation and Development (OECD) provides a commonly used definition of e-commerce as the sale or purchase of products or services carried out through digital platforms using procedures specifically designed for the purpose of receiving or placing orders (Qin et al., 2022). However, the growth of e-commerce has led to fraud practices emerging as one of the most significant threats to the commerce sector. Since fraudulent activity can lead to considerable financial losses, e-commerce fraud is a big risk for online business enterprises.

Research from Rahman et al., (2022), there are several types of e-commerce fraud, such as: (i) classic fraud, this is the most basic kind of fraud, which involves obtaining or buying a victim's credit card information on the Dark Web; (ii) triangulation fraud, is a term offered to this kind of fraud since it includes an e-commerce company, a fraudster, and a real customer; (iii) interception fraud, in this kind of fraud, fraudsters make an order with a matching billing and shipping address to the card's address. (iv) merchant app fraud, refers to fraudulent activity by companies which consent to transactions using mobile applications; (v) digital payment fraud, the launch of EMV standards and the development of technology greatly raised the standard for physical shops' security; (vi) sign-up fraud, are an effective way to increase customer loyalty. Detecting and preventing fraud thus becomes essential to the success of e-commerce enterprises. Fraud detection methods in the context of e-commerce often concentrate on spotting fraudulent activity and transactions that take place inside an online marketplace.

Machine Learning for Fraud Detection Techniques

The world of digital services evolves constantly with a spotlight on implementing machine learning into fundamental digital service activities, recent developments in machine learning in general have opened up possible opportunities for responding to fraud (Psychoula et al., 2021). Machine learning could assist with combat fraud in three ways: detection and interdiction, litigation, then prevention. When a financial institution bans credit card transactions in real time in a case of suspicious behaviour, that's an example of detection and interdiction. An instance where machine learning analysis is utilized to develop a legal argument represents litigation. Prevention is a strategy whereby a company relies on machine learning insights to analyze the fundamental causes of the problem, restructure its business processes, and reduce the chance of fraud popping up in the first place.

As stated by Najem and Kadhem (2021), machine learning is one of the most popular methods for detecting fraud in e-commerce. Machine learning techniques are used to recognize valuable underlying patterns in complicated data sets that human beings would otherwise struggle to detect. The two most popular machine learning techniques are supervised learning, in which algorithms are trained using examples of input and output data that have been labeled by humans, and unsupervised learning, in which the algorithm is given no labeled data in order to allow it to discover structure in the input data (Papadakis et al., 2021).

Previous Research

There have been many previous studies that are relevant to machine learning for fraud detection in e-commerce, as shown in table 1. The following will be presented the findings of previous studies that are considered relevant to the research to be conducted.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Table 1. Previous Research

No	Title	Researcher	Machine Learning Method	Result
1	Fraud Detection using Machine Learning in e-commerce	(Saputra and Suharjito, 2019)	Machine learning with the algorithm Decision Tree, Naïve Bayes, Random Forest, and Neural Network.	This research discovered that analyzing machine learning methods can be utilized to detect fraudulent transactions in e-commerce with high accuracy.
2	Fraudulent Transaction Detection in FinTech using Machine Learning Algorithms	(Abdulsattar and Hammad, 2020)	Classify transactions using five various machine learning algorithms: Stochastic Gradient Descent, Decision Tree, Random Forest, J48, and IBk.	Machine learning systems can detect fraudulent transactions with high accuracy. The study trained five different machines learning algorithms on a dataset of fraudulent and valid transactions.
3	E-commerce Merchant Fraud Detection using Machine Learning Approach	(Hasan *et al.*, 2022)	Rely on machine learning methods which include Random Forests, Decision Trees, and Logistic Regression.	It is discovered that from the accuracy percentage Random Forest outperformed the others for both the datasets. They concluded that machine learning is a potential tool for detecting fraud in e-commerce transactions.
4	Credit Card Fraud Detection Using Machine Learning	(Ruttala Sailusha *et al.*, 2020)	Applying of machine learning techniques, specifically the Random Forest and Adaboost methods.	According to their findings, it is clear that various machine learning algorithms are utilized to detect fraud, however the results are unsatisfactory.
5	Detection of Phishing Websites by Using Machine Learning-Based URL Analysis	(Korkmaz *et al.*, 2020)	Using 8 different methods in the machine learning-based system.	The study discovered that machine learning can detect phishing websites in high accuracy.

Source: Processed by the Author

As shown in the table 1, several research have been conducted to study the application related of machine learning for fraud detection in e-commerce. They use a variety of machine learning approaches and routinely show high accuracy in detecting fraudulent transactions. Some research support Random Forest as a preferable technique, while others indicate that outcomes from diverse algorithms might be unsatisfactory. Furthermore, machine learning is useful in spotting phishing websites. These findings demonstrate machine learning's potential as a useful tool in combatting e-commerce fraud.

Research Method

This study using qualitative research approach. Collectiong and analyzing non-numerical data to better comprehend concepts, viewpoints, or experiences. These techniques have the purpose to provide in-depth insights into a topic or to develop new research concepts (Creswell et al., 2018). To get a comprehensive understanding of the topic, the research adopts a SLR technique to discover relevant research papers and synthesizes the findings. The method of analysis employed for this research adopts the guidelines provided by Kitchenham and Brereton (2013) to conduct a systematic literature review, which is based on many well-defined steps to ensure a reliable procedure. Researchers organized the systematic literature review research into three important steps, as shown in this figure 1 below, using these guidelines: planning, execution, and reporting.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

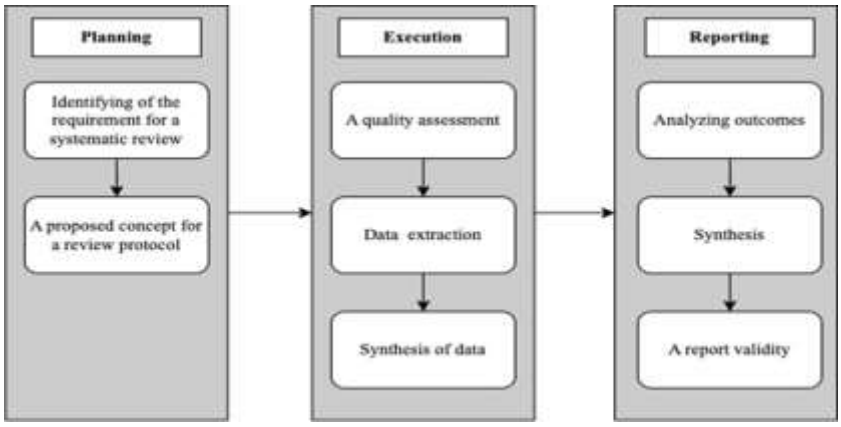

Figure 1. Stages of Systematic Literature Review
Source: Kitchenham and Brereton (2013)

Planning

Search String

The researcher specified the search engines and the search terms to find the most relevant research on databases. To create a search string, certain keywords were created. This text was divided into research units and merged together using Boolean operators. Acronyms, synonyms, and variant spellings were also provided, such as "machine learning" AND "e-commerce" OR "electronic commcerce" AND "fraud detection" OR "fraud prevention" OR "fraud identification" OR "fraud mitigation".

Inclusion and Exclusion Criteria

As stated by Kitchenham and Brereton (2013), Researchers should define inclusion and exclusion criteria based on the research questions, and any studies that are irrelevant to the research questions should be excluded. A presents the following inclusion and exclusion criteria shown in table 2 below:

Table 2. Inclusion and Exlusion Criteria

Inclusion Criteria	Exclusion Criteria
• The paper / journal written in English • The paper / journal match with the search string keyword • Published in between 2012 to 2022 • ScienceDirect, Emerald insight, Wiley online library, and Springer link are among the databases used.	• Review article, book, and chapter from a book • SLR technique used in research article • Preview only / unavailable full text • Didn't have result research

Source: Processed by the Author

The inclusion and exclusion criteria mentioned in table 2 are guidelines used by researchers to pick relevant research papers or articles while conducting a systematic literature review (SLR). The inclusion requirements for this research state that selected papers must be written in English, match search string keywords, have publication date between 2012 and 2022, and be sourced from certain dabatse. However, reviewing articles, books, and book chapters, as well as papers that describe the SLR method, must be removed according to the exclusion criteria. Research findings-only papers or

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

papers with only preview content are not accepted. These criteria assist in reducing the selection of articles that will be considered for the review, ensuring that the chosen studies match with the research goals and objectives of the research.

Search Protocol

Reliability and accuracy in the systematic literature review process depend on a well-structured and documented search protocol. It makes the systematic literature review more dependable and credible by enabling other researchers to comprehend and imitate the research inquiry technique. See table 3 for detail search protocol in this study.

Table 3. Search Protocol

Database	Article type	Fields searched	Search string	Time span
Science-Direct	Research articles Journal Articles	Computer science Business, management and accounting All fields	("machine learning") AND ("e-commerce" OR "electronic commerce") AND ("fraud detection" OR "fraud prevention" OR "fraud identification" OR "fraud mitigation")	2012-2022
Wiley online library	Journals	All fields		
Springer link	Article	Computer Science		

Source: Processed by the Author

As shown in table 3, the provided search protocol provides an organized method for screening several academic databases, including ScienceDirect, Wiley Online Library, and SpringerLink, with a focus on finding articles of interest. It makes the systematic literature review more dependable and credible by enabling other researchers to comprehend and imitate the research inquiry technique. Overall, this search protocol describes the databases to be searched, the precise topics of interest, the search strings used to obtain suitable articles, and, in specific cases, the time frame for the articles to be found.

Quality Assessment Procedure

Assessing high-quality papers is essential for carrying out a valuable systematic literature review (SLR) and obtaining beneficial outcomes. Table 4 present that purpose of the research quality assessment is to specify the previously outlined inclusion and exclusion criteria in more detail. It could be helpful in evaluating the paper's quality and relevancy.

Table 4. Quality Assessment

No	Question	Answer
1	Does the article properly describe the goals of the research?	YES or NO or PARTIAL
2	Is the methodology used throughout that research properly described?	YES or NO or PARTIAL
3	Is a machine learning approach used in the study?	YES or NO or PARTIAL
4	Does the paper provide research results?	YES or NO or PARTIAL
5	Does the article consist of conclusions that correspond to the research's purpose/problem?	YES or NO or PARTIAL

Source: Processed by the Author

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Based on table 4, the quality of the research is assessed by providing a checklist. Results of the study were given quality assessment of 1 to 'yes', 0.5 for 'partially', and 0 for 'no'. Every single piece of literature is worth a maximum of 5 points and a minimum of 0. Literatures with inadequate quality (less than two points) will be failed to include from this research.

Result

The number of records found using the search string on the databases chosen, Science Direct, Emerald Insight, Wiley, and Springer, was 351 data entries. As shown in the figure 2 below, the screening procedure included two steps: abstract screening and full-text screening. Science Direct, Emerald Insight, Wiley, and Springer are the four databases from which the 29 extracted literatures were gathered. Science Direct's database contains the majority of the results. Also, the Science Direct database findings are the most commonly used for data extraction.

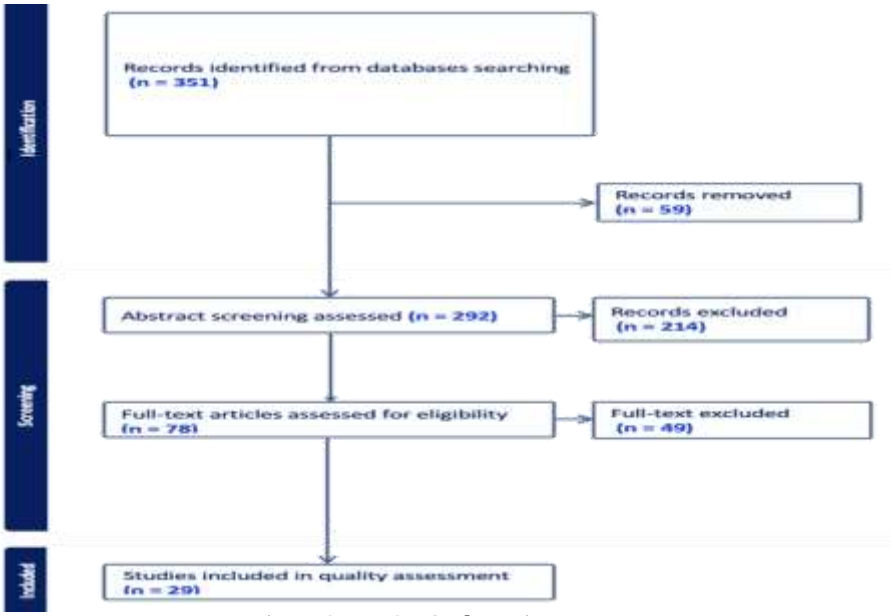

Figure 2. PRISMA Flow Diagram
Source: Processed by the Author

This study, the author was supported by other researchers in this quality control, in which other researchers analyze whether journals are included or not. Any differences of opinion should be reconciled through discussion. The author was supported by other researchers in this quality control, in which other researchers analyze whether journals are included or not. Any differences of opinion should be reconciled through discussion. Synthesis of data in this research can be done with data triangulation. The data extraction outcomes were obtained using MAXQDA, which is marked with three different colors that represent three research questions. Then, the number of instances of these findings throughout the selected publications is referred to as the "frequency" of that particular information. The frequency is concerned with the number of individual occurrences of a finding throughout every piece of paper, not the number of times it appears inside every single paper.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

The Effectiveness of Machine Learning Powered E-Commerce Fraud Detection

Based on analysis of 29 literatures used in the extraction process. The results proved that machine learning is an effective method for detecting e-commerce fraud. Table 5 prosent seven indicators of machine learning effectiveness for detecting e-commerce fraud.

Table 5. Effectiveness of machine learning on e-commerce fraud detection

No	Effectiveness	Frequency	Author
1	Improve fraud detection	5	(Chang et al., 2022; Dastidar et al., 2022; Lucas et al., 2020; Patil et al., 2018; Sadaoui and Wang, 2017)
2	False positive rate	8	(Askari and Hussain, 2020; Baesens et al., 2021; Chang et al., 2022; Ebrahim and Golpayegani, 2022; Dastidar et al., 2022; Kodate et al., 2020; Vorobyev and Krivitskaya, 2022; Wei et al., 2013)
3	Detection rate	3	(Askari and Hussain, 2020; Rezvani and Wang, 2022; Wei et al., 2013)
4	Improved prediction	4	(Riera et al., 2022; Sadaoui and Wang, 2017; Somasundaram and Reddy, 2019; X. Zhang et al., 2022)
5	Increases the accuracy	16	(Almahmoud et al., 2022; Askari and Hussain, 2020; Baesens et al., 2021; Carta et al., 2019; Chang et al., 2022; Dang et al., 2019; Ebrahim and Golpayegani, 2022; Dastidar et al., 2022; Gopal et al., 2022; Goswami et al., 2017; Ileberi et al., 2022; Lebichot et al., 2021; Lucas et al., 2020; Ruan et al., 2020; Takahashi et al., 2018; Wei et al., 2013)
6	True positive rate	7	(Baesens et al., 2021; Carta et al., 2019; Chang et al., 2022; Kodate et al., 2020; Riera et al., 2022; Somasundaram anReddy, 2019; Wei et al., 2013)
7	Fraud prevention	4	(Baesens et al., 2021; Dang et al., 2019; Wei et al., 2013; Westland, 2022)

Source: Processed by the Author

In summary, as shown in the Table 6 above, machine learning has proven to be highly effective in detecting e-commerce fraud, as evidenced by numerous studies that report improvements in fraud detection (5 frequency), which means machine learning can spot trends and abnormalities that humans might fail to recognize, resulting in fewer unreported fraudulent transactions; reduced false positive rates (8 frequency), fewer valid transactions are incorrectly marked as fraudulent, limiting difficulties for real consumers; increased detection rates (3 frequency), more fraudulent transactions are detected; enhanced prediction capabilities (4 frequency), machine learning detects fraud-related characteristics, allowing for specific fraud prevention actions; higher accuracy (16 frequency), by learning from past data, machine learning decreases false positives and false negatives, boosting overall accuracy; improved true positive rates (7 frequency), more fraudulent transactions are precisely reported, leading to fewer false positives; and fraud prevention (4 frequency), machine learning assists in identifying and blocking fraudulent transactions, protecting organizations and customers from financial losses. These findings show that machine learning has a substantial influence on the efficacy and integrity of fraud detection on e-commerce systems.

The Challenges Related to Machine Learning Powered E-Commerce Fraud Detection

The most effective approach will be determined by the e-commerce's individual needs. However, when determining the most effective machine learning strategy for detecting fraud in e-commerce, all of the signs listed below should be considered. Then the frequency of results findings regarding challenging of machine learning in detecting e-commerce fraud is shown in table 6.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Table. 6 Challenges related to Machine Learning Powered E-Commerce Fraud Detection

No	Challenges	Frequency	Author
1	Data availability and quality	8	(Baesens et al., 2021; Carta et al., 2019; Ileberi et al., 2022; Lucas et al., 2020; Sadaoui & Wang, 2017; Saia and Carta, 2019; J. Wang et al., 2020; Wei et al., 2013)
2	Imbalanced issue	4	(Baesens et al., 2021; Chang et al., 2022; Dastidar et al., 2022; Goswami et al., 2017)
3	Model drift	8	(Baesens et al., 2021; Chang et al., 2022; Gopal et al., 2022; Patil et al., 2018; Rezvani and Wang, 2022; Ruan et al., 2020; Sadaoui and Wang, 2017; Zhang et al., 2022)
4	Misclassification due to indetermincay	2	(Askari and Hussain, 2020; Dastidar et al., 2022)
5	Complication in data structure	1	(Dang et al., 2019)
6	Cost factors	3	(Chang et al., 2022; Ebrahim and Golpayegani, 2022; Kodate et al., 2020)

Source: Processed by the Author

These challenges have been identified based on their existence in relevant literature. In summary, the challenges relating to machine learning-powered e-commerce fraud detection include 8 frequencies of data availability and quality, 4 frequencies of addressing imbalanced datasets, 8 frequencies of combating model drift, 2 frequencies of dealing with misclassification due to indeterminacy, 1 frequency of managing complex data structures, and 3 frequencies of considering the financial implications of the fraud detection process.

The Best Effective Machine Learning Approaches for identifying E-Commerce Fraud Detection

According to the findings of the research, machine learning algorithms are effective in identifying fraud, but it is necessary to measure these indicators in order to reach a consensus on which method is most effective. Because it is critical to evaluate the individual needs in order to choose the most successful machine learning algorithms for e-commerce. The most effective approach will be determined by the e-commerce's individual needs. However, when determining the most effective machine learning strategy for detecting fraud in e-commerce, all of the signs of table 7 below should be considered.

Table. 7 The Best Effective Machine Learning Approach for identyfing E-Commerce Fraud Detection

No	Indicators Approach	Frequency	Author
1	The accuracy of the model	20	(Askari ans Hussain, 2020; Baesens et al., 2021; Carta et al., 2019; Chang et al., 2022; Dang et al., 2019; Dastidar et al., 2022; Gopal et al., 2022; Goswami et al., 2017; Ileberi et al., 2022; Lebichot et al., 2021; R. Najem et al., 2022; Patil et al., 2018; Riera et al., 2022; Ruan et al., 2020; Saia and Carta, 2019; Somasundaram and Reddy, 2019; Takahashi et al., 2018; Wei et al., 2013; Westland, 2022; X. Zhang et al., 2022)
2	The recall of the model	12	(Almahmoud et al., 2022; Ebrahim and Golpayegani, 2022; Lucas et al., 2020; R. Najem et al., 2022; Patil et al., 2018; Riera et al., 2022; Ruan et al., 2020; Saia and Carta, 2019; Vorobyev and Krivitskaya, 2022; J. Wang et al., 2020; Z. Wang et al., 2018; X. Zhang et al., 2022)
3	The F1 score of the model	7	(Askari and Hussain, 2020; Baesens et al., 2021; Dang et al., 2019; Gopal et al., 2022; Goswami et al., 2017; Patil et al., 2018; Zhang et al., 2022)
4	The precision of the model	7	(Almahmoud et al., 2022; Baesens et al., 2021; Dang et al., 2019; Ileberi et al., 2022; Ruan et al., 2020; Takahashi et al., 2018; J. Wang et al., 2020)

Source: Processed by the Author

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

When it comes to effective machine learning algorithms for detecting e-commerce fraud, different criteria are critical in evaluating their effectiveness. As the table 7, the model's accuracy is provided at 20 occurrences in this context, demonstrating how effectively it properly identifies fraud issues. Furthermore, the model's recall is reported at 12 occurrences, indicating its capacity to catch all real fraud occurrences. The F1 score, which is a combination of precision and recall, is recorded at 7 occurrences, indicating the model's overall efficacy. The model's precision, which shows the percentage of successfully recognized fraud instances among those flagged, is likewise claimed to be 7 occurrences. These metrics give an understanding of the model's effectiveness in detecting e-commerce fraud.

Discussion

Based on figure 3, trend data reveals an overall upward trend, with the number of occurrences growing from zero in 2012 to twelve in 2022. There were minor changes in the statistics, such as no occurrences in 2014, 2015, and 2016, it was because the development of the technology was still in its early stages. The task of using machine learning for fraud detection is difficult and complex, and in 2014 to 2016, the technology was not as developed as it is now. This could have resulted in fewer researchers working in this field and few publications. As a result, research articles from those years are far less likely to be eligible for inclusion in this study

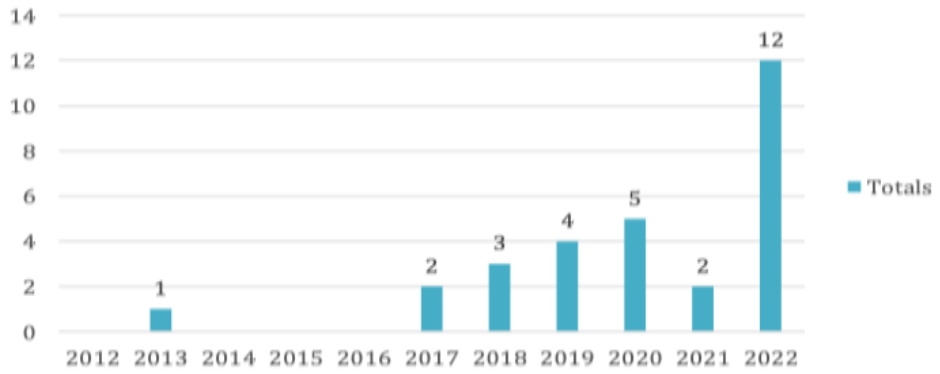

Figure 3 Publication Trend
Source: Processed by the Author

The decreasing pattern in 2021 has been triggered by the widespread pandemic, which may have distracted people's attention. The COVID-19 pandemic had a huge influence on business entities in 2020, including fraud detection. Plenty of businesses were forced to prioritize other objectives, such as keeping their operations operating during the pandemic, which may have resulted in a drop in 2021 fraud detection research on this topic. However, there is a significant increase in the number of publications in 2022, which might be due to a variety of factors such as the availability of new data or methodologies or the development of new research issues.

The authors discovered that the most frequently reported effectiveness of machine learning on e-commerce fraud detection is the ability to increase accuracy.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

According to Lucas et al., (2020) article, the application of HMM-based features increases accuracy on both e-commerce and face-to-face transactions, allowing the classifiers to achieve the highest levels of accuracy on both e-commerce and face-to-face transactions. Massive trials also demonstrate that the machine learning approach significantly increases the accuracy of identifying fraud and outperforms conventional fraud detection techniques and systems in terms of both efficiency and accuracy (Wei et al., 2013).

One of the most commonly observed challenges throughout the research is data availability and quality. The most critical challenge in detecting e-commerce fraud is the fact that invalid transactions are often less than valid ones, and such a poorer quality data distribution decreases the effectiveness of machine learning algorithms (Saia and Carta, 2019). Added to that, as noted by J. Wang et al., (2020) lack of sufficient labeled data is always a significant and unavoidable challenge in the fraud detection field in the field of e-commerce. The other one is model drift. This is an issue which all machine learning techniques face over time. As patterns of fraudulent activity change, the machine learning model may become obsolete and less effective. This means that the model must be updated on a frequent basis to guarantee that it remains effective. This argument can be supported by Baesens et al., (2021) the first highlighted feature and related issue is the reality that fraud is uncommon. Those who commit fraud are able to adapt or improve their strategies as needed, such as when fraud detection mechanisms change.

The findings revealed that the accuracy of the machine learning model is one of the most important metrics for determining the best machine learning methodologies. The best possible machine learning techniques way to fraudulent prediction implemented by the algorithm to the total observations to establish its effectiveness in identifying the fraud transaction is accuracy (Chang et al., 2022). These variables, including accuracy, precision, recall, and F1 score, can be used to evaluate the effectiveness of each ML technique. In terms of accuracy, precision, recall, and f1 parameters, the random forest model outperforms logistic regression and decision trees when built and tested using the same data (Patil et al., 2018). Moreover, stated by Takahashi et al., (2018) according to the outcome, Random Forest outperforms XGBoost in terms of resilience and accuracy when parameter tuning costs are taken into account. Following that is model recall, which is the second most significant attribute when assessing the best machine learning approaches. The top objective in this situation is to get rid of the greatest possible amount of attacks, implying an investment of time and money in correcting the number of not present attacks (false positives). In this kind of situation, recall is the most effective statistic to use because it maximizes attack detection (Riera et al., 2022).

Conclusion

In this systematic literature review, the author examined the application of machine learning methods in e-commerce fraud detection. Based on the study, which was conducted it would beconclude that the effectiveness of machine learning to detect fraud on e-commerce most frequently reported is the ability to increase the accuracy. Moreover, the challenging that face on this topic is data

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

availability and quality, because the majority of studies reported are unable to be reproduced is one of the main issues with using machine learning methods to solve the e-commerce fraud detection problem. This is due to the fact that e-commerce transactions are highly confidential. In addition, the accuracy of the machine learning approach is one of the most important metrics for determining the best machine learning methodologies. From these indicators stated, that random forest approach is one model that outperformances than the other model. However, to get more effectiveness, e-commerce may acquire a more comprehensive perspective of the fraud environment and identify fraudulent transactions more effectively by combining different machine learning algorithms. This can assist e-commerce companies in reducing fraud and protecting their customers.

Limitations

This section describes the limitations of the review approach used throughout the study. Here, we intend to explain to readers what may be investigated in further study by extending what is currently being studied. We only looked at research initiatives and did not examine commercial solutions. Unfortunately, a systematic literature review is dependent on search strings to research databases that do not lead to commercial solutions. Then, this study has several limitations, including data availability and quality, possible data biases, and present-day bias. Patterns of fraud change throughout time. Because data from 2012 to 2022 may not represent the most current fraud patterns and issues the implications may be having less significance. Due to these limitations, the findings of the research may have less practical value and application, which may require some additional research or concern when applying the results to real-world situations.

Suggestions

These suggestions meet the need for interpretability, real-time efficiency, and privacy issues in the developing area of machine learning-based e-commerce fraud detection. E-commerce fraud detection often requires deciding in real time. Future studies need to look into techniques for real-time fraud detection that can adjust to shifting fraud trends and make prompt choices to prevent fraudulent transactions while minimizing reports of false positives. This research has some recommendations for further research based on the limitations of the research already mentioned, such as: (i) for this research, only literature from four databases were used: Science Direct, Emerald insight, Wiley, and Springer. Future research should be conducted relying on other databases to get more literature data because we do not treat all available papers due to the unavailability of some papers; (ii) the results of this research can be used in meta-analysis, and future research may develop new techniques to undertake a deeper examination of the data. It is possible to combine the findings from multiple studies using this quantitative approach. This can contribute to a more robust and solid estimates of the outcome.

Implication

The findings of this study could serve to improve the effectiveness of fraud detection systems and make e-commerce safer and more secure for customers. It provides a comprehensive review of the effectiveness of e-commerce fraud

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

detection technologies over a ten-year period, providing useful insights on the development of the field. It demonstrates the current difficulties and limitations in machine learning-based e-commerce fraud detection, spotlighting them in order to direct future research and development initiatives. The research also aims to strengthen fraud detection applications, enhancing the security and safety of their clients' online purchases. This increases the overall trustworthiness of e-commerce platforms and protects both customers and businesses against fraudulent conduct.

Reference

Abdulsattar, K., and Hammad, M. 2020. Fraudulent Transaction Detection in FinTech using Machine Learning Algorithms. *International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT*.

Almahmoud, S., Hammo, B., Al-Shboul, B., and Obeid, N. 2022. A hybrid approach for identifying non-human traffic in online digital advertising. *Multimedia Tools and Applications*. Vol.81 No.2. Pp.1685–1718.

Askari, S. M. S., and Hussain, M. A. 2020. IFDTC4.5: Intuitionistic fuzzy logic-based decision tree for E-transactional fraud detection. *Journal of Information Security and Applications*. Vol.52 No.1. Pp.1-13.

Baesens, B., Höppner, S., and Verdonck, T. 2021. Data engineering for fraud detection. *Decision Support Systems*. Vol.150 No.1. Pp.1-3.

Carta, S., Fenu, G., Reforgiato Recupero, D., and Saia, R. 2019. Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model. *Journal of Information Security and Applications*. Vol.46 No.1. Pp.13–22.

Chang, V., Doan, L. M. T., Di Stefano, A., Sun, Z., and Fortino, G. 2022. Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*.Vol.100 Nol.1. Pp.1-21.

Cressey D. R. 1953. *Other people's money: a study in the social psychology of embezzlement*. Free Press.

Dang, T. K., Pham, D. M. C., and Ho, D. D. 2019. On verifying the authenticity of e-commercial crawling data by a semi-crosschecking method. *International Journal of Web Information Systems*. Vol.15 No.4. Pp.454–473.

Ebrahim, M., and Golpayegani, S. A. H. 2022. Anomaly detection in business processes logs using social network analysis. *Journal of Computer Virology and Hacking Techniques*. Vol.18 No.2. Pp.127–139.

Ghosh Dastidar, K., Jurgovsky, J., Siblini, W., and Granitzer, M. 2022. NAG: neural feature aggregation framework for credit card fraud detection. *Knowledge and Information Systems*. Vol. 64 Vol.3. Pp.831–858.

Gopal, R. D., Hojati, A., and Patterson, R. A. 2022. Analysis of third-party request structures to detect fraudulent websites. *Decision Support Systems*. Vol.154 No.1. Pp.1-12.

Goswami, K., Park, Y., and Song, C. 2017. Impact of reviewer social interaction on online consumer review fraud detection. *Journal of Big Data*. Vol.4 No.1. Pp. 1-15.

Gupta, D., Polkowski, Z., Khanna, A., Bhattacharyya, S., and Castillo, O. 2021. Lecture Notes on Data Engineering and Communications Technologies. *Proceedings of Data Analytics and Management*. Volume 54.

Han, J., Kamber, M., and Pei, J. 2019. *Data Mining: Concepts and Techniques (4th)*. United States: Morgan Kaufmann Publishers.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Hasan, F., Mondal, S. K., Kabir, M. R., Al Mamun, M. A., Rahman, N. S., and Hossen, M. S. 2022. E-commerce Merchant Fraud Detection using Machine Learning Approach. *7th International Conference on Communication and Electronics Systems, ICCES 2022 - Proceedings*, 1123–1127.

Ileberi, E., Sun, Y., and Wang, Z. 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*. Vol. 9 No.1. Pp.1-17.

John W. Creswell, and J. David Creswell. 2018. *Research Design Qualitative, Quantitative, and Mixed Methods Approaches (Vol. 5th)*. United States: SAGE Publication, Inc.

Kitchenham, B., and Brereton, P. 2013. A systematic review of systematic review process research in software engineering. In *Information and Software Technology*. Vol. 55 No.12. Pp. 2049–2075

Kodate, S., Chiba, R., Kimura, S., and Masuda, N. 2020. Detecting problematic transactions in a consumer-to-consumer e-commerce network. *Applied Network Science*. Vol.5 No.1. Pp.1-18.

Kominfo. 2021. *https://www.kominfo.go.id/*.

Korkmaz, M., Koray Sahingoz, O., and Diri, B. 2020. Detection of Phishing Websites by Using Machine Learning-Based URL Analysis. 11th International Conference on Computing, Communication, and Networking Technologies (ICCNT).

Lebichot, B., Paldino, G. M., Siblini, W., He-Guelton, L., Oblé, F., and Bontempi, G. 2021. Incremental learning strategies for credit cards fraud detection. *International Journal of Data Science and Analytics*. Vol.12 No.12. Pp.165–174.

Lucas, Y., Portier, P. E., Laporte, L., He-Guelton, L., Caelen, O., Granitzer, M., and Calabretto, S. 2020. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems*. Vol.102 No.2. Pp.393–402.

Maulidi, A. 2020. When and why (honest) people commit fraudulent behaviours? : Extending the fraud triangle as a predictor of fraudulent behaviours. *Journal of Financial Crime*. Vol.27 No.2. Pp.541–559.

Najem, R., Amr, M. F., Bahnasse, A., and Talea, M. 2022. Artificial Intelligence for Digital Finance, Axes and Techniques. *Procedia Computer Science*. Vol.203 No.1. Pp.633–638.

Najem, S. M., and Kadhem, S. 2021. A Survey on Fraud Detection Techniques in E-Commerce. *Journal Techknowledge.* Vol.1 No.1. Pp.33-47.

Papadakis, S., Alexandros Garefalakis, Christos Lemonakis, Christiana Chimonaki, and Constantin Zopounidis. 2021. *Machine learning applications for accounting disclosure and fraud detection*. IGI Global.

Patil, S., Nemade, V., and Soni, P. K. 2018. Predictive Modelling for Credit Card Fraud Detection Using Data Analytics. *Procedia Computer Science*. Vol.132 No.1. Pp.385–395.

Psychoula, I., Gutmann, A., Mainali, P., Lee, S. H., Dunphy, P., and Petitcolas, F. 2021. Explainable Machine Learning for Fraud Detection. *Computer*. Vol.54 No.10. Pp.49–59.

Qin, Z., Shuai, Q., Wang, G., Zhang, P., Cao, M., and Chen, M. 2022. *E-Commerce: Concept, Princples, and Application.* United States: Springer.

Rezvani, S., and Wang, X. 2022. Intuitionistic fuzzy twin support vector machines for imbalanced data. *Neurocomputing*. Vol.507 No.1. Pp.16–25.

Jurnal Riset Akuntansi dan Bisnis Airlangga Vol. 8. No. 2 (2023) 1562-1577
ISSN 2548-1401 (Print) ISSN 2548-4346 (Online)

Riera, T. S., Higuera, J. R. B., Higuera, J. B., Herraiz, J. J. M., and Montalvo, J. A. S. 2022. A new multi-label dataset for Web attacks CAPEC classification using machine learning techniques. *Computers and Security*. Vol. 120 No.1. Pp.1-18.

Ruan, N., Deng, R., and Su, C. 2020. GADM: Manual fake review detection for O2O commercial platforms. *Computers and Security*. Vol.88 No.1. Pp.1-11.

Russell, S., and Norvig, P. 2021. *Artificial Intelligence, Global Edition a Modern Approach*. Munchen: Pearson Deutschland.

Ruttala Sailusha, V. Gnaneswar, R. Ramesh, and G. Ramakoteswara Rao. 2020. *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS)*

Sadaoui, S., and Wang, X. 2017. A dynamic stage-based fraud monitoring framework of multiple live auctions. *Applied Intelligence*. Vol.46 No.1. Pp.197–213.

Saia, R., and Carta, S. 2019. Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*. Vol.93 No.1. Pp.18–32.

Saputra, A., and Suharjito. 2019. Fraud Detection using Machine Learning in e-Commerce. *International Journal of Advanced Computer Science and Applications*. Vol.10 No.9. Pp.332-339.

Somasundaram, A., and Reddy, S. 2019. Parallel and incremental credit card fraud detection model to handle concept drift and data imbalance. *Neural Computing and Applications*. Vol.31 No.1. Pp. 3–14.

Takahashi, M., Azuma, H., and Tsuda, K. 2018. A Study on Delivery Evaluation under Asymmetric Information in the Mail-order Industry. *Procedia Computer Science*. Vol.126 No.1. Pp.1298–1305.

Vorobyev, I., and Krivitskaya, A. 2022. Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models. *Computers and Security*. Vol.120 No.1. Pp.1-11.

Wang, J., Guo, Y., Wen, X., Wang, Z., Li, Z., and Tang, M. 2020. Improving graph-based label propagation algorithm with group partition for fraud detection. *Appl Intell.* Vol.50 No.1. Pp.3291-3300.

Wang, Z., Gu, S., Zhao, X., and Xu, X. 2018. Graph-based review spammer group detection. *Knowledge and Information Systems*. Vol.55 No.3. Pp.571–597.

Wei, W., Li, J., Cao, L., Ou, Y., and Chen, J. 2013. Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*. Vol.16 No.4. Pp. 449–475.

Westland, J. C. 2022. A comparative study of frequentist vs Bayesian A/B testing in the detection of E-commerce fraud. *Journal of Electronic Business & Digital Economics*. Vol.1 No.1-2. Pp.3–23.

Yellapantula, K., and Ayachit, M. 2019. Significance of Emotional Intelligence in the Era of Artificial Intelligence: A Study on the Application of Artificial Intelligence in Financial and Educational Services Sector. *Ushus - Journal of Business Management*. Vol.18 No.1. Pp.35–48.

Zhang, X., Du, Q., and Zhang, Z. 2022. A theory-driven machine learning system for financial disinformation detection. *Production and Operations Management*. Vol. 31 No. 8. Pp.3160–3179.