ONLINE PAYMENT FRAUD DETECTION USING GRAPH NEURAL NETWORK AND COMPARISON WITH TRADITIONAL MACHINE LEARNING TECHNIQUES

Table of Contents

Introduction

Detecting online payment fraud is an essential duty in the modern digital environment. “Graph neural networks (GNNs)” are increasingly being utilised to examine and speckle fraud patterns in many businesses (Das et al., 2023). “GNNs” can be utilised in this position to show the interconnections and connections between the many groups experiencing online transactions, including buyers, sellers, and payment networks. “GNNs” are able to successfully capture intricate relationships and spot fraudulent behaviour by leveraging the graph configuration of the data. “Graph Neural Networks (GNNs)”, a specific type of “deep learning model”, are prepared to take data that is collected as graphs. The relations and interdependence among various institutions involved in a dealing, such as users, merchants, and payment networks, can be effectively captured by a “GNN”. when attempting to determine online payment fraud (Ren, 2021). Through the addition of graph information, “GNNs” can improve the accuracy of fraud detection. Payment online fraud is a complex issue that calls for taking into account a number of variables and how they interact. With users, merchants, and payments all connected, the transaction data naturally creates a network structure (El Orche *et al.*, 2020). Graph Neural Networks is a promising choice for handling and identifying fraudulent transactions in payments via the Internet since they have lately emerged as a potent tool for processing graph-structured data. "GNNs" may capture and take advantage of the intricate dependencies and relationships found in a transaction network by utilizing the built-in graph structure. The main goal of this study is to evaluate the performance of neural networks based on graphs in payments via internet fraud detection and contrast it with that of more conventional machine learning methods. Utilizing a real-world dataset with labelled examples of both fraud and genuine transactions, extensive experimental research is carried out (Audibert *et al.*, 2022). A full assessment of the models' detecting abilities may be made because the data set represents a wide variety of fraudulent actions. Several performance indicators, comprising precision, recall, precision, and F1-score, are used to assess the success of the suggested strategy. With the least amount of positive results and false negatives, these measures offer a thorough evaluation of the models' capacity to recognize fraudulent transactions. In addition, the interpretability of the models is examined to learn more about the graph-based traits that are most helpful in the identification of fraud. The findings of the experimental investigation show that in the identification of online payment fraud, the "Graph Neural Network" models perform better than conventional machine learning methods (Nicholls *et al.*, 2021). The “GNN” performs better in terms of precision, recall, precision, and F1-score, demonstrating how well it can distinguish between legitimate and fraudulent transactions. The “GNN” offers a more accurate representation of the complex dependencies and patterns found in the transaction network.

Concept

The idea underlying the concept of online payment fraud detection is the use of graph neural networks (GNNs) to detect fraudulent activity in online payment systems. To analyse structured data, graph-based neural networks were developed (Yang et al., 2022). In the context of online payment systems, graphs can be used to depict various linkages and interactions that occur among users, transactions, and various other entities. Traditional machine learning techniques in fraud detection sometimes use feature engineering, which is manually collecting specific features or patterns from the data and applying them as inputs to the machine learning model. The numerous dependencies and relationships present in the data may, however, be beyond the scope of this strategy. On the other hand, GNNs may work directly with graph-structured data and extract the structural information that is there (Vatter et al., 2023). The interactions, dependencies, and patterns indicating fraudulent behaviour can be efficiently learned and modelled by GNNs by taking into account the relationships between various entities in the payment system. This makes using GNNs to detect online payment fraud a promising strategy. GNNs provide several advantages over conventional machine learning methods, including the capacity to handle various graph architectures and add node and edge properties into the learning process (Munikoti *et al*., 2023). GNNs may learn edge embeddings, which capture interactions between things, as well as node embeddings, which capture representations of specific entities like users or transactions. The capacity of GNNs to shed light on the graph-based properties that are most important for fraud detection is one of their advantages. This characteristic of interpretability enables stakeholders to comprehend the logic underlying the model's forecasts and get insightful knowledge of the transaction graph's patterns and indicators of fraud (Nazir *et al*., 2023). A type of neural network called GNN is made to work with data that is organized into graphs. To execute calculations and learn representations that reflect global as well as local patterns inside the graph, they take advantage of the underlying graph topology. GNNs are well suited for capturing complex linkages and interconnections in transaction networks due to their capacity to transmit knowledge across nodes and include contextual information. Feature Extraction: Useful features must be gathered from a transaction graph in order to construct a GNN model for identifying fraud. The properties of nodes (such as user attributes and merchant attributes), transactional information (such as the amount and date), and inferred graph-based features (such as node centrality and clustering coefficients) can all be included in these features. The representation of transaction data in a format appropriate for GNN-based analysis depends heavily on feature extraction (Liu *et al.*, 2021). In general, the idea of using Graph Neural Networks to detect online payment fraud entails making use of the structure of graphs of transaction data, using the GNN model to capture complex linkages and dependencies, and evaluating their effectiveness against conventional machine learning methods. With the help of this strategy, banking organizations and e-commerce platforms can better protect themselves against fraudulent actions involving online payment systems by improving the precision and comprehension of fraud detection systems (Saeed, 2023).

Literature Review

According to Zhou *et al.*, 2021, study, The financial industry's expansion model has been changed by the fast evolution of information and communication technologies such as “Big Data”, “Internet of Things”, “Artificial Intelligence”, “Machine Learning”, “Blockchain”, etc. These technologies include held a substantial effect on customer behaviour. Customers or customers have profited from the efficiency and reassurance that economic services on the Internet and “IoT” control obtained them, but there are even further concealed fraud threats that have occurred. The outcome of finance on the Internet and “IoT” has mourned antagonistic repercussions and consequential failures due to “imitation”, “arbitrage”, “vicious collection”, etc. However, living rule-based professional plans and traditional machine learning sample systems are discovering it increasingly and it is hard to determine economic fraud from large-scale recorded data as the part of economic data persists to increase dramatically. Meanwhile, as economic and all type of crime evolves more specialised, fraudsters might evade standing caught by constantly changing their ways of deception. The chart embedding algorithm “Node2Vec” is executed in this research as part of an intellectual and spread “Big Data” strategy for “Internet financial fraud detection”. This algorithm comprehends and describes the topological elements in the economic web graph as “low-dimensional dense vectors”, allowing deep neural networks to efficiently and intelligently organise and forecast data models from the “large-scale dataset”.

In recent years, fraud concerning "credit card" transactions affects card issuers by billions of dollars. Decreasing fraud or scam-related losses is supposed to require a well-designed fraud detection method with a cutting-edge fraud detection instance. Zhang *et al.*, 2021, have stated the work's major assistance stands as the result of a fraud detection method operating a "deep learning architecture" and a "refined quality engineering method" established on "homogeneity-oriented behaviour analysis (HOBA)". The authors launch a comparison study based on the "real-world dataset" from one of the largest retail rises in many countries to evaluate the usefulness of the proposed modules. The practical results indicate that the researchers suggested procedure is a functional and thriving instrument for detecting credit card fraud. The researchers suggested method, with a passable "false positive rate", can detect extensively more deceitful transactions than the standard methods. The key findings of the research are to have organisational importance for credit card issuers, who can use the suggested procedure to fast determine fraudulent dealings, protect the interests of their clients, and cut down on fraud losses and regulatory expenses.

The internet market is encountering a severe issue with “click fraud” due to the rapid rise of online advertisements. By connecting on pay-per-click adverts, click fraud is a fraudulent try to enhance a website's income or spend an advertiser's budget. This unlawful activity has endangered the industrial sectors for a while. Due to the numerous groups endeavouring to profit from themes, these organisations are unwilling to promote their outgrowth on mobile apps, social platforms and websites. A dedicated system for practical click fraud detection is needed for companies to safely promote their benefits and effects online. An ensemble architecture of “machine learning” and “deep learning“ is meant to handle this issue and determine click fraud in online advertising drives. A “Convolutional Neural Network (CNN)”, a “Bidirectional Long Short-Term Memory network (BiLSTM)”, which is used to remove hidden parts, and a “Random Forest (RF)”, which is utilised for variety, make up the suggested architecture. The immediate goal of the presented research study by Batool *et al.*, 2022, is to make a “hybrid DL model” for automatically removing features from clicks data, which will then be processed through an “RF” classifier to divide clicks into two categories, such as detectable and non-detectable clicks. A preprocessing module is made to manage definite characteristics and imbalanced data in order to improve the consistency and dependability of click data.

There are lots of people who are using credit cards to make investments and purchases online since they present a timely and sufficient approach. Credit card mishandling is currently more likely as a consequence of improved credit card use. Alarfaj *et al.*, 2022, have stated that both the proprietors of credit cards and economic institutions suffer huge economic losses as an outcome of credit card theft. The primary goal of this research study was to determine such frauds, which contain high-class data inequality, data accessibility, modifications in fraud nature, and increased false alarm rates. Many “machine learning-based algorithms” for credit card detection are shown in the relevant literature, including the “Extreme Learning Method”, “Decision Tree”, “Support Vector Machine”, “Random Forest”, “Logistic Regression”, and “XG Boost”..Current “deep learning algorithms” must still be used to facilitate fraud losses despite their poor precision. The immediate area of attention has been the current development of “deep learning algorithms”. A comparison of both “machine learning” and “deep learning algorithms” was functioned to reach successful results. A thorough empirical research was carried out utilising the “European card benchmark dataset” for fraud detection. So a “machine learning technique” was involved in the dataset, which marginally enhanced the precision of fraud detection.

There were some methods discussed in this research by Tingfei *et al.*, 2020, have acknowledged the methods were repeatedly employed by Zhoud to explore and find the grave problem of credit card theft. However, due to their extremely uneven class allocations, standard credit card datasets display unstable type scenarios. Although professionals have offered several tactics to manage these inequalities, deficiencies still exist. To handle this case, the researchers deliver a “variational automatic coding (VAE)”-based oversampling technique that blends classic “deep learning” methods. In an unstable dataset, the “VAE” method is employed to deliver a sizable number of additional instances from minority parties, which are thereafter utilised to train the category network. The “VAE” method exceeds manufactured juvenility oversampling techniques and conventional “deep neural network techniques”, according to testing results. Similarly, it functions better than current oversampling approaches made on “generative adversarial network (GAN)” standards. The “VAE” standard trials well on metrics such as accuracy, F-measure, and particularity after being shown the enlarged dataset for activity. According to these observed findings, imbalanced classification problems can be successfully dined using the “VAE”-based oversampling process.

For multiple forecast tasks, representation learning in charts has been adequate. In this study, Van Belle *et al.*, 2020, consider the viability of expression learning in the context of credit card fraud. In earlier studies, data analytics was victorious at indicating fraud. The research society has, however, focused on forms that require time-consuming and costly hand-crafting of parts. Additionally, data on the network of dealings is often overlooked in existing positions. “Graph representation learning” handles both of these problems. At the start, it presents the option to utilise the relational and structural elements of the marketing network to create a predictive measure. Second, it feature-engineers the chart without the requirement for tedious manual work. By living the first to sincerely and thoroughly explain how fraud detection modelling can gain from expression learning, this work counts to the body of knowledge. In this research, the authors differentiate between three distinct methods: traditional network quality engineering, an inductive term learning algorithm, and a transductive representative learner. Researchers indicate the supremacy of state-of-the-art miniature learning in charts over traditional chart component extraction utilising thorough practical examination of a real-world dataset.

Numerous studies utilising “deep neural networks (DNNs)” for the purpose of catching credit card fraud have focused on improving point forecast accuracy and determining undesirable biases by creating different network structures or learning standards. It is important to quantify luck together with point analysis. It facilitates model injustice and allows practitioners to develop dedicated systems that bypass causing poor decisions because of uncertainty. In real-world card fraud detection settings, it is necessary to explicitly set the delays associated with “DNN” forecasts for a numeral of reasons, including fraudsters often change their tactics, so “DNNs” meeting statements that are not made by the same method as the activity distribution, and due to the “time-consuming process”, very few dealings are conveniently reviewed by experienced professionals to correct models. In order to see card fraud utilising transaction data, this paper which is made by Habibpour *et al.*, 2023, presents three “uncertainty quantification (UQ) techniques”. Examples of the techniques are “Monte Carlo dropout” and “ensemble Monte Carlo dropout”.So, the “UQ” chaos matrix and a numeral of implementation needles are utilised to evaluate the predictive indecision estimations. The researchers explain via observed findings that the ensemble charges indecision associated with developed predictions more efficiently. Similarly, the authors demonstrate that the proposed “UQ” systems add more context to the actual predictions, enhancing the fraud prevention approach.

With the rapid growth of mobile Internet and financial technology, online e-commerce transactions have been rapidly developing and extending, bringing a lot of conveniences and accessibility to our lives internationally, but in the meantime, the risks of committing fraud come in all forms and sizes. Furthermore, because of the huge volumes of data created in e-commerce, which makes fraudulent transactions more surreptitiously interspersed with real transactions than previously, fraud detection in online transactions in e-commerce is not completely the same as that in existing sectors. In this article, Zhou *et al.*, 2019, propose a uniquely scalable and comprehensive strategy for identifying fraudulent activity in online e-commerce transactions, with four logical modules that use machine learning algorithms and big data analytics to parallelize the processing of data from a Chinese e-commerce company. Experiment findings suggest that the technique is more accurate and efficient in detecting fraud in online e-commerce transactions, as well as scalable for big data processing to acquire real-time information.

The identification of graph anomalies is a common use for “graph neural networks (GNNs)”. Tang *et al*., 2022, take the first step towards analysing irregularities via the prism of the graph spectrum since choosing a customised spectral filter is one of the essential elements for GNN construction. The key finding is that the presence of anomalies causes the 'right-shift' phenomena, in which the spectral energy distribution concentrates more on high frequencies than on low frequencies. Here suggest the “Beta Wavelet Graph Neural Network (BWGNN)” in response to this phenomenon. In order to effectively manage the "right-shift" issue in anomalies, BWGNN does indeed have spectral and spatially localised band-pass filters. This example shows how BWGNN performs on four sizable datasets for anomaly identification.

Credit card fraud, when transactions are conducted without the knowledge of the legitimate user is one of the negative aspects of the digital age. The following goals are attained based on the analysis of several articles on credit card fraud that were published between 1994 and 2018: The many forms of credit card fraud have been discovered, and adaptive machine learning methods (AMLTs) have been researched along with their benefits and drawbacks in order to automatically identify these frauds. The many datasets that have been utilised in the literature have been examined and divided into genuine and synthesised datasets. The fraud detection system has been evaluated using a summary of the performance matrices and assessment criteria. The performance (sensitivity, specificity, and accuracy) of current machine learning algorithms in the domain of credit card fraud detection has also been thoroughly analysed and compared in this work. The results of this investigation which is made by Singh and Jain., 2019, clearly demonstrate the increased usage of supervised learning, card-not-present fraud, skimming fraud, and website cloning techniques. This study provides useful guidelines for future research in the area of credit card fraud detection while also noting the shortcomings of current fraud detection approaches.

The credit card is currently the most widely used form of payment for both online and offline transactions, enabling cashless shopping at all malls. It is the most practical method of doing an Internet transaction. Consequently, there is also an increase in the likelihood of fraudulent credit card transactions. Financial fraud crimes have dramatically expanded along with the rise in credit card usage, which has resulted in enormous losses for the banking sector. All banks must now have an effective fraud detection system in order to reduce these losses. The credit card fraud data sets are significantly unbalanced since the number of unauthorised transactions is substantially lower than the number of genuine transactions, which presents a significant difficulty for credit card fraud detection systems. In order to evaluate different classifiers, this research which is made by Warghade *et al.*, 2020, analyses several machine learning approaches using a variety of measures. The goal of this methodology is to better detect fraud rather than incorrectly label a legitimate transaction as fraudulent.

The everyday use of bank credit cards has been rising tremendously along with technological innovation. As a result, one of the new crimes that is rapidly expanding is the fraudulent use of credit cards by third parties. Because of this, research into identifying and thwarting these assaults is now underway. In this paper, Baratzadeh and Hasheminejad (2022) explore the difficulties in identifying fraudulent financial transactions and offer deep learning-based solutions. The transactions are reviewed and contrasted with other established fraud detection methods. The combination model of deep convolutional networks and short-term memory, which is trained using the aggregated data acquired from the generative adversarial network, exhibits the best performance, according to the results. The uneven class distribution problem will be addressed in this study using practical data, which is far more efficient than the conventional approaches. Additionally, it combines the deep convolutional network with the long short-term memory network to boost performance by combining the advantages of the two methods. The measurement of distance score and the comparable error rate are utilised for evaluating the models more transparently and precisely due to the inefficiency of the criteria for assessment such as accuracy in this application. In order to assess the effectiveness of the experiment, the conventional approaches and the suggested strategy are contrasted.

Table

Author	Title	Comments
Alarfaj., Malik., Khan., Almusallam., Ramzan, and Ahmed., 2022.	“Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms.”	The primary goal of this research study was to determine such frauds, which contain high-class data inequality, data accessibility, modifications in fraud nature, and increased false alarm rates.
Van Belle., Mitrović, and De Weerdt., 2020.	“Representation learning in graphs for credit card fraud detection. In Mining Data for Financial Applications:	In this research, the authors differentiate between three distinct methods: traditional network quality engineering,

	4th ECML PKDD Workshop, MIDAS 2019, Würzburg, Germany, September 16, 2019, Revised Selected Papers 4 (pp. 32-46). Springer International Publishing.”	an inductive term learning algorithm, and a transductive representative learner. Researchers indicate the supremacy of state-of-the-art miniature learning in charts over traditional chart component extraction utilising thorough practical examination of a real-world dataset.
Batool, and Byun., 2022.	“an ensemble architecture based on a deep learning model for click fraud detection in Pay-Per-click advertisement campaigns.”	In this paper, a preprocessing module is made to manage definite characteristics and imbalanced data in order to improve the consistency and dependability of click data.
Habibpour., Gharoun., Mehdipour., Tajally., Asgharnezhad., Shamsi., Khosravi, and Nahavandi., 2023.	“Uncertainty-aware credit card fraud detection using deep learning. Engineering Applications of Artificial Intelligence.”	In this paper, researchers explain via observed findings that the ensemble charges indecision associated with developed predictions more efficiently. Similarly, the authors demonstrate that the proposed “UQ” systems add more context to the actual predictions, enhancing the fraud prevention approach.
Tingfei., Guangquan, and Kuihua., 2020.	“Using variational auto encoding in credit card fraud detection.”	In this paper the researchers deliver a “variational automatic coding (VAE)”-based oversampling technique that blends classic “deep learning” methods. In an unstable dataset, the “VAE” method is employed to deliver a sizable number of additional instances from minority parties, which are thereafter utilised to train the category network.
Zhou., Sun., Fu., Wang., Hu, and Gao., 2021.	“ Internet financial fraud detection based on a distributed big data approach	This algorithm comprehends and describes the topological elements in the economic

	with node2vec.”	web graph as “low-dimensional dense vectors”, allowing deep neural networks to efficiently and intelligently organise and forecast data models from the “large-scale dataset”.
Zhang., Han., Xu, and Wang., 2021.	“HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences.”	The key findings of the research are to have organisational importance for credit card issuers, who can use the suggested procedure to fast determine fraudulent dealings, protect the interests of their clients, and cut down on fraud losses and regulatory expenses.
Zhou., Sun., Fu., Jiang, and Xue., 2019.	“A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics. Computers, Materials & Continua.”	This study proposes a uniquely scalable and comprehensive strategy for identifying fraudulent activity in online e-commerce transactions, with four logical modules that use big data analytics and machine learning algorithms to parallelize the processing of data from a Chinese e-commerce company.
Tang., Li., Gao, and Li., 2022.	“Rethinking graph neural networks for anomaly detection. In International Conference on Machine Learning.”	This article takes the first step towards analysing irregularities via the prism of the graph spectrum since choosing a customised spectral filter is one of the essential elements for GNN construction.
Singh, and Jain., 2019.	“An Empirical Study of AML Approach for Credit Card Fraud Detection—Financial Transactions. International Journal of Computers Communications & Control.”	The results of this investigation clearly demonstrate the increased usage of supervised learning, card-not-present fraud, skimming fraud, and website cloning techniques.

References

1. Alarfaj, F.K., Malik, I., Khan, H.U., Almusallam, N., Ramzan, M. and Ahmed, M., 2022. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, pp.39700-39715.
2. Audibert, J., Michiardi, P., Guyard, F., Marti, S. and Zuluaga, M.A., 2022. Do deep neural networks contribute to multivariate time series anomaly detection?. Pattern Recognition, 132, p.108945.
3. Baratzadeh, F. and Hasheminejad, S.M., 2022. Customer Behavior Analysis to Improve Detection of Fraudulent Transactions using Deep Learning. Journal of AI and Data Mining, 10(1), pp.87-101.
4. Batool, A. and Byun, Y.C., 2022. an ensemble architecture based on a deep learning model for click fraud detection in Pay-Per-click advertisement campaigns. IEEE Access, 10, pp.113410-113426.
5. Das, R. and Soylu, M., 2023. A key review on graph data science: The power of graphs in scientific studies. Chemometrics and Intelligent Laboratory Systems, p.104896.
6. El Orche, A. and Bahaj, M., 2020. Approach to combine an ontology-based on payment system with neural network for transaction fraud detection. Advances in Science, Technology and Engineering Systems Journal, 5(2), pp.551-560.
7. Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., Khosravi, A. and Nahavandi, S., 2023. Uncertainty-aware credit card fraud detection using deep learning. Engineering Applications of Artificial Intelligence, 123, p.106248.
8. Liu, N., Jian, S., Li, D., Zhang, Y., Lai, Z. and Xu, H., 2021. Hierarchical adaptive pooling by capturing high-order dependency for graph representation learning. IEEE Transactions on Knowledge and Data Engineering.
9. Munikoti, S., Agarwal, D., Das, L., Halappanavar, M. and Natarajan, B., 2023. Challenges and opportunities in deep reinforcement learning with graph neural networks: A comprehensive review of algorithms and applications. IEEE Transactions on Neural Networks and Learning Systems.
10. Nazir, S., Dickson, D.M. and Akram, M.U., 2023. Survey of explainable artificial intelligence techniques for biomedical imaging with deep neural networks. Computers in Biology and Medicine, p.106668.
11. Nicholls, J., Kuppa, A. and Le-Khac, N.A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. Ieee Access, 9, pp.163965-163986.
12. Ren, Y., 2021. Mining on Graphs: Graph Neural Network and Applications. The Florida State University.
13. Saeed, S., 2023. A customer-centric view of E-commerce security and privacy. Applied Sciences, 13(2), p.1020.
14. Singh, A. and Jain, A., 2019. An Empirical Study of AML Approach for Credit Card Fraud Detection—Financial Transactions. International Journal of Computers Communications & Control, 14(6), pp.670-690.
15. Tang, J., Li, J., Gao, Z. and Li, J., 2022, June. Rethinking graph neural networks for anomaly detection. In International Conference on Machine Learning (pp. 21076-21089). PMLR.
16. Tingfei, H., Guangquan, C. and Kuihua, H., 2020. Using variational auto encoding in credit card fraud detection. IEEE Access, 8, pp.149841-149853.
17. Van Belle, R., Mitrović, S. and De Weerdt, J., 2020. Representation learning in graphs for credit card fraud detection. In Mining Data for Financial Applications: 4th ECML

PKDD Workshop, MIDAS 2019, Würzburg, Germany, September 16, 2019, Revised Selected Papers 4 (pp. 32-46). Springer International Publishing.

18. Vatter, J., Mayer, R. and Jacobsen, H.A., 2023. The Evolution of Distributed Systems for Graph Neural Networks and their Origin in Graph Processing and Deep Learning: A Survey. ACM Computing Surveys.
19. Warghade, S., Desai, S. and Patil, V., 2020. Credit card fraud detection from the imbalanced dataset using machine learning algorithm. International Journal of Computer Trends and Technology, 68(3), pp.22-28.
20. Yang, Y., Cui, H. and Yang, C., 2022, December. Pre-train Graph Neural Networks for Brain Network Analysis. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 4993-4994). IEEE.
21. Zhang, X., Han, Y., Xu, W. and Wang, Q., 2021. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences, 557, pp.302-316.
22. Zhou, H., Sun, G., Fu, S., Jiang, W. and Xue, J., 2019. A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics. Computers, Materials & Continua, 60(1).
23. Zhou, H., Sun, G., Fu, S., Wang, L., Hu, J. and Gao, Y., 2021. Internet financial fraud detection based on a distributed big data approach with node2vec. *IEEE Access*, *9*, pp.43378-43386.