Software Engineering
2024, Vol. 10, No. 2, pp. 15-23
https://doi.org/10.11648/j.se.20231002.11

Research Article

Real-Time Big Data Analytics for Detecting Credit Card Fraud in Cyber Forensics Using Deep Learning Models

Chukwudum Chiemeka Prince[1, *], Ekwealor Oluchukwu Uzoamaka[2], Uchefuna Charles Ikenna[3], Ezuruka Evelyn Ogochukwu[2]

[1]Department of Forensic Science, Nnamdi Azikiwe University Awka, Awka, Nigeria
[2]Department of Computer Science, Nnamdi Azikiwe University Awka, Awka, Nigeria
[3]Department of Computer Science, Federal Polytechnic, Oko, Nigeria

Abstract

Real-time big data analysis and deep learning techniques for credit card fraud have been described, along with the effectiveness of a framework that has been proposed to improve the speed and accuracy of fraud detection. The framework implemented state-of-the-art technologies so that credit card transactions were monitored consistently, and dynamically developed algorithms recognized fraudulent activities. The work reflected that detection rates of deep learning models like Convolutional Neural Network (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) were higher and false positives negligible. Moreover, the analysis covered the circumstances in which the system operated in real-time interfaces and stressed that low latency and high speed in processing the many transaction records are crucial to the effective functioning of a system. The identified results highlighted the effectiveness of real-time analytics over the more conventional practices, presenting the opportunities these technologies could open for improved and more rapid fraud identification and preventing or addressing potential security threats. Specific recommendations were made concerning how financial institutions can manage big data analytics and deep learning models for fraud detection and prevention; a primary requirement was the establishment of effective data architecture, consistent training staff, etc. The implications of this research apply to cyber forensic investigators because real-time fraud detection mechanisms that stem from this research can result in more efficient identification and prosecution of fraud cases and, therefore, lower levels of loss and higher levels of security in the banking sector.

Keywords

Credit Card Fraud, Big Data Analytics, Deep Learning Models, Real-Time Detection, Fraud Detection Framework

1. Introduction

Every year, credit card fraud poses a severe challenge to global financial institutions, leading to enormous losses in billions of dollars. With the increasing number of e-transactions, this problem has been made worse. Fraud detection that can operate in real-time is now more vital than ever among financial institutions [55]. With consumers spending more and more on online credit card purchases, more secure measures must be implemented. Real-time fraud

*Corresponding author: pc.chiemeka@unizik.edu.ng (Chukwudum Chiemeka Prince)

Received: 6 November 2024; **Accepted:** 20 November 2024; **Published:** 25 December 2024

detection systems use big data analytics and deep learning algorithms to analyze transaction patterns for anomalies that may signal fraudulent activity [56]. Not only can these advanced tools sharpen the accuracy of fraud detection, but they also expedite reaction to potential threats at the same time. Consequently, they help consumers and financial institutions reduce damage caused by fraud [2]. Processing vast amounts of transaction data in real-time, including big data analytics in cyber forensics, is vital. Traditional methods for detecting fraud lag behind the pace of transactions [10]. Accordingly, it is faster and simpler to deal with transactions directly in real time through computer processing capabilities [45]. In this research, the author will explore the application of these new technologies in improving cyber forensic methods for fraud detection.

Problem Statement

The main difficulty in detecting credit card fraud is handling the daily transaction data generated. Current fraud detection systems often suffer from an inability to do real-time analysis, which results in increased vulnerabilities and the rate of fraudulent activities simultaneously [47]. Many current macro system frameworks are founded on historical data and preset rules, which may lead to fat rates of false positives and negatives, thus reducing the ability of such systems to stop fraud [31]. With the growth of clever swindlers, conventional detection techniques are becoming increasingly inadequate, and new solutions are being called for that can adapt to new threats [52]. This paper addresses these problems by investigating the potential for real-time big data analytics and deep learning models to enhance fraud detection capabilities.

Objectives of the Study

The key objectives are twofold. First, it seeks to probe the application of real-time big data analytics to credit card fraud detection, emphasizing high-tech integration for improving accuracy and efficiency [43]. Second, the study aims to build and test deep learning models explicitly tailored for fraud detection using cyber forensics, measuring their effectiveness vis-à-vis traditional methods [1]. By achieving these objectives, our research will contribute to ongoing efforts in fraud prevention in the financial sector.

Significance of the Study

Many stakeholders can benefit from the results of this study. Relevant people include financial institutions, law enforcement agencies, and cyber forensics experts. The research should make it known that extensive data analysis and deep learning are scientific methods to modernize fraud detection. Therefore, with traditional methods fading away, it is theoretically necessary to say that development methods to eliminate fraud from society will enjoy new prospects. Furthermore, the results of this study have some practical implications. Financial institutions attempting to install fraud-detection systems with higher predictive power will use loss numbers as evidence. How digital transactions take place is changing fast. Results from this study will also be valuable to any credit card company struggling with counterfeit products, which could ruin its business.

2. Literature Review

2.1. Credit Card Fraud

Various types of credit card fraud confront financial institutions and consumers with unique challenges. 'Card Not Present' fraud is common in which fraudsters steal credit card information and use it to buy things over the Internet or by phone without a physical card present [64]. Now it has become popular due to the rise in e-commerce, making it easier for a criminal to exploit in an online transaction system.

Skimming is a standard method. Items attached to ATMs or point-of-sale terminals capture the card's data as it is normally used in legitimate transactions [44, 33]. Phishing is another trick involving misleading emails or other illicit communications that induce individuals to divulge their credit card or other personal details--even passwords [33]. In cyber forensics, spotting and controlling fraud of these kinds is essential.

2.2. Role of Cyber Forensics in Investigating and Prosecuting Financial Crimes

Research has shown that cyber forensics plays a vital role in the tracing and prosecuting financial fraud, such as credit card fraud. Its process includes handling, protecting, examining, and presenting the digital information of criminality in a way that is admissible in court [27]. Using advanced tools and techniques, cyber forensic experts track fraudulent transactions, identify the unscrupulous criminals responsible, and bring back stolen money [12].

Forensic methods combined with police work contribute to discovering and arresting masterminds in credit card fraud. Moreover, information gathered by forensic investigations will lead to more robust security measures and improved fraud detection systems, preventing such occurrences from recurrin. As financial [7] crime occurs more and more often online, with each case, the importance of cyber forensics heightens, and thus, technology is advancing continuingly.

2.3. Approaches for Detecting Credit Card Fraud

There are currently two main approaches to detecting credit card theft: rule-based systems and traditional machine-learning models. Rule-based systems use preset conditions in the transaction database to signal potential fraudulent actions. For instance, payouts above a specific amount or multiple runs from different areas can all be captured [5]. However, these systems might work most fruitfully when applied appropriately and strictly; not adjusting flexibility may easily lead them [53] into high rates of false classification that make customers feel unhappy and produce operational

inefficiency. On the other hand, traditional machine learning models like decision trees and logistic regression have been used for fraud detection using transactional data modes [59]. These models can improve detection accuracy by utilizing historical data, but they still might face real-time processing and scaling problems. This is particularly likely given the burgeoning amount of data created by credit card transactions [52]. The changing environment in credit card kicking has led to a resounding demand for new recognition techniques that lure upon the large-activation aspect of curvature analysis and its problems, such as more sophisticated detection methods independent from crime control that emerged recently and involvement from modern AI applications.

3. Big Data Analytics in Cybersecurity

Big data analytics is the process of examining large and varied datasets characterized by volume, velocity, and variety to uncover hidden methods, correlations, or insights that may inform decision-making [26]. About cyber defense, the importance of extensive data analysis is even more significant. As cyber threats grow in sophistication, traditional security measures often fall far short of ideal, and it becomes necessary to deploy advanced analytical techniques for better threat detection and response capabilities [51]. Being able to deal with vast data streams quickly and analyze it in real time allows organizations to spot and head off potential hazards before they become real things. It is a proactive approach that is essential in contemporary cybersecurity settings, where threats evolve faster than ever and responses must be equally responsive.

3.1. Applications of Big Data Analytics in Real-Time Threat Detection and Fraud Prevention

Large data analysis plays a key part in real-time threat detection and fraud prevention for all trades. By utilizing machine learning algorithms and data mining techniques, companies may conduct transaction patterns, study user behaviors, and monitor network traffic to find conditions that differ from typical [42]. Financial institutions, for example, use extensive data analysis to keep an eye on dealings in real-time to spot suspicious activity and end it before it happens [15]. Cyber security teams use big data analytics to enhance their incident response procedures. With the fast spotting of intrusions now conceivable, they can also hit back more effectively [65]. When big data analytics are integrated with enterprise security best practices, detection rates improve, and the time to react to an incident is shortened. In addition to providing ultimate protection for sensitive info, it also enhances customer trust with services like these.

3.2. Challenges in Processing Large Datasets

Processing large datasets presents several difficulties despite its advantages. Proponents of big data argue that it simplifies and accelerates the process of data management, analysis, and storage. Nonetheless, latency, scalability, and data management are all problems associated with processing large datasets: If real-time or near-real-time data analysis is required, interference with the delivery and processing times of messages may impede timely decision-making and action [50]. Thus, the inability to scale becomes an issue that organizations need to solve. As the amount of data processed by today's information systems continues to grow toward stratospheric levels due to ever-greater quantities and types of digital information being created from multiple sources, organizations must ensure that their data processing systems can continue to support more and more data with equal or increased performance [34]. At the same time, good data management practice is essential to ensure that other information is free from corruption and can be securely retained. This is particularly important when discussing sensitive data in cybersecurity [57]. Realizing these benefits requires companies to implement rigorous data governance frameworks and make substantial investments in advanced technology.

4. Deep Learning Models for Fraud Detection

Deep learning methods are applied widely in fraud detection as artificial neural networks, convolutional neural networks, recurrent neural networks, and long short-term memory (LSTM) networks [9]. Unlike traditional algorithms, ANNs replicate human brains and learn to process information similarly, making them suitable for picking up complex patterns in large data samples. Among other things, CNNs are convenient tools for image and video analysis. At the same time, RNNs and LSTMs are particularly good at processing data sequences–making them ideal in the world where time is analyzed through series. In a fraud detection context, these deep learning models can extract features automatically from raw data, meaning that human intervention becomes less necessary to reduce the chances of being trapped by engineering errors and replace them with systems of higher precision.

Advantages of Deep Learning Over Traditional Machine Learning

Compared to traditional machine learning methods, another feature of deep learning is that it can identify very complex patterns and anomalies in large datasets. Traditional machine learning models often rely on fixed features, and this is perhaps the reason it could be difficult for ASA traffic managers to adapt to new forms of fraud as they emerge ("Industry 4.0 and Supply Chain Management. In contrast, the deep learning model can learn directly from raw data. This allows it a greater adaptability to ever-changing fraud patterns and increases its ability to detect fraud over time [56]. This adaptability is vital in the fast-melting world of cyber security,

where scammers are continually devising new ways to evade capture.

Applications of Deep Learning in Real-Time Fraud Detection and Cyber Forensics

Deep learning is being implemented in live fraud prevention and cyber forensics. Traditional banks now increasingly use deep-learning models to analyze transaction data in real-time. It enables them to detect fraudulent activities more accurately and quickly than before [8]. Furthermore, deep learning technology is used in cyber forensics to analyze digital evidence and find signs of cyber crimes. With the power of deep learning, organizations can significantly enhance their capacity for detecting fraud and raising their overall cyber security situational awareness.

5. Real-Time Analytics in Cyber Forensics

For successfully tracking down culprits in cyber forensics, real-time analytics has laid a solid foundation for perpetrators to be recognized and apprehended as soon they try their hand. Forensics teams can immediately ascertain whether related data is standard- and, therefore, what it represents. This speeds up the investigation and responses [22]. In the area of cybercrime mainly, taking this proactive approach is essential. Any delay in noticing fraud has already given fraudsters time to cause severe financial harm and start wrecking their target's reputation [20]. Incorporating real-time analytics into their operations also helps companies improve their incident response planning and makes it easier for them to repel cyber-attacks.

Use Cases of Real-Time Big Data Analytics in Other Cybersecurity Domains

In various applications outside fraud prevention, real-time big data analytics has now been successfully used in cybersecurity. For example, businesses possess real-time analytics to watch their networks for indications of trespass, allowing them to close down possible violations on the spot. This preserves valuable data from being interfered with further than necessary [51, 21]. Organizations can also employ real-time analytics for threat intelligence, which they use to gather and analyze probable threats and problematic spots in their security situation using information sources from across the web [16]. In these instances, the adaptability and potency of actual time analytics can be seen in reconstructing lines of defense.

6. Methodology

The methodology for developing a real-time credit card fraud detection system integrates big data analytics and deep learning models within a qualitative framework. The proposed framework encompasses a comprehensive system architecture designed for continuous credit card transaction monitoring, consisting of data ingestion, preprocessing, model training, and fraud detection. The data flow architecture facilitates real-time streaming of transaction data, ensuring immediate processing and analysis to identify fraudulent activities. Big data platforms like Apache Hadoop, Apache Spark, or Flink are selected for their ability to manage large-scale transactional data efficiently. Data collection methods involve gathering credit card transaction data from financial institutions or utilizing publicly available datasets, while preprocessing techniques such as cleaning, normalization, and feature extraction prepare the data for deep learning model training. The implementation of deep learning models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks, is central to the framework, with training conducted on historical transaction data using labeled datasets for supervised learning. Model tuning and optimization techniques enhance performance, focusing on hyperparameter adjustments and regularization methods to prevent overfitting. Evaluation metrics such as accuracy, precision, recall, F1-score, and area under the receiver operating characteristic (ROC) curve (AUC-ROC) are utilized to assess model effectiveness alongside real-time performance metrics like latency and detection speed. This qualitative approach ensures a thorough understanding of the strengths and limitations of various deep learning techniques in real-time credit card fraud detection.

7. Results and Discussion

The performance of deep learning models in credit card fraud detection is evaluated using key metrics such as accuracy, precision, recall, and F1-score. These metrics provide a comprehensive view of the model's effectiveness in identifying fraudulent transactions while minimizing false positives. A comparative analysis of different models, specifically Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks reveals distinct strengths and weaknesses in their ability to detect fraud. For instance, CNNs may excel in processing spatial data. At the same time, RNNs and LSTMs are better suited for sequential data analysis, making them particularly effective in capturing time-dependent patterns in transaction data [17, 66]. Insights from model results indicate the importance of detecting true positives, representing actual fraud cases, and minimizing false positives, where legitimate transactions are incorrectly flagged as fraudulent. This balance is crucial for maintaining customer trust and operational efficiency.

Figure 1. *Performance metrics—accuracy, precision, recall, and F1-score—of CNN, RNN, and LSTM models in credit card fraud detection.*

The graph above shows the performance metrics—accuracy, precision, recall, and F1-score—of CNN, RNN, and LSTM models in credit card fraud detection.
CNN: High accuracy and precision, suitable for spatial data processing.
RNN: Moderate across metrics, effective for time-series but with slightly lower precision.
LSTM: Superior in all metrics, demonstrating effectiveness in capturing time-dependent patterns, with the highest precision and recall rates.

Real-Time Big Data Analytics

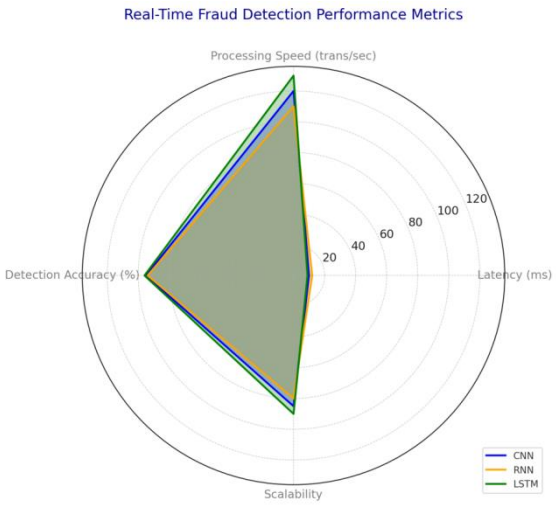

Figure 2. *Real-time fraud detection performance metrics—latency, processing speed, detection accuracy, and scalability—for CNN, RNN, and LSTM models.*

Latency and Processing Speed: LSTM achieves the lowest latency and highest processing speed, showing its robustness in real-time applications.
Detection Accuracy: LSTM and CNN perform well, with LSTM slightly leading.
Scalability: LSTM also demonstrates the highest scalability, which is beneficial for handling large data volumes.

The system performance assessment findings for real-time fraud detection show essential aspects like latency and throughput. Unlike traditional frameworks, this prominent data structure is capable of processing transactional data in large volumes while at the same time achieving the necessary level of accuracy in detecting fraud, which is essential for their timely detection. Real-time data processing is highly crucial in this case because any delay in analyzing data would result in severe losses and a negative impact on the reputation of financial institutions [13, 62]. As one of the core facets of big data, scalability, and parallel processing form the basis of the ability to manage the increasing burden of the data without a dramatic decline in the overall efficiency of the system. This capability is especially relevant to credit card transactions where the volume of data can be significant, thereby requiring flexible processing frameworks in response to increasing utilization [35].

Comparison with Traditional Methods

A comparison of deep learning models with conventional methods, including rule-based systems and conventional machine learning techniques, underlines the benefits of analyzing data in real time in fraud detection. Generally, conventional techniques depend on rules or past knowledge that may fail in dealing with new fraud schemes. On the other hand, deep learning models utilize sophisticated machine learning to process big data, and it also becomes possible for them to identify fraud much more quickly than traditional methods while cutting down on the time needed to respond to possible security threats [3]. The advantages of real-time analytics are

not only confined to detection but also serve as an enabler in stepping up the security level of financial institutions. However, applying all these techniques is challenging, as it involves computational costs, data imbalance, ethical issues, and data privacy and security [25, 37]. Solving these problems is crucial to achieving further deep learning and considerable data analytics potential for combating credit card fraud.

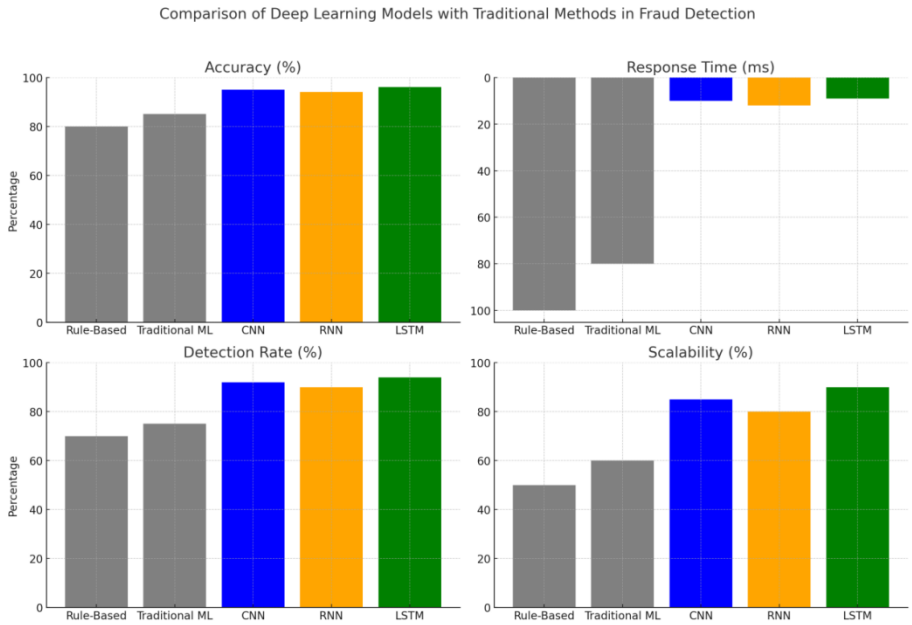

Figure 3. *Comparism of Deep learning Models with Traditional Methods of Fraud Detection*

Challenges and Limitations

Providing deep learning models in credit card fraud detection poses several issues and limitations. One major problem is computational overhead in training complex models of higher dimensions on large datasets that can overload resources and overtime. Moreover, imbalanced data is a significant problem in the credit card fraud detection problem since fraudulent transactions are relatively rare against the background of numerous legitimate ones, which can lead to a biassed model [38, 19]. This imbalance can be addressed by methods such as oversampling or undersampling, but the use of these methods complicates the situation. Data privacy and security ethical issues are also crucial because financial data is being worked on here. The requirement to adhere to the rules and the protection of customers' rights are among the main concerns of economic organizations. Moreover, including deep learning models in real-time big data platforms creates technical issues for the systems to be integrated and must be capable of accurately providing anti-fraud sentiment in real-time. These problems must be solved to implement further improvements in advanced fraud detection systems in the financial sector.

Implications for Cyber Forensics

The significance of real-time fraud detection for cyber forensic investigators is significant. Thus, these high-level systems help improve forensic activities' effectiveness when needed to analyze fraudulent transactions much faster. Real-time analysis means that investigators are better positioned to attend to occurrences in good time and, in the process, get vital evidence and control potential damage before it happens. This capability is most important in credit card fraud cases, where an early intervention can avoid additional losses and help prosecute the offenders. The general implications to financial institutions are developing advanced methods to combat fraud, protecting the institution's property, and promoting customers' transactions. With the emergence of new and continuously changing threats in the cybersphere, the real-time fraud detection system must be integrated to promote the cleanliness and safety of financial activities as well as shield consumers from the dangers of credit card fraud [4, 52].

8. Conclusion

In conclusion, experience based on applying real-time big data analytics and deep learning models for credit card fraud shows that there has been a remarkable improvement in the detection of credit card fraud. The specified framework combines these technologies to promote the efficiency of falsification identification by enabling financial institutions to respond to believed behaviors swiftly. Given the ability of deep learning models, the system can predict more sophisticated and previously unseen patterns in the transaction data, which results in higher predictive accuracy of actual fraud

cases with low false alarm rates. This shields the customers and over-enhances the security of the financial institutions in broad terms.

Abbreviations

ROC	Receiver Operating Characteristics
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Adelakun, B. (2024). Enhancing fraud detection in accounting through ai: techniques and case studies. Finance & Accounting Research Journal, 6(6), 978-999. https://doi.org/10.51594/farj.v6i6.1232

[2] Agarwal, S. and Usha, J. (2023). Detection of fraud card and data breaches in credit card transactions. International Journal of Science and Research Archive, 9(2), 576-582. https://doi.org/10.30574/ijsra.2023.9.2.0603

[3] Anai, S., Hisasue, J., Takaki, Y., & Hara, N. (2022). Deep learning models to predict fatal pneumonia using chest x-ray images. Canadian Respiratory Journal, 2022, 1-12. https://doi.org/10.1155/2022/8026580

[4] Angkurawaranon, S. (2023). A comparison of performance between a deep learning model with residents for localization and classification of intracranial hemorrhage. Scientific Reports, 13(1). https://doi.org/10.1038/s41598-023-37114-z

[5] Aquilanti, L., Santarelli, A., Mascitti, M., Procaccini, M., & Rappelli, G. (2020). Dental care access and the elderly: what is the role of teledentistry? a systematic review. International Journal of Environmental Research and Public Health, 17(23), 9053. https://doi.org/10.3390/ijerph17239053

[6] Ayinla, B. (2024). Utilizing data analytics for fraud detection in accounting: a review and case studies. International Journal of Science and Research Archive, 11(1), 1348-1363. https://doi.org/10.30574/ijsra.2024.11.1.0221

[7] Azimi, S., Wong, K., Lai, Y., Bourke, J., Junaid, M., Jones, J., … & Leonard, H. (2022). Dental procedures in children with or without intellectual disability and autism spectrum disorder in a hospital setting. Australian Dental Journal, 67(4), 328-339. https://doi.org/10.1111/adj.12927

[8] Bangui, H., Ge, M., Buhnová, B., & Trang, L. (2021). Towards faster big data analytics for anti‐jamming applications in vehicular ad‐hoc network. Transactions on Emerging Telecommunications Technologies, 32(10). https://doi.org/10.1002/ett.4280

[9] Bashir, M., Gill, A., & Beydoun, G. (2022). A reference architecture for iot-enabled smart buildings. Sn Computer Science, 3(6). https://doi.org/10.1007/s42979-022-01401-9

[10] Bhardwaj, S. and Gupta, S. (2022). Effects of feature selection with machine learning algorithms in detection of credit card fraud. International Journal of Engineering Research in Computer Science and Engineering, 9(7), 46-51. https://doi.org/10.36647/ijercse/09.07.art011

[11] Bousdekis, A., Papageorgiou, N., Magoutas, B., Apostolou, D., & Mentzas, G. (2020). Sensor-driven learning of time-dependent parameters for prescriptive analytics. Ieee Access, 1-1. https://doi.org/10.1109/access.2020.2994933

[12] Christian, B., George, A., Veginadu, P., Villarosa, A., Makino, Y., Kim, W., … & Mijares-Majini, M. (2023). Strategies to integrate oral health into primary care: a systematic review. BMJ Open, 13(7), e070622. https://doi.org/10.1136/bmjopen-2022-070622

[13] Do, L., Lee, H., Im, C., Park, J., Lim, H., & Park, I. (2022). Predicting underestimation of invasive cancer in patients with core-needle-biopsy-diagnosed ductal carcinoma in situ using deep learning algorithms. Tomography, 9(1), 1-11. https://doi.org/10.3390/tomography9010001

[14] Doshi, S., Desai, K., & Shukla, D. (2023). Comparative study of fraudulent activities and various fraud detection techniques. International Journal for Research in Applied Science and Engineering Technology, 11(8), 1140-1148. https://doi.org/10.22214/ijraset.2023.55308

[15] Empl, P. and Pernul, G. (2023). Digital-twin-based security analytics for the internet of things. Information, 14(2), 95. https://doi.org/10.3390/info14020095

[16] Enache, G. (2023). Logistics security in the era of big data, cloud computing and iot. Proceedings of the International Conference on Business Excellence, 17(1), 188-199. https://doi.org/10.2478/picbe-2023-0021

[17] Gao, G., Li, Y., Zhou, X., Xiang, X., Li, J., & Yin, S. (2023). Deep learning-based subseasonal to seasonal precipitation prediction in southwest china: algorithm comparison and sensitivity to input features. Earth and Planetary Physics, 7(4), 471-486. https://doi.org/10.26464/epp2023049

[18] Ghahfarokhi, A., Mansouri, T., Moghaddam, M., Bahrambeik, N., Yavari, R., & Sani, M. (2021). Credit card fraud detection using asexual reproduction optimization. Kybernetes, 51(9), 2852-2876. https://doi.org/10.1108/k-04-2021-0324

[19] Gülgün, O. and Erol, H. (2020). Classification performance comparisons of deep learning models in pneumonia diagnosis using chest x-ray images. Turkish Journal of Engineering, 4(3), 129-141. https://doi.org/10.31127/tuje.652358

[20] Guo, Y., Yang, Z., Feng, S., & Hu, J. (2018). Complex power system status monitoring and evaluation using big data platform and machine learning algorithms: a review and a case study. Complexity, 2018(1). https://doi.org/10.1155/2018/8496187

[21] Habeeb, R., Nasaruddin, F., Gani, A., Hashem, M., Ahmed, E., & Imran, M. (2019). Real-time big data processing for anomaly detection: a survey. International Journal of Information Management, 45, 289-307. https://doi.org/10.1016/j.ijinfomgt.2018.08.006

[22] Hart, M. (2023). Next-generation intrusion detection and prevention system performance in distributed big data network security architectures. International Journal of Advanced Computer Science and Applications, 14(9). https://doi.org/10.14569/ijacsa.2023.01409103

[23] Hlouli, F. (2023). Detecting fraudulent transactions using stacked autoencoder kernel elm optimized by the dandelion algorithm. Journal of Theoretical and Applied Electronic Commerce Research, 18(4), 2057-2076. https://doi.org/10.3390/jtaer18040103

[24] Hole, P. (2024). Fraud detection and prevention in e-commerce using decision tree algorithm. International Journal for Research in Applied Science and Engineering Technology, 12(4), 2187-2196. https://doi.org/10.22214/ijraset.2024.60307

[25] Hu, K., Deng, X., Han, L., Xiang, S., Xiong, B., & Pinhu, L. (2022). Development and validation of a predictive model for feeding intolerance in intensive care unit patients with sepsis. Saudi Journal of Gastroenterology, 28(1), 32. https://doi.org/10.4103/sjg.sjg_286_21

[26] Ieracitano, C., Adeel, A., Gogate, M., Dashtipour, K., Morabito, F., Larijani, H., … & Hussain, A. (2018). Statistical analysis driven optimized deep learning system for intrusion detection., 759-769. https://doi.org/10.1007/978-3-030-00563-4_74

[27] Johnson, V., Brondani, M., Bergmann, H., Grossman, S., & Donnelly, L. (2022). Dental service and resource needs during covid-19 among underserved populations. JDR Clinical & Translational Research, 7(3), 315-325. https://doi.org/10.1177/23800844221083965

[28] Kadam, D. (2024). Machine learning approaches to credit card fraud detection. International Journal for Research in Applied Science and Engineering Technology, 12(4), 2802-2807. https://doi.org/10.22214/ijraset.2024.60531

[29] Kellerton, T. and Smith, M. (2023). Healthcare analytics in non-profits: evidence from north america. Business & It, XIII(1), 160-171. https://doi.org/10.14311/bit.2023.01.18

[30] Kour, R. and Karim, R. (2020). Cybersecurity workforce in railway: its maturity and awareness. Journal of Quality in Maintenance Engineering, 27(3), 453-464. https://doi.org/10.1108/jqme-07-2020-0059

[31] Kumar, G. and Nalini, D. (2021). Accuracy analysis for logistic regression algorithm and random forest algorithm to detect frauds in mobile money transaction. Revista Gestão Inovação E Tecnologias, 11(4), 1228-1240. https://doi.org/10.47059/revistageintec.v11i4.2182

[32] Mahida, A. (2024). Enhancing fra1ud detection in real time using dataops on elastic platforms. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10(3), 118-125. https://doi.org/10.32628/cseit2410310

[33] Mahony, T. (2023). Dental clinicians' perceptions on the use of tele‐dentistry consultations during covid‐19 within public dental clinics in sydney, australia. Australian Dental Journal, 68(4), 282-293. https://doi.org/10.1111/adj.12979

[34] Megeid, N. (2022). The role of big data analytics in supply chain "3fs": financial reporting, financial decision making and financial performance "an applied study" 26(2), 207-268. https://doi.org/10.21608/atasu.2022.259858

[35] Moon, J. (2024). Frequency domain deep learning with non-invasive features for intraoperative hypotension prediction. Ieee Journal of Biomedical and Health Informatics, 28(10), 5718-5728. https://doi.org/10.1109/jbhi.2024.3403109

[36] N, P. (2024). Combined feature set with logistic regression model to detect credit card frauds in real time applications. Journal of Machine and Computing, 804-812. https://doi.org/10.53759/7669/jmc202404074

[37] Na, J., Lee, Y., Kim, T., Lee, H., Won, H., Ye, M., … & Kim, J. (2022). Utility of a deep learning model and a clinical model for predicting bleeding after endoscopic submucosal dissection in patients with early gastric cancer. World Journal of Gastroenterology, 28(24), 2721-2732. https://doi.org/10.3748/wjg.v28.i24.2721

[38] Nam, J., Sinn, D., Bae, J., Jang, E., Kim, J., & Jeong, S. (2020). Deep learning model for prediction of hepatocellular carcinoma in patients with hbv-related cirrhosis on antiviral therapy. Jhep Reports, 2(6), 100175. https://doi.org/10.1016/j.jhepr.2020.100175

[39] Nandi, A., Randhawa, K., Chua, H., Seera, M., & Lim, C. (2022). Credit card fraud detection using a hierarchical behavior-knowledge space model. Plos One, 17(1), e0260579. https://doi.org/10.1371/journal.pone.0260579

[40] Naufal, N. (2023). Strategic communication management: crafting a positive image for madrasah excellence. jemr, 2(2), 94-105. https://doi.org/10.61987/jemr.v2i2.243

[41] Nazir, I. (2023). Impact of machine learning in cybersecurity augmentation., 147-154. https://doi.org/10.48001/978-81-966500-9-4_12

[42] Odeyemi, O. (2024). Reviewing the role of ai in fraud detection and prevention in financial services. International Journal of Science and Research Archive, 11(1), 2101-2110. https://doi.org/10.30574/ijsra.2024.11.1.0279

[43] Oh, J., Lee, J., Schwarz, D., Ratcliffe, H., Markuns, J., & Hirschhorn, L. (2020). National response to covid-19 in the republic of korea and lessons learned for other countries. Health Systems & Reform, 6(1). https://doi.org/10.1080/23288604.2020.1753464

[44] Pan, E. (2024). Machine learning in financial transaction fraud detection and prevention. TEBMR, 5, 243-249. https://doi.org/10.62051/16r3aa10

[45] Pillay, K. and Merwe, A. (2021). A big data driven decision making model: a case of the south african banking sector. South African Computer Journal, 33(2). https://doi.org/10.18489/sacj.v33i2.928

[46] Pitsane, M., Mogale, H., & Rensburg, J. (2022). Improving accuracy of credit card fraud detection using supervised machine learning models and dimension reduction. ICONIC, 2022, 290-301. https://doi.org/10.59200/iconic.2022.032

[47] Qayoom, A. (2024). A novel approach for credit card fraud transaction detection using deep reinforcement learning scheme. Peerj Computer Science, 10, e1998. https://doi.org/10.7717/peerj-cs.1998

[48] Ramkumar, M. (2022). "credit card fraud" detection using data analytics a comparative analysis. JEMM, 8(1), 24-29. https://doi.org/10.46632/jemm/8/1/4

[49] Rizvi, M. (2023). Enhancing cybersecurity: the power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science, 10(5), 055-060. https://doi.org/10.22161/ijaers.105.8

[50] Saeed, S. (2023). Digital transformation and cybersecurity challenges for businesses resilience: issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

[51] Santana, D., Barbosa-Lima, R., & Andrade, A. (2023). Impact of the covid-19 pandemic on the performance of pediatricians and pediatric dentists in the brazilian unified health system. Revista Ci ências Em Sa úde, 13(2), 52-58. https://doi.org/10.21876/rcshci.v13i2.1419

[52] Sapitri, W. (2023). The impact of data augmentation techniques on the recognition of script images in deep learning models. Jurnal Online Informatika, 8(2), 169-176. https://doi.org/10.15575/join.v8i2.1073

[53] Sassite, F., Addou, M., & Barramou, F. (2022). A machine learning and multi-agent model to automate big data analytics in smart cities. International Journal of Advanced Computer Science and Applications, 13(7). https://doi.org/10.14569/ijacsa.2022.0130754

[54] Shoetan, P. (2024). Reviewing the role of big data analytics in financial fraud detection. Finance & Accounting Research Journal, 6(3), 384-394. https://doi.org/10.51594/farj.v6i3.899

[55] Sipayung, E., Yanti, H., & Setya, A. (2023). Impact of anti-fraud awareness, fraud detection procedures, and technology to fraud detection skill., 783-787. https://doi.org/10.2991/978-2-494069-49-7_132

[56] Souza, J., Leung, C., & Cuzzocrea, A. (2020). An innovative big data predictive analytics framework over hybrid big data sources with an application for disease analytics., 669-680. https://doi.org/10.1007/978-3-030-44041-1_59

[57] Spearin, T. (2024). Instructional strategies and challenges for implementing teledentistry in dental hygiene curricula: a qualitative study. Journal of Dental Education, 88(6), 777-785. https://doi.org/10.1002/jdd.13495

[58] Tantawi, M., Lam, W., Giraudeau, N., Virtanen, J., Matanhire, C., Chifamba, T., … & Foláyan, M. (2023). Teledentistry from research to practice: a tale of nineteen countries. Frontiers in Oral Health, 4. https://doi.org/10.3389/froh.2023.1188557

[59] Tewari, S. (2021). Necessity of data science for enhanced cybersecurity. International Journal of Data Science and Big Data Analytics, 1(1), 63-79. https://doi.org/10.51483/ijdsbda.1.1.2021.63-79

[60] Ullah, F. and Babar, M. (2019). Architectural tactics for big data cybersecurity analytics systems: a review. Journal of Systems and Software, 151, 81-118. https://doi.org/10.1016/j.jss.2019.01.051

[61] Wang, D., Hu, Y., Zhan, C., Zhang, Q., Wu, Y., & Ai, T. (2022). A nomogram based on radiomics signature and deep-learning signature for preoperative prediction of axillary lymph node metastasis in breast cancer. Frontiers in Oncology, 12. https://doi.org/10.3389/fonc.2022.940655

[62] Xu, F., Qin, Y., He, W., Huang, G., Lv, J., Xie, X., … & Tang, N. (2021). A deep transfer learning framework for the automated assessment of corneal inflammation on in vivo confocal microscopy images. Plos One, 16(6), e0252653. https://doi.org/10.1371/journal.pone.0252653

[63] Yulistiyono, A. (2024). Internal communication management strategy to increase office administration effectiveness. Journal La Sociale, 5(1), 13-20. https://doi.org/10.37899/journal-la-sociale.v5i1.1015

[64] Zayyad, M. (2022). Assessing the impact of big data analytics in the telecommunications sector. Journal of Applied Science Information and Computing, 3(2), 6-11. https://doi.org/10.59568/jasic-2022-3-2-02

[65] Zhang, J., Lu, H., Hou, J., Wang, Q., Yu, F., Zhong, C., … & Chen, S. (2023). Deep learning-based prediction of mandibular growth trend in children with anterior crossbite using cephalometric radiographs. BMC Oral Health, 23(1). https://doi.org/10.1186/s12903-023-02734-4

[66] Zhang, X., Xiang, D., Saripan, M., Du, D., Wu, Y., Wang, Z., … & Marhaban, M. (2023). Deep learning pet/ct ‐ based radiomics integrates clinical data: a feasibility study to distinguish between tuberculosis nodules and lung cancer. Thoracic Cancer, 14(19), 1802-1811. https://doi.org/10.1111/1759-7714.14924

[67] Zhang, Y., L ü, H., Lin, H., Qiao, X., & Zheng, H. (2022). The optimized anomaly detection models based on an approach of dealing with imbalanced dataset for credit card fraud detection. Mobile Information Systems, 2022, 1-10. https://doi.org/10.1155/2022/8027903