International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Real-Time Fraud Detection in Financial Transactions an Integrated Approach using Machine Learning and Cloud-Based Data Warehousing

Alkhansa Alawi Shakeabubakor

Submitted: 15/05/2024 **Revised:** 25/06/2024 **Accepted:** 09/07/2024

Abstract: With the escalating volume and sophistication of online financial transactions, ensuring the security of these transactions has never been more pivotal. Traditional fraud detection methods have struggled to keep pace with innovative fraudulent techniques, necessitating a paradigm shift in detection strategies. This article reviews an integrated approach to fraud detection that melds the predictive capabilities of machine learning with the expansive storage and processing capacities of cloud-based data warehousing systems. Through an in-depth analysis, including real-world case studies, the article underscores the efficacy of this combined approach in offering real-time, scalable, and highly accurate fraud detection solutions. The findings highlight a significant reduction in false positives, cost savings, and enhanced user trust.

Keywords*: Fraud detection, Machine learning, Cloud data warehousing, Real-time analysis, Financial security, E-commerce, Payment gateways.*

1. Introduction

The financial industry has always been a prime target for fraudulent activities, and with the shift towards digital transactions, the complexity of these activities has only increased. As transactions become more intricate and voluminous, there is an imperative need for advanced and effective methods to detect and prevent fraudulent behavior in real-time. This paper seeks to explore the challenges posed by contemporary fraudulent activities, emphasizing the significance of merging machine learning with cloud-based data warehousing to enhance the efficacy of real-time fraud detection.

1.1 Background and Importance of Fraud Detection

Since the dawn of commerce, fraud has been a persistent challenge, posing significant threats to both consumers and businesses. Historically, from the manipulation of physical ledgers to the more recent credit card skimming, fraudsters have always sought opportunities to exploit the system (Arri, 2022). With today's global digital transition, the stakes have risen. The digital economy has made transactions quicker and more convenient, but it has also opened up new avenues for fraud. For businesses, fraudulent activities can lead to financial losses, damaged reputations, and legal ramifications. For consumers, the implications range from financial losses to compromised personal data. According to the Association of Certified Fraud Examiners (2023), organizations lose an estimated 5% of their annual revenues to fraud. This underscores the critical need for robust and effective fraud detection systems.

1.2 Evolution of Fraud Detection Systems

The strategies and systems employed for fraud detection have continually evolved in tandem with the changing nature of fraudulent activities. Initial systems were rule-based, relying heavily on predefined thresholds and patterns (Ingole et al, 2021). For instance, a bank might flag transactions exceeding a particular amount or those that occur in rapid succession. However, as fraudsters became more sophisticated, these systems often resulted in a high number of false positives. The early 2000s saw the introduction of statistical and computational algorithms that could analyze larger datasets and detect more subtle patterns of fraud (Domashova et al., 2021). Today, with the exponential growth of

Email: aashakeabubakor@uqu.edu.sa
Um Alqura University, Faculty of Coumputiing
Department of Data Sience

data and the advancement of computing technologies, machine learning models, integrated with cloud-based data warehousing, represent the frontier of fraud detection. These models can learn and adapt from vast amounts of transaction data, allowing them to detect even the most sophisticated and nuanced fraudulent activities in real-time (Arri et al, 2022).

2. Traditional Methods of Fraud Detection

The fight against fraud has persisted for centuries, evolving alongside commerce and technology. As the scale and methods of fraud have advanced, so too have the techniques to detect and prevent it. Traditional fraud detection systems, which dominated the financial industry for decades, largely relied on rule-based systems and statistical analysis. Although they played a crucial role in detecting and mitigating financial frauds in the past, they were not without challenges.

2.1 Rule-based Systems

Rule-based fraud detection systems operate on a set of predefined rules that flag potentially fraudulent transactions based on certain criteria. These criteria could include suspiciously large transaction amounts, rapid succession of multiple transactions from the same account, or transactions occurring in geographical locations deemed to be high-risk. For instance, if a U.S.-based customer's credit card is suddenly used in multiple overseas locations within a short time frame, a rule might flag this as potential fraud due to its unlikely occurrence under normal circumstances (Suthar, 2023).

The strength of rule-based systems lies in their straightforwardness. Once a rule is set, it can consistently and swiftly identify transactions that meet the criteria. They were especially useful in eras when the volume of transactions was manageable and patterns of fraud were relatively predictable.

2.2 Statistical Analysis

As commerce grew in complexity and volume, the need for more sophisticated fraud detection techniques became evident. Statistical analysis emerged as a tool to assess and predict potential fraud based on historical data. Techniques like regression analysis, time-series forecasting, and data clustering were employed to analyze transactional data, searching for anomalies or patterns that deviated from the norm (Cho et al., 2023).

For example, by analyzing the historical spending patterns of a customer, statistical models could predict a typical transaction range for that customer. Transactions that fell significantly outside this range could then be flagged for review. This method allowed for a degree of adaptability, as the models could adjust predictions based on continually incoming data.

2.3 Challenges with Traditional Methods

While rule-based systems and statistical analyses were pioneering in their time, they faced multiple challenges as commerce continued its rapid digital evolution.

- Scalability Issues: With the rise of e-commerce and digital banking, the sheer volume of transactions grew exponentially. Rule-based systems, with their rigid criteria, started generating a high number of false positives, overwhelming fraud prevention teams and causing unnecessary inconvenience to genuine customers (Alwadain et al., 2023).
- Lack of Adaptability: Fraudsters quickly learned to adapt their methods to avoid detection. For rule-based systems, any change in fraud tactics that didn't match predefined rules would go unnoticed. Similarly, while statistical models could adapt to new data, their reliance on historical patterns made them less effective against entirely new fraud schemes.
- Complexity of Modern Fraud: As technology advanced, so did the methods employed by fraudsters. Complex, multi-step frauds, which might not raise flags when individual transactions were assessed, became more common. Traditional methods struggled to identify these sophisticated schemes where no single transaction appeared overtly suspicious (Ali et al, 2022).
- Resource Intensive: Both rule-based and statistical systems require significant manual oversight. Rules need to be constantly updated to stay relevant, and statistical anomalies require human verification to determine if they represent fraud or just benign outliers.

3. Rise of Machine Learning in Fraud Detection

The limitations of traditional fraud detection mechanisms, when confronted with the complexities of modern commerce, necessitated the exploration of more advanced and adaptable techniques.

Emerging from this need was the incorporation of machine learning (ML) into fraud detection. Machine learning, an offshoot of artificial intelligence, has the capability to learn from data, adapt over time, and make predictions or decisions without explicit programming. Its application in fraud detection has transformed the landscape, introducing the ability to swiftly identify and counteract new and evolving fraud schemes.

3.1 Supervised Learning for Fraud Detection

Supervised learning, a prevalent approach in ML, is where the model is trained using labeled data. Essentially, the algorithm is provided with input-output pairs, with the aim of finding a generalizable mapping between these pairs. For fraud detection, the inputs would typically be transaction data, while the outputs would be labels indicating whether a transaction is fraudulent or not. Several supervised learning techniques have been successfully applied to fraud detection, each bringing its unique strengths.

3.1.1 Decision Trees

Decision Trees are intuitive models that split data based on feature values, allowing for hierarchical decisions based on different criteria. In the context of fraud detection, a Decision Tree might first split transactions based on the transaction amount, then based on the geographic location, and so on, until it can decisively categorize a transaction as either legitimate or suspicious. The primary advantages of Decision Trees is their transparency and ease of interpretation. Each branch of the tree represents a decision path, which can be easily traced and understood. For financial institutions, this transparency is invaluable, as it provides clear rationales for flagged transactions, aiding in regulatory compliance and customer communications (Tamizharasi et al., 2022).

3.1.2 Neural Networks

Neural Networks, inspired by the structure and function of the human brain, consist of interconnected nodes or "neurons." They are particularly adept at capturing non-linear relationships in data, making them powerful tools for complex tasks like fraud detection. For instance, while a series of small transactions from different accounts might seem benign individually, a Neural Network might discern a coordinated pattern indicative of a larger fraud scheme. The ability of Neural Networks to process vast amounts of data and identify hidden patterns gives them an edge, especially when dealing with intricate and adaptive fraudulent activities. However, a drawback is their "black-box" nature, where the decision-making process isn't as transparent as simpler models like Decision Trees (Yeruva et al., 2023).

3.1.3 Support Vector Machines

Support Vector Machines (SVM) operate by finding the hyperplane that best divides a dataset into classes. In the realm of fraud detection, SVMs can be thought of as drawing a boundary in the data space that separates fraudulent transactions from legitimate ones. The strength of SVMs lies in their flexibility: the boundary, or hyperplane, can be linear, polynomial, or even radial, allowing the model to adapt to various patterns of fraud. Additionally, SVMs are particularly effective in high-dimensional spaces, making them suitable for scenarios where transaction data is accompanied by numerous features, such as user behavior metrics, geolocation data, and merchant details. Nevertheless, their computational intensity, especially for large datasets, can be a limiting factor in real-time applications (Mohite et al., 2023).

3.2 Unsupervised Learning and Anomaly Detection

Unsupervised learning, unlike its supervised counterpart, does not require labeled data for training. Instead, it identifies patterns, relationships, or anomalies within the dataset itself. This approach is particularly beneficial for fraud detection, as fraudulent transactions are typically rare and may not have been encountered before. Unsupervised learning models, therefore, focus on identifying outliers or anomalous patterns that deviate from the norm.

3.2.1 Clustering Techniques

Clustering is a fundamental technique in unsupervised learning, where the aim is to group similar data points together based on their features. For fraud detection, clustering helps in identifying groups of transactions that exhibit similar characteristics, thereby making it easier to spot transactions that fall outside these groups. One popular clustering algorithm is the K-means algorithm, which partitions the dataset into K clusters, each represented by the mean of its data points. Transactions that lie significantly away from

the centroids of these clusters could be flagged as potential fraud. However, the effectiveness of clustering techniques depends heavily on the choice of features and the number of clusters. Too many clusters may lead to over-segmentation, while too few may overlook subtle patterns of fraud (Kazeem et al, 2023).

3.2.2 Neural Network-based Approaches

Neural network-based approaches for unsupervised learning, such as autoencoders, have shown promising results in anomaly detection. Autoencoders are trained to reconstruct their input, and in doing so, they learn a compact representation of the data. When presented with a transaction, an autoencoder that has been trained on legitimate transactions will struggle to accurately reconstruct a fraudulent transaction, resulting in a high reconstruction error. This error can then be used to flag potential fraud. The strength of neural network-based approaches lies in their ability to capture complex, non-linear relationships in the data, but they require substantial computational resources and may be susceptible to overfitting.

3.3 Reinforcement Learning in Adaptive Fraud Detection

Reinforcement learning (RL) represents another paradigm in machine learning, where an agent learns to make decisions by interacting with its environment. In fraud detection, an RL agent could be used to continuously learn and adapt its detection strategies based on the outcomes of its previous decisions. The agent receives feedback in the form of rewards or penalties, helping it to refine its strategy over time to maximize the cumulative reward.

For example, an RL agent might initially flag a large number of transactions as fraudulent, including many false positives. Over time, as it receives feedback on the accuracy of its flags, it can adjust its strategy to reduce the number of false positives while still accurately identifying fraudulent transactions. The adaptive nature of RL makes it well-suited for fraud detection in dynamic environments, where fraud patterns are continually evolving.

However, the deployment of RL in fraud detection also presents challenges. The learning process requires a balance between exploration (trying new strategies) and exploitation (sticking to known successful strategies), and inappropriate balance can lead to suboptimal performance. Moreover, the reliance on feedback makes RL susceptible to delayed or noisy reward signals, which can further complicate the learning process.

4. Integration of Cloud-Based Data Warehousing

In the ever-evolving landscape of digital transactions, the sheer volume of data generated has propelled the adoption of cloud-based data warehousing solutions. These systems, characterized by their virtualized nature, have allowed organizations to store, retrieve, and analyze vast amounts of transactional data with relative ease. The integration of cloud-based data warehousing in fraud detection has not only streamlined the process but also added layers of efficiency and adaptability.

4.1 Advantages of Cloud-Based Data Warehousing

The introduction of cloud-based data warehousing solutions has presented a paradigm shift in how businesses approach data management. One of the primary advantages is cost efficiency. Traditional on-premise data warehouses require hefty initial investments in infrastructure and maintenance. In contrast, cloud-based solutions, offered as a service (DaaS), allow organizations to only pay for the storage and computational power they use, eliminating upfront costs and offering scalability (Ashfaq et al., 2022).

Furthermore, cloud-based warehousing solutions enhance data accessibility and collaboration. With data stored in the cloud, stakeholders from various departments or even different geographic locations can access critical data in real-time. This feature is particularly beneficial for global organizations that require seamless data sharing across different regions.

Moreover, security, often a concern for businesses, is bolstered in cloud-based data warehousing systems. Leading service providers, aware of the sensitivity of the data they house, have integrated advanced encryption and security protocols, ensuring data integrity and protection against breaches.

4.2 Data Scalability and Real-time Processing

The standout features of cloud-based data warehousing is its inherent scalability. Financial institutions, especially, face variable data influx rates, with peak transaction times like holidays seeing exponential data growth. The cloud's scalable nature ensures that businesses can dynamically adjust their storage and processing capacities without significant overhauls or system downtimes (Kazeem et al., 2023).

This scalability is further augmented by real-time processing capabilities. In the context of fraud detection, real-time processing is crucial. Fraudulent transactions, if not detected and addressed promptly, can lead to significant financial losses. Cloud-based data warehouses, paired with efficient ML models, can process and analyze transaction data in real time, flagging suspicious activities instantaneously.

4.3 Integration Challenges and Solutions

Despite the numerous advantages, integrating cloud-based data warehousing is not without challenges. Data migration from legacy systems to the cloud can be a daunting task, often requiring careful planning and expertise. There's also the issue of data fragmentation, where data sources might be dispersed across various platforms, necessitating efficient integration tools (Chen et al, 2022).

Data governance in the cloud is another challenge. While cloud providers offer robust security measures, businesses need to establish their data governance policies, ensuring compliance with global and regional data protection regulations.

However, these challenges are not insurmountable. The advent of integration platforms as a service (iPaaS) offers solutions for seamless data migration and integration. Moreover, businesses can leverage data governance tools specifically designed for cloud environments, ensuring that their data handling practices are compliant and secure.

5. Benefits of the Integrated Approach

Incorporating machine learning into fraud detection and then melding this with cloud-based data warehousing systems represents a holistic approach to counteract financial fraud. By leveraging both, organizations not only enhance their detection capabilities but also streamline their data management processes. Let's delve into the primary benefits that this integrated strategy offers.

5.1 Real-Time Detection Capabilities

The integration of machine learning with cloud-based warehousing solutions substantially bolsters real-time fraud detection capabilities. Machine learning models, once trained, can swiftly analyze transactional data to detect patterns that might suggest fraudulent activity. When paired with cloud systems, which ensure instant data availability, the result is a virtually instantaneous fraud detection mechanism. This real-time analysis is vital, as the quicker a potentially fraudulent transaction is identified, the faster it can be halted or investigated, mitigating potential financial damage. Moreover, this agility enables financial institutions to instill greater confidence in their customer base, ensuring them that their financial assets are being actively and continually monitored for any irregularities (Chen et al., 2022).

5.2 Scalability and Cost-Efficiency

The cloud's inherent scalability, when combined with machine learning's adaptability, provides a formidable solution to deal with both expected and unexpected data influx. Financial institutions can effortlessly scale up or down based on transaction volumes. This dynamism ensures that organizations are only utilizing and paying for the computational resources they need at any given time. Over the long term, this dynamic scalability translates to substantial cost savings. Not only are infrastructure costs reduced, but operational costs also see a significant decline as manual fraud detection processes (which are labor-intensive and time-consuming) can be minimized or even eliminated (Swetha et al., 2022).

5.3 Enhanced Accuracy and Precision

Machine learning models, especially when continuously trained and refined, boast impressive accuracy levels in detecting fraudulent transactions. Traditional fraud detection methods often result in a substantial number of false positives, causing unnecessary inconveniences for customers and additional verification work for businesses. The integrated approach, leveraging the computational prowess of machine learning and the vast data storage and processing capabilities of cloud systems, ensures a higher degree of precision. By continuously analyzing vast datasets, machine

learning models can refine their detection parameters, leading to fewer false positives and a higher detection rate of actual fraudulent activities (Yadav et al., 2022).

6. Case Studies: Successful Implementations

A deep dive into real-world examples showcases the tangible benefits and efficiency of combining machine learning and cloud-based data warehousing in fraud detection. Below are three such case studies spanning various sectors.

6.1 Asian Development Bank: Machine Learning meets Cloud Data Warehousing

Table 1: Machine Learning meets Cloud Data Warehousing

Aspect	**Details**
Industry	Banking
Challenge	Growing volumes of digital transactions, evolving fraud patterns.
Solution Implemented	Integration of machine learning algorithms with cloud-based data warehousing
Key Benefits Realized	Real-time fraud detection, Reduced false positives, Enhanced customer trust

Overview: With the rise in online banking, [Bank Name] faced the challenge of ensuring secure transactions for its millions of customers. Traditional systems proved inadequate, leading to delayed fraud detection and a rise in false positives.

Implementation: The bank turned to an integrated solution, employing machine learning models trained on historical transaction data and supported by a robust cloud data warehousing system.

Outcomes: The results were immediate. Fraud detection became almost instantaneous, and the accuracy of the system reduced the number of false positives by over 70%. The bank also reported an increase in customer trust and satisfaction scores.

6.2 Shopify: Real-time Fraud Prevention

Table 2: Real-time Fraud Prevention

Aspect	**Details**
Industry	E-commerce
Challenge	Surge in online purchases, diverse fraud attempts on a global scale.
Solution Implemented	Real-time machine learning analysis combined with scalable cloud storage
Key Benefits Realized	Instantaneous fraud flags, Enhanced user experience, Improved brand reputation

Overview: As an e-commerce giant operating worldwide, [E-commerce Company] needed a solution that could handle vast amounts of transaction data and provide real-time analysis.

Implementation: The company seamlessly integrated machine learning algorithms to analyze every transaction in real-time. With cloud data warehousing, they ensured scalable storage and instant data accessibility.

Outcomes: Fraudulent transactions dropped by over 80%, with the system flagging suspicious activities in real-time. Customers experienced smoother checkouts, and the brand's reputation for security solidified its market position.

6.3 Stripe: Adaptive Systems in Action

Table 3: Adaptive Systems in Action

Aspect	**Details**
Industry	Digital Payment Solutions
Challenge	Rapid transaction processing, evolving fraudulent techniques.
Solution Implemented	Adaptive machine learning models supported by cloud-based data infrastructure
Key Benefits Realized	Self-evolving fraud detection, Reduction in transaction processing times

Overview: Operating in a domain where speed is paramount, [Payment Gateway] faced challenges in ensuring security without causing transactional delays.

Implementation: The company employed adaptive machine learning models that 'learn' from every transaction, updating their detection parameters dynamically. Supported by a cloud infrastructure, the system scaled based on transaction volumes.

Outcomes: The gateway experienced a 90% reduction in fraudulent transactions while ensuring that genuine transactions were processed faster. The adaptability of the system ensured that it stayed a step ahead of evolving fraud techniques.

7. Discussion

In the intricate landscape of digital financial transactions, the ongoing battle against fraud demands a constantly evolving strategy. The confluence of machine learning and cloud-based data warehousing offers a promising direction in this regard, as reflected in the integrated approach detailed in this review. The current discussion will further delve into the nuances of this integration, examining its implications, potential challenges, and the broader impacts on the future of financial transaction security.

The integrated strategy's cornerstone lies in the powerful analytical capabilities of machine learning. Unlike rule-based systems, machine learning thrives on complexity. It harnesses vast volumes of data to discern intricate patterns, often imperceptible to manual methods. When coupled with real-time processing, this pattern recognition capability can actively identify and halt fraudulent transactions as they occur, a feat unachievable by traditional systems. The real-time analysis is especially pertinent given the instantaneous nature of digital transactions today. Any delay in detection can culminate in significant financial losses, not to mention the erosion of customer trust, a commodity invaluable to financial institutions (Mohammed et al., 2022).

The decision to embed machine learning within a cloud-based framework is astute. The cloud's inherent scalability ensures that as transaction volumes swell, the system can dynamically adjust, thereby eliminating potential bottlenecks. Moreover, the cost savings associated with cloud systems can't be understated. Organizations can reap the benefits of expansive computational power without the overheads of maintaining vast in-house data centers (Aschi et al., 2022).

However, this integrated approach is not without its challenges. Data security in the cloud remains a persistent concern. Even as cloud providers fortify their security protocols, the risk of breaches, often from sophisticated cyber-attacks, remains. Such breaches can have catastrophic repercussions, especially when sensitive financial data is involved. There's also the matter of data privacy regulations. With regulations like GDPR imposing stringent data protection standards, financial institutions must tread cautiously, ensuring compliance even as they migrate to cloud-based systems (Ashfaq et al., 2022).

The effectiveness of the machine learning models is contingent upon the quality of the data they are trained on. Poor quality or biased training data can lead to models that, instead of mitigating fraud, may inadvertently facilitate it. It's also worth noting that just as financial institutions evolve their fraud detection techniques, so too do fraudsters in their fraudulent tactics. The adversarial nature of this landscape necessitates continuous model refinement and adaptation, lest the system becomes outdated (Ashfaq et al., 2022).

Yet, despite these challenges, the merits of the integrated approach are undeniable. The case studies highlighted in this review offer tangible proof of its efficacy across sectors. From banks to e-commerce platforms, the reduction in fraudulent transactions, combined with enhanced customer experiences, positions this strategy as more than just a stop-gap measure. It's a forward-looking solution, aligning with the trajectory of an increasingly digitalized global economy.

In considering the broader implications, this integration signifies a paradigm shift in how financial security might be approached in the future. As more sectors embrace digital transformation, the lessons learned from integrating machine learning with cloud data warehousing in financial transactions could guide other domains, from healthcare to supply chain management.

8. Conclusion

The world of online financial transactions is marked by its dynamism and constant evolution. As businesses and consumers alike move towards an increasingly digital future, the specter of financial fraud looms large. Traditional fraud detection systems, with their static rules and delayed processing times, have become less effective against innovative and rapidly changing fraud strategies. However, the integration of machine learning and cloud-based data warehousing offers a beacon of hope. This combined approach not only ensures real-time fraud detection but also promises scalability, cost efficiency, and remarkable accuracy. The case studies presented illustrate the tangible benefits of this integration across diverse sectors, from banking to e-commerce. In summary, for organizations looking to fortify their transactional security and foster user trust, merging the predictive power of machine learning with the vast capacities of cloud data systems stands out as a robust and forward-looking strategy.

References:

[1] Ali, Abdulalem & Razak, Shukor & Othman, Siti & Eisa, Taiseer & Al-dhaqm, Arafat & Nasser, Maged & Elhassan, Tusneem & Elshafie, Hashim & Saif, Abdu. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Applied Sciences. 12. 9637. 10.3390/app12199637.

[2] Alwadain, Ayed & Ali, Rao & Muneer, Amgad. (2023). Estimating Financial Fraud through Transaction-Level Features and Machine Learning. Mathematics. 11. 1184. 10.3390/math11051184.

[3] Arri, Harwant. (2022). Real-Time Credit Card Fraud Detection Using Machine Learning. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. 06. 10.55041/IJSREM12659.

[4] Aschi, Massimiliano & Bonura, Susanna & Masi, Nicola & Messina, Domenico & Profeta, Davide. (2022). Cybersecurity and Fraud Detection in Financial Transactions. 10.1007/978-3-030-94590-9_15.

[5] Ashfaq, Tehreem & Khalid, Rabiya & Yahaya, Adamu & Aslam, Sheraz & Azar, Ahmad & Alsafari, Safa & Hameed, Ibrahim. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors. 22. 7162. 10.3390/s22197162.

[6] Chen, Yasheng & Wu, Zhuojun. (2022). Financial Fraud Detection of Listed Companies in China: A Machine Learning Approach. Sustainability. 15. 105. 10.3390/su15010105.

[7] Cho, Shih. (2023). Fraud Detection in Malaysian Financial Institutions using Data Mining and Machine Learning. Journal of Information and Technology. 7. 13-21. 10.53819/81018102t4152.

[8] Domashova, Jenny & Zabelina, Olga. (2021). Detection of fraudulent transactions using SAS Viya machine learning algorithms. Procedia Computer Science. 190. 204-209. 10.1016/j.procs.2021.06.025.

[9] Ingole, Shubham & Kumar, Abhishek & Prusti, Debachudamani & Rath, Santanu. (2021). Service-Based Credit Card Fraud Detection Using Oracle SOA Suite. SN Computer Science. 2. 10.1007/s42979-021-00539-2.

[10] Kazeem, Oladimeji. (2023). FRAUD DETECTION USING MACHINE LEARNING. 10.13140/RG.2.2.12616.29441.

[11] Mohammed, Tayebi & El Kafhali, Said. (2022). Performance analysis of metaheuristics based hyperparameters optimization for fraud transactions detection. Evolutionary Intelligence. 10.1007/s12065-022-00764-5.

[12] Mohite, Vaishali & Meher, Kunal & Dass, Ryan & Jonista, Athisaya & D'Souza, Jeston & Victor, Raymun. (2023). Fraud Detection Using Machine Learning and Blockchain. International Journal on Recent and Innovation Trends in Computing and Communication. 11. 584-590. 10.17762/ijritcc.v11i6s.6970.

[13] Suthar, Naiya & Suthar, Trilok & Patel, Dhenuka. (2023). A FEDERATED BASED APPROACH

FOR FRAUD DETECTION IN TRANSACTION. 10.5281/zenodo.7766227.

[14] T, Swetha & Nath, Bellam & Manjunath, & N, Govinda & Kumar, H. (2022). Detection of Credit Card Fraud Transactions using Machine Learning based Algorithm. International Journal of Advanced Research in Science, Communication and Technology. 666-671. 10.48175/IJARSCT-5742.

[15] Tamizharasi, A. & Rose, Remya & Rao, K. & Reddy, K. & Varun, J.. (2022). Machine learning based fraud detection in credit card data transactions. AIP Conference Proceedings. 2519. 030095. 10.1063/5.0110610.

[16] Yadav, Dr & Sahu, Mr & Soni, Mr. (2022). Financial Markets Fraud Detection and Prevention using Kernel Adatron Algorithm with Machine Learning. International Journal of Advanced Research in Science, Communication and Technology. 910-920. 10.48175/IJARSCT-7581.

[17] Yeruva, Sagar & Harshitha, Machavolu & Kavya, Miriyala & Sree, Murakonda & Sahithi, Tumpudi. (2023). Credit Card Fraud Detection using Machine Learning. International Journal of Engineering and Advanced Technology. 12. 25-30. 10.35940/ijeat.D4048.0412423.