Real-Time Behavioural Anomaly Detection in Digital Payments: A Supervised Learning Framework for Financial Transaction Fraud Identification

Dr. Seungjin Oh, Professor of Electrical Engineering, Pohang University of Science and Technology (POSTECH), South Korea

1. Introduction

Today's business environments primarily depend on electronic transactions, thereby increasing the urgency of a more powerful fraud detection regime. Research reveals some shocking facts regarding this evil trend. International markets frequently encounter several types of fraud and monetary losses, affecting financial institutions, businesses, and other societies. Most organizations suffer from damaging charges, data, and reputation. In the US, around six million fraudulent activities are reported annually. Attackers can conduct fraudulent activities, including identity fraud and credit card fraud, using various sources such as computer networks, the Internet, and mobile devices. Consequently, fraudulent activities could be reduced or controlled through the development of intelligent and robust fraud detection systems. The detection of illegal activities has developed into an essential and effective tool for creating safe, smart, and confident financial systems. The traditional system for detecting fraudulent activities, however, has so far been unable to satisfy the growing demands. Contrastingly, AI-based solutions enhance financial fraud detection activities and detect fraudulent activities efficiently and with high performance.

Recent technological advancements in AI, big data sharing, and machine learning enable advanced fraud detection technologies that are more intelligent than systems available for business fraud detection. The exponential development of AI in financial activities as a significant component of driverless wallets increased this review's scope to stand out in AI for detecting fraudulent activities. The identification of financial fraud is a challenging issue; distributed ledger technology, trade, law enforcement, and consensus are included. It is an emerging, developing, and thrilling topic, both according to the

search, social networks, keyword ranking, scientific data search trends, and the number of downloaded journey creditors. Nonetheless, most of the relevant studies and research are centered on statistical and deep learning. The goal of this report is to conduct a study to assess AI accuracy in fraudulent detection activities. Approaching AI technologies to evaluate the validity of detection results of activities.

1.1. Background and Significance

1.1.1. Criminal Evolutions: Economic function is a critical component in terms of causing fraud in the modern economy due to duality. The development of technology to support business processes has provided a great leap in positive economic activities for people. It certainly can make transactions easier, but on the negative side, the development of business processes utilizing this technology also increases the opportunity for financial crime to grow. This is the business of criminals with their financial mechanisms to further damage the conditions of a suffering economy. One of the most common frauds, which is currently growing, is based on a digital mechanism—theft of customer or third-party financial data; the impact of this has spread rapidly across the world. Another case is investment fraud by redeeming broker portfolios for the benefit of the employer and employees.

However, several elements have raised the importance of discussing this. First, the occurrence of money exchange fraud is closely related to the security of third-party funds, namely customers who have trusted their money to VAD in accordance with their financial arrangements. From this type of foreign exchange fraud, the customer may experience additional adverse effects such as loss of income, a criminal record, termination of work, or family disputes and divorce. Customers who have been victimized certainly want help from the bank to provide solutions in the form of guarantees for the obligations they have not carried out as a form of effective legal certainty. Second, money laundering is a crime that affects the international community to the detriment of the state, especially in terms of finance. In many countries, money laundering is considered a crime that harms the international community and the state in a broader sense due to various dangers. In systems where deposits are dominated by savings deposits and current accounts, efforts to prevent it are equally broad and deep.

1.2. Research Objectives

This study represents the design and development of new fraud detection systems in financial transactions, applied through the implementation of AI techniques. The aim is to highlight a linear and comparative study of the most competitive AI-based systems in the identification of possible external attacks based on large data related to real-world transactions. The detection of fraud in financial transactions is a global issue for credit card companies and financial institutions. The main goal of AI-based systems in the detection of fraudulent transactions is to identify operations that pose potential financial risk. With this research study, the intent is to evaluate the application of basic AI techniques and improve the performance of these approaches by adding two different components. System performance parameters are also evaluated through accuracy, precision, recall, F1-score, ROC-AUC, HTER, and CA evaluations. Finally, the research findings and scientific considerations related to the AI techniques are provided, as well as an overview of the whole scenario of microscopic AI technology application. The objectives of this research study are based on the analysis of the different existing theoretical aspects of AI for the detection of fraudulent operations and concern the proposal and experimental verification of four different AI-based systems. In addition to the purpose of highlighting an innovative development with respect to real case scenarios, the proposed research also aims at identifying critical issues still to be addressed. In accordance with the state of the art of business practices, the proposed research study arguments would provide interesting information for the potential stakeholders who are willing to adopt an AI-based fraud detection system in their context-aware situation of fraud detection.

2. Understanding Financial Fraud

Financial fraud is the deceitful means to acquire monetary or personal gains and, consequently, it is a dangerous menace to society. Fraud may be classified into insurance, banking, mortgage, credit card, e-commerce, and multiple other forms. From a transaction perspective, financial fraud is majorly segregated into two broad categories: banking fraud (for in-branch or transactions outside of the bank, such as demand drafts, pay orders, and checks on one side, and altered, washed, faded, counterfeit notes and forgeries on the other) and online transactions (credit card fraud, insurance fraud, internet fraud, auction fraud, and spam). A significant percentage of

businesses reported suffering from fraud, while a smaller percentage reported fraud in subsequent years, amounting to a substantial loss per annum.

In a survey, someone in the UK became a victim of these tactics every 15 seconds, and a large sum was lost to online banking fraud, amounting to an increase during the first half of the year due to various attacks. In India, instances of credit and debit card fraud increased significantly over 4 years. A considerable amount was lost to mobile credit card and debit card frauds, whereas forex trading accounted for a notable loss alone, and double the forex loss was reported through user IDs and password theft. Identity theft is no longer an old issue; online coerced debt write-offs are continuously raising alarms, as a significant percentage of all data breaches in India have been found to be financially motivated. Small businesses and financial institutions such as banks and credit card companies face a momentous challenge in relation to payment security on the Internet. Large-scale datasets are being fraudulently transacted by roving critical data, which is now offering itself as a tradeable asset. Banks adopt several measures, such as creating policies to study transaction history and conduct behavioral profiling, in order to observe irregular trends. However, with the massive rise in the volume and sophistication of financial fraud, the inadequacy of a rule-based system to detect the same is overthrown.

2.1. Types of Financial Fraud

With the development of the modern economy, financial fraud activities have also grown. According to the nature of the phenomenon, it can be initially divided into two main categories: consumer fraud and business fraud. From the point of view of the types of services offered, most financial frauds involve the following categories of financial risks: payment fraud, online banking fraud, fraud based on social benefits, investment fraud, and others. Credit card fraud is one of the most common types of electronic payment fraud. Out of the available products, credit cards are reported as a top priority in online payment services. Credit cards have a higher upper limit of electronic payment amounts than other payment methods, and they have no restrictions on the extraction of banknotes, so they are easily misused when they are lost or stolen. It can be argued that there are three main fraud methods: fraud by non-face value writing, theft by violence, and replication. Technological advances, especially the Internet, have provided fraudsters with easier access to financial institutions and new operations. The illegal

acquisition and use of another person's personal data in the electronic environment are generally known as identity theft. Phishing is a form of social engineering, characterized by an exploit in the user's psychology through fraudulent emails or websites in order to obtain the user's personal data. Based on the latest statistical reports on the most common types of financial fraud, it appears that the aforementioned types or classifications are subject to further clarification in order to ensure their neutrality and objectivity. Many papers consider that fraud, this more insidious form of deception, manifests itself in different subcategories, and that psychological factors identify a number of specific, characteristic strategies. It appears that fraudulent behavior can take a wide variety of forms, thus there are a number of subcategories and converging methods designed to isolate the victim from their goods and other material acquisitions, or to manipulate the behavior or state of mind of the defrauded individual, so as to obtain an advantage. Given the context, one can assume that an attempt at a clear, unitary, and complete definition of fraud is bound to encounter multiple difficulties. Thus, a scientific, doctrinal, or jurisprudential explanation will provide a more comprehensive perspective of these more generally accepted general points. In this specific context, the fraud suspect's ability to camouflage their actions is presented by the classical theory. This theory supports the idea that fraud is socially harmful and, in direct opposition to the neoclassical economic approach, is influenced by behavioral findings about the individual's economic decision-making process, also reflecting the money and behavioral methods of fraudsters. In the present paper, as a result of a vast literature review, we present the methods, trends, and patterns that have been utilized to model the detection and decision-making process of fraudulent financial transactions in order to explain the second approach. Fraud detection models can generally be built for different types of fraud, given the number of transactions present in the database. These models are built either satisfactorily or not, since we can only learn from transactions known to be frauds. Each of these fraudulent methods presents specific detection strategies.

2.2. Challenges in Detecting Fraudulent Transactions

Today's global financial systems increasingly run on digital transactions. All kinds of financial institutions process a huge number of transactions every day. This might be the reason why the global industry experienced a 19% increase in the value of fraud-related losses over the last five years. The need for fraud detection in a transaction is not just to

identify fraudulent actions post hoc, but also to deter fraudsters from attempting any malicious action by having the right deterrence systems in place and bringing in the deterrence at the right time before it allows criminals to find new ways of performing malicious transactions. The main aim of an effective fraud detection system is to assess the data within a short span of time while still aiming for a high level of accuracy without any intrusion on consumers' right to data privacy. Therefore, every transaction should be analyzed for fraudulent activity, ideally in real time. Ticking all the previous boxes with just raw data is not optimal in traditional neural networks or machine learning algorithms. When using machine learning models to forecast any sort of fraudulent actions, the historical data is not a guide as the nature of fraudulent transactions evolves. Another challenge faced by traditional machine learning models is the occurrence of false negatives that swing between 2% to 15%. Missing out on fraudulent cases hurts the trust and image of financial institutions, which further results in legal and regulatory consequences. When false positives are at play, it leads to abuse from genuine, fraud-free consumers. But it is the fear of missing out on a single fraudulent case that drives organizations towards stronger fraud management security measures.

3. AI and Deep Learning in Fraud Detection

Artificial intelligence (AI), particularly deep learning, has revolutionized the detection of fraud, being able to analyze a huge amount of transactional data much more quickly and efficiently than traditional systems, identifying the key patterns of fraud. Machine learning algorithms make it possible to analyze data, identify evolving behaviors and patterns of fraud, adapting in a dynamic way and requiring less human intervention. The use of deep learning in fraud detection systems offers the advantage of interpreting unstructured data, such as images and sound. It consists of several layers of processing units, called neurons, set up in a network that roughly mimics the human brain. As technology and techniques increase in complexity each year, fraudsters become more technologically advanced and cyberattacks become more frequent, making accurate fraud detection increasingly challenging. If institutions can predict a fraudulent transaction with a higher level of certainty in real-time, they can make decisions more effectively in order to reduce potential losses. AI-based processing systems transform the industry. Instead of defining if we implement AI-based systems for processing and storage, we could wonder how these systems could be implemented effectively and

offer a great advantage. Considering the current explosion of data, it has become essential for financial institutions to adopt AI algorithms to process data efficiently and make the best decision in real-time. The development of AI and deep learning is rapidly changing the situation by offering a variety of new techniques for prediction, fraud detection, and analysis of unstructured and large volumes of data. The integration of AI techniques that can process a large amount of data reliably and faster than traditional systems can become a promising ally for financial institutions to protect against new types of cyberattacks.

3.1. Overview of AI in Banking

In contemporary society, AI is increasing its influence in the banking industry. The continuous integration of AI components and techniques will shape a future where human service providers are not efficient. AI will be essential for risk assessment and optimization, hyper-personalization of customer experience, demand prediction, information processing, communication, and much more. From simple daily banking accounts to trading and portfolio management, both customers and corporations are encouraged to turn to AI applications. Banks have begun using AI in the areas of their business that benefit the most. To turn fragmented data into an important commitment of knowledge, banks approach customers using AI digital assistants. Currently, with the deep learning component of the AI megatrend, most banks are making headway. AI can predict the main parameters of businesses and assess a potential borrower's loan risk. Risk departments invest further in AI to optimize big data sets known as business information for new findings, transformations, and pattern recognition using machine learning. AI, without any manual processes or the introduction of human bias, guarantees efficiency and reduces human error. One more significant improvement of AI banking implementations includes fraud detection and anti-money laundering. The surveillance of transactions through behavioral analytics and AI can help banks combat international crime. The project showed major improvements in financial crime management techniques.

3.2. Deep Learning Techniques

Neural Networks: Progress in deep learning techniques has made neural networks successfully applicable to a wide range of fields including computer vision, natural language processing, and voice recognition, as well as in fraud detection. Neural

networks, also popularly known as deep learning models, are inspired by the human brain. With layers of non-linear processing units, neural networks are capable of converting complex input into output, an ability key to processing big data, high dimensionality, and mixed data. The systematic layers calculate the likelihood of patterns through node connections, and the output from one layer will be fed as input to the next layer, allowing interactions between multiple layers.

Advantages: Deep learning in fraud detection is especially advantageous in two ways: feature extraction and pattern recognition. First, unsupervised feature extraction can reduce the demands for domain knowledge and manual selection of variables significantly. Many big financial events are driven by multiple and various types of data, and conventional unsystematic feature engineering techniques are usually of limited effectiveness. Second, fraud patterns vary over time, which makes it difficult to infer existing and potential unseen fraud patterns based on ever-changing big data from dissimilar sources. As neural networks capture underlying and latent structures in different data, they become one of the most popular options in various fields. Furthermore, simple implementation and less need for domain knowledge become additional reasons to invest in this technique.

Deep Learning in Practice: Deep learning techniques are widely integrated into the core of most electronic payment systems. The cross-border B2B transfer service has recently been auctioned at a price due to its strong fraud prevention capability brought by the operation of a shared neural network. Its service relies on more than 100 banks and money transfer institutions, working in a similar way as Visa, especially in selling fraud detection services. Although traditional state detectors are widely used in various industries, many fraudsters are looking for assistance from the detection capability of neural network predictors. Financial stock auditors have also used tactics with spare cash to force fraudulent sales. Due to the association between verified cards and tactics in stock accounts, this type of neural network has been widely studied. As most tactics suffer from this verification, they tend to provide high-quality alternative tactics in the selection of tactics.

Necessary Training and Data Requirements: Although deep learning models exhibit high accuracy in many fields, some issues remain. More specifically, quality overfitting in out-of-sample fields can be lacking in generalization, and convergence may not

always occur. It also faces a challenge in strategy design: how to train and update the model, and how and when to use historical knowledge for rapid deployment. Since the neural network relies heavily on input data, the knowledge from the entire historical data learning sample is known and required for fraud payment technology. This neural network technology attempts to extract information from the learning sample to identify suspects and predict their fraud probability. Authorities must be updated frequently to track the changing patterns of the movement.

4. Implementing AI-Based Systems

First steps of building a successful system involve data collection and preprocessing. High-quality data prove to be one of the most crucial elements of a system. Based on the characteristic features and classification criteria, a database of transactions must be generated. The dataset is divided into specific time intervals and applied for the development phase. Afterward, significant functions can be developed in order to sense potentially fraudulent events. To generate trustworthy predictions, a plethora of AI-based methods has been developed. It is generally believed that a combination of these algorithms will produce the best detection results. The following phase focuses on training the detection procedure. Proper model assessment is crucial for AI systems. Its effectiveness has to be investigated as regards the value of mathematical functions, additional restrictions, or control curves.

If the system is controlled and evaluated, it can be implemented into the mainstream banking system. This can be difficult due to the required practical service connected with various money transfer methods and the massive compatibility problems. If all of these standards are satisfied, the developed system is controlled at a specific site. Necessary corrections are introduced to the system in order to increase its precision. In the financial market, fraudulent activities can constantly develop. The system should be continuously checked and updated with the developed new kinds of financial crime activities. If the AI detection system complies with the requirements of general and functional demands of the business, then compliance with national and international regulations and ethical and legal roles must be guaranteed in addition to the operational aspect.

4.1. Data Collection and Preprocessing

It is essential to collect high-quality, granular data to build effective AI-based fraud detection systems. Retail transactions from all customer devices should be documented in granular detail, reviewed by fraud investigation experts using sophisticated fraud management systems, and audited for accuracy through regular control procedures. Payment transaction logs may assist in the creation of datasets for machine learning and AI modeling that can be used to identify fraudulent activity. Many fraud management systems are capable of automatically capturing and documenting all customer points of contact.

In addition to internal transaction logs, financial institutions and merchants may consider obtaining and using external or third-party data feeds. In highly organized and digitized financial crime in which fraud accrues much more quickly, an external reference database has become a requirement. In addition to log data, reference databases may be used to provide contextual information about the fraud victim, payment instrument features, merchant reputation, and other information that can be useful in fraud identification. All such data should be disclosed, and its use and any validation or washing routines should be clearly spelled out for all relevant data and downstream machine learning modeling, auditing, and control functions of the organization from which external or third-party data is sought.

The data preprocessing step is the "block and tackle" portion of the AI fraud detection process that ensures the data quality in the model development dataset. It is an iterative cleaning and normalization effort to ensure all the log and third-party data points required and going into the AI model development are of high quality. This data preprocessing effort is foundational to building AI models that are later in the chain for fraud detection and refers the machine learning and AI modeling team back to the top three strategies for improving AI/ML model accuracy.

4.2. Model Development and Training

The identification of potential fraudulent transactions is a typical application case for AI-based systems. The features of this application case are explained in this subsection. The typical approaches for the development of models based on deep learning and artificial intelligence for fraud detection are presented. One of the most important steps in the development of AI systems based on deep learning and artificial intelligence for the

detection of transaction fraud is model deployment. Different types of models can be deployed in the system. Model training is one of the most crucial steps in the development of AI-based systems. There are two popular types of models for the development of AI-based systems: supervised learning and unsupervised learning. The dataset for the training of a supervised learning model should include tagged data, which consists of both normal transactions and those that are fraudulent. The dataset for the training of unsupervised learning models, unlike the supervised learning model, does not require the tag 'fraudulent' in the transaction dataset. The accuracy of the detection model depends on the quantity and accuracy of the data used for its training. The procedure to construct an optimal training dataset is an important task for the development of a fraud detection model and will be depicted in detail. Model development is composed of several steps. A common problem is the imbalance of the original dataset. The imbalance of the original dataset creates a bias in the constructed model; therefore, the construction of a balanced dataset is among the major tasks that should be solved when building a fraud detection model. The best model is chosen by the highest prediction rate; therefore, the construction of a balanced dataset should be taken into account. RP is another valuable tool for determining the model that has the highest power when balancing a dataset to construct several competing models. The development of a fraud detection model includes several steps, such as defining the identification metrics, selecting the correct structure of the model, and setting the detection model. The hyperparameters should be tuned to give the designed model performance and make the deep learning and artificial intelligence model a well-regulated one. The best hyperparameters should be carefully chosen when developing AI-based systems for fraudulent transaction detection. Model validation is another important step in the development of a fraud detection model. Each model that has been developed and trained should be verified to assess its design properties and suitability of the developed system. Overfitting is a problem that occurs when the AI-based system overfits the training dataset. The optimum performance of the model in practice appears to be unrelated to the problem caused by choosing the best AI-based system. The best result does not necessarily need to be the highest value. The AI-based system used in practice needs to be updated with fresh datasets to adjust the model since financial transactions involve change. Detection evaluation and training of the fraud detection model include a sequence of components. Valuable assistance will be provided to the

practitioner in this new complex environment for the development of an AI system based on this integrative approach. Mass or biased data used to train the model for fraud detection cannot be used to prepare the model if practitioners have even a small concern about the detection of fraudulent transactions. The results could be handled or aggregated if the model fails to be sized correctly, but they are only improved through the key price process of AI-based system training, which specifically compels practitioners to invest in this matter and take appropriate precautions. An AI model specifically trained for fraud detection that will be trained using balanced data will support professional fraudsters or auditors in decision-making and help avoid suffering or wasted costs.

4.3. Integration with Existing Banking Systems

Among all the factors listed in this subsection, this is perhaps the most critical to be aware of when considering the adoption of AI-based fraud detection systems. While all the technical and banking protection measures can be updated and modified as needed, it is the integration with already established banking systems that can pose real difficulties if not addressed appropriately. In terms of integration, the primary thing to note is the potential compatibility and interoperability with the organization's existing systems. Because of this, during the initiation of this process, a dialogue between the business and technical areas is necessary, as well as the inclusion of representatives from the organization's systems that work with the necessary bank protection. The first and most important part of the integration process is to ensure the system that is chosen will work seamlessly with standard institution management systems and will perform as expected.

Currently, there are many systems that offer interoperability through the use of Application Programming Interfaces or software that easily interacts with already established business intelligence software. Having integration that is clean, clear, and simple will help your team to be able to start on the platform without spending weeks in extra development. Software tools can be quite beneficial in these instances, like those that provide simple-to-use business rules and data plugs to quickly and easily connect different business systems. This facilitates a quick add-on solution to your existing banking system to start analyzing information sooner rather than later. At the same time, all the critical stakeholders in the banking process across all members need to be

part of the discussion process. In addition, it is most effective if it is an international discussion. It is important to have people who have experience working within such a system that uses the mechanism from the beginning. This most likely includes bank workers and software developers, and possible state regulatory authorities. By making the integration compatible for everyone, smooth and simple in each instance, you can realize a very advanced and sophisticated anti-fraud system that operates in real time.

5. Case Studies and Results

5.1 Initial Integration and Implementation Approaches In the following subsections, we outline a number of real-world case studies that detail AI-based fraudulent transaction systems across numerous financial institutions. Additionally, the organizations' approaches in their use of AI are provided. However, these in-depth cases are not intended to single out any specific financial institution; rather, they are shared to provide new insights and principles by detailing technical implementations of AI systems and the challenges faced during their initial integration. Accordingly, we provide a discussion of lessons learned through real, practical implementations. We begin the subsection by presenting a solution that integrates multi-agent AI for large-scale banks.

5.2 Case Studies and Results 5.2.1 A Multi-Agent AI Model for Big Banks A study identifying the delta between small community banks and the top 100 banks in terms of anti-money laundering compliance shows that for big banks, the average cost of the discrepancy between their own noncompliance and the regulatory bias is disproportionate to that of small banks. While these costs encompass spending by AML personnel and software, they also include regulatory fines for the big banks. In 2010, anti-fraud and AML spending averaged 3% of revenue for financial institutions, and the projected cost of fighting financial crime over the next seven years is estimated to surpass $20 billion. The rationale behind predictive data mining-based anti-fraud systems is that there are mathematical patterns in data that can give signals and indicators of fraud. These types of comparisons are useful to prove where AI technologies work well in closed applications, but we will emphasize methods for wider-range, real-time testing and evaluations in order to create unbiased study results.

5.2.2 A Study in a Mid-Sized Broker-Dealer A second study was performed in an organization that subcontracts clearing and settlement services from a large bank. The

participating organization has low direct access to financial data and a priori is second to last to know about a final transaction event. The target of the fraud system in 5.2.3 was greatly expanded to examine a very large data set including over 134 million stock transactions. Three hundred and sixty-three tool runs attempted to machine learn relationships between inputs and outputs in SIP-generated variables that could conclusively pre-verify or reject transactions as fraudulent. Results concerning a one to three-month window: 1. SVM classified customers as frosts or non-frosts. Classification is by the SVM prediction of the Time value as held out from the model. The model uses the Stocks, Amount, and Number Trade inputs to classify. This model is based on stock trade behavior, and fraudulent activities are hidden well enough that frauds don't show overwhelming withdrawal patterns. From all runs of the model, 113,473 transactions showed the tell-tale Time characteristics of fraud. 2. From the 113,473, the EMV period of fraud was computed as the tell-tale window where I really don't want to face any surprises and where he can definitely be indemnified. This leaves 6,419 transactions in a Time & Length hotlist. These transactions can be blocked en masse or individually investigated to identify any unindemnifiable chronic fraudsters. 3. Twenty-eight customers don't entirely fit the Time & Length telltale windows of fraud behavior. The question is raised at the broker-dealer: Which instead of war, which ones?

5.1. Real-World Applications of AI in Fraud Detection

Today, leading retailers, banks, insurance companies, and fintechs use AI-based systems to combat scams and fraud. Among them, MegaFon and Tinkoff reduced the false alarm rate from 10% to 1%. American Express uses AI to help prevent fraud, using unsupervised learning to directly detect instances of fraudulent charges. The introductory detection system became four times more precise in finding fraud and led to a 15% drop in the number of calls from clients questioning purchases. Nordea Bank adopted a solution for money laundering detection based on AI and reskilled risk department employees to improve the analysis of alerts. As a result, suspicious transaction detection accuracy improved by 18%. TNSC Bank, a subsidiary of the Michelin Group, along with Alphaliner, implemented an IT platform for operational risk management and fraud prevention in the banking business, which is built on AI. Société Générale Maroc used an automated anti-fraud system that uses Big Data and machine learning. British bank NatWest has implemented a new technology platform designed to prevent scams targeting older customers. VTB Bank used AI-based systems to prevent

fraud in mobile and electronic banking. SEB Bank has implemented a system with AI functions that protect customers from counterfeit documents. Bank of China New Zealand uses e-KYC, which analyzes user behavior and requests information about account opening transactions. Sberbank has been using machine learning technologies for anti-phishing protection since 2019. The AI model will know the limits and logic of user operations and, if necessary, notify them of the possible theft of their funds.

5.2. Performance Metrics and Evaluation

Updating the AI-Based Fraud Detection Systems explains that the success of an AI-based detection system depends on the performance of the applied model, but also on the evaluation of the selected system performance metrics. Thus, the frequent model evaluation serves for continuous model improvement and the timely updating of the existing detection algorithms. Finally, it is expected that AI-based models outperform the existing rule-based detection based on well-defined system performance parameters such as precision, recall, and F1-score. This subsection discusses the relevant performance points and possible challenges in flexible fraud detection systems and applicable techniques. The AI-based models are often used as models with the highest average recall and are indicated as well-performing systems. Future research studies should complement the use of already popular statistical and performance indicators with more detailed methods for interpretability and additionally defined techniques for the explanation of adopted decisions. The ever-increasing number of false positive predictions for a given alerting data acquisition cost induces more complex systems with an elevated threshold for model deployment. The rule-based models outperform the machine learning alternatives when the prediction may lead to legal consequences. Based on the types of electronic payment systems in banks, newer techniques could be implemented using the hybrid framework consisting of many diverse algorithms, not limited to the statistical and AI-based techniques. To improve, organizations may focus only on the systematically wrongly predicted instances for explanatory data-driven decisions rather than reasonable model performance parameters.

6. Future Direction

In this article, we are interested in framing the future directions concerning AI-based systems for fraudulent transaction detection. There are significant emerging trends in AI-based technologies of which financial institutions and practitioners need to be aware.

As such, focusing on a discussion on the future of AI specifically in the development of more advanced and autonomous detection systems is implicit.

There are significant advances occurring in the quantum mechanical aspects of AI technology, from the development of increased optimization and search technologies combined with advanced data analytic algorithms. As such, financial institutions should be prepared to benefit from collaboration with these providers. Moreover, discussing future developments in the field of AI ethics is important as advancements in AI-based technologies will require a review of the regulatory and ethical considerations in place. In the future, AI will become better equipped to make more complex judgments concerning fraudulent activity, hopefully fulfilling the call to create "human intelligence empowered by technology." Given the previous rise in the application of AI technologies within fraud prevention, accountholder behavioral analytics, and malware and data breaches, there is considerable scope for further research and development to address a range of application domains.

The deployment of autonomous or semi-autonomous AI technologies would greatly help in minimizing the need for using human intervention methods and would provide a powerful tool to further deter a range of fraudulent activities. In summary, more research and development is required to keep ahead of the game by designing systems that can consider vulnerabilities or cyberattacks that have not been previously seen, and possibly using automated sub-symbolic AI-based pattern recognition techniques for detection. For instance, further research in data science and the integration of semi-automated AI techniques such as network analysis, generative adversarial networks, transfer learning algorithms, and online learning techniques require significantly more attention to respond to such issues involved in literature and commercial systems deployed today.

7. Conclusion

In this paper, we have discussed technological systems based on AI for detecting fraudulent transactions while introducing the techniques and strategies implemented in these systems. We have also discussed several real-life scenarios and use of AI-based systems in the detection of fraudulent transactions. It was observed that AI technologies, specifically features of convolutional neural networks and machine learning techniques, were successfully applied to improve false positive and true positive rates thereby

enhancing the performance of the systems. Finally, we observed that the well-implemented AI model produces better results when the system is fully trained. Often, retail data networks and online transactions use the capabilities of reinforcement-learning mechanisms towards adopting a fraud-detection strategy for effective financial security. The inclusion of fraud detection systems has improved the accuracy of detecting online fraudulent transactions. Thus, there is a continual need to integrate the emerging technological systems, including artificial intelligence, to automate fraud-detection systems, reduce false-positive rates, and decrease financial losses. AI-based systems are well-developed to implement artificial experts in different areas in more sophisticated ways, for increased performance in fraud detection systems, and to thwart financial-sector fraudsters effectively. The financial sector should invest in developing new AI resources with the view that they will be used fraudulently. Fraudsters first innovate, then businesses adapt, and finally, legal systems are forced to respond. In some areas of security, AI is heavily armed as a solution to protect against fraud. For example, AI enables the military to predict the behavior of cyber attackers in warfare.