IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A COMPREHENSIVE SURVEY FOR ONLINE TRANSACTION FRAUDS DETECTION USING DEEP LEARNING

[1]Mohammed Ehtasaam, [2]Mohammed Arfath, [3]Mohammed Salman Makandar, [4]Mohammed Faizan

[1]Undergraduate Student, [2]Undergraduate Student, [3]Undergraduate Student, [4]Undergraduate Student
[1]Department of Computer Science and Engineering, [2]Department of Computer Science and Engineering, [3]Department of Computer Science and Engineering, [4]Department of Computer Science and Engineering
[1]HKBK College of Engineering, Bangalore, India, [2]HKBK College of Engineering, Bangalore, India, [3]HKBK College of Engineering, Bangalore, India, [4]HKBK College of Engineering, Bangalore, India

Abstract : Due to the increase in various threats and frauds emerging due to virtual Payment operations. Deep in the branch of Artificial Intelligence and Machine Learning it is widely exploited for inspecting and recognizing various multiplex patterns of vast repositories of data such as Online Transaction frauds or Illicit financial activities which can be employed using sophisticated neural systems and convolutional mechanisms. Other various Deep Learning techniques such as using Radial Basis Neural Networks and using Forward and Backward propagations for scanning the images. However, most of the online transaction frauds can be detected using various Machine learning techniques but recently Deep Learning has been considered elevation. The empirical findings and the analytical results can be made through aggregation of real life data sources.

IndexTerms **-Online Transaction Fraud Detection,Deep Learning Techniques,Radial Basis Neural Networks (RBNN).**

INTRODUCTION

Credit Card Scam Operations and Online fraud Transactions has been accelerated utterly due to the advancement of technologies and involvement of electronic innovations which have been a significant challenge and critical concern in modern world technology. To overcome these difficulties various Machine Learning and Deep Learning techniques have been taken place to minimize the fraud happened through various sectors such as Banking, E-Commerce websites, Healthcare and Medical for online Pharmacies, Education sectors such as E-Learning platform, Real Estate areas and even in food delivery applications etc.,Online transactions include theft, phishing, and unauthorized card access, which risks in the fiscal vulnerabilities of the modern world technologies. There are many global losses happening through online transactions in various sectors where the payments are fully digital through credit cards, upi payments such as google pay and phone pe which are third party applications in which act as intermediate between the user or the consumer and the Bank accounts, Banking apps which performs direct transactions, E-commerce platforms such as Amazon, eBay and Shopify.

Approximately 28.65, 28.50, and 32.34 billion dollars were lost due to credit card fraud in 2019, 2020, and 2021, respectively, according to the Nielsen report [1], [2], and [3].Cryptocurrency wallets like Bitcoin, Ethereum, and Bitcoin Cash are among the many other digital wallets that are rarely used in India. These digital wallets are not very popular in India, but they are frequently utilized in the US, New York, and other nations due to the numerous transaction scams that have occurred. Deep Learning developed a variety of artificial neurons, including biological neurons, to identify these types of frauds. The artificial neurons, which have input weights, activation functions, and outputs, were constructed using deep learning techniques.

Biological Neurons contain electrical impulses but the Artificial Neurons take numerical inputs from the models created which gets multiplied by weights. After performing using weighted inputs the Activation functions are used through which the final output for the model of an Deep Learning is determined and detected whether the transaction is fraud or legitimate. A neural network is a type of machine learning with a learning process that mimics the human brain and can be supervised or without supervision [4]. Multiple-layer neural networks, commonly known as deep learning (DL), are capable of gradually extracting higher-level data and analyzing intricate patterns with improved predictions. DL techniques have been applied to credit card data in order to detect fraudulent transactions. For instance, Mienye and Sun [5] created a method for detecting credit card fraud that uses a multilayer perceptron (MLP) as the base learner and a stacked ensemble of long short-term memory (LSTM) and gated recurrent unit (GRU) networks.There are different threshold levels in the activation functions that is used to sense and detect the various parameters of the datasets. Though, Machine Learning requires the attributes for the datasets from the user but this Deep Learning itself detects the models using forward and backward propagations and provides the attributes and parameters required.

BACKGROUND AND TERMINOLOGY

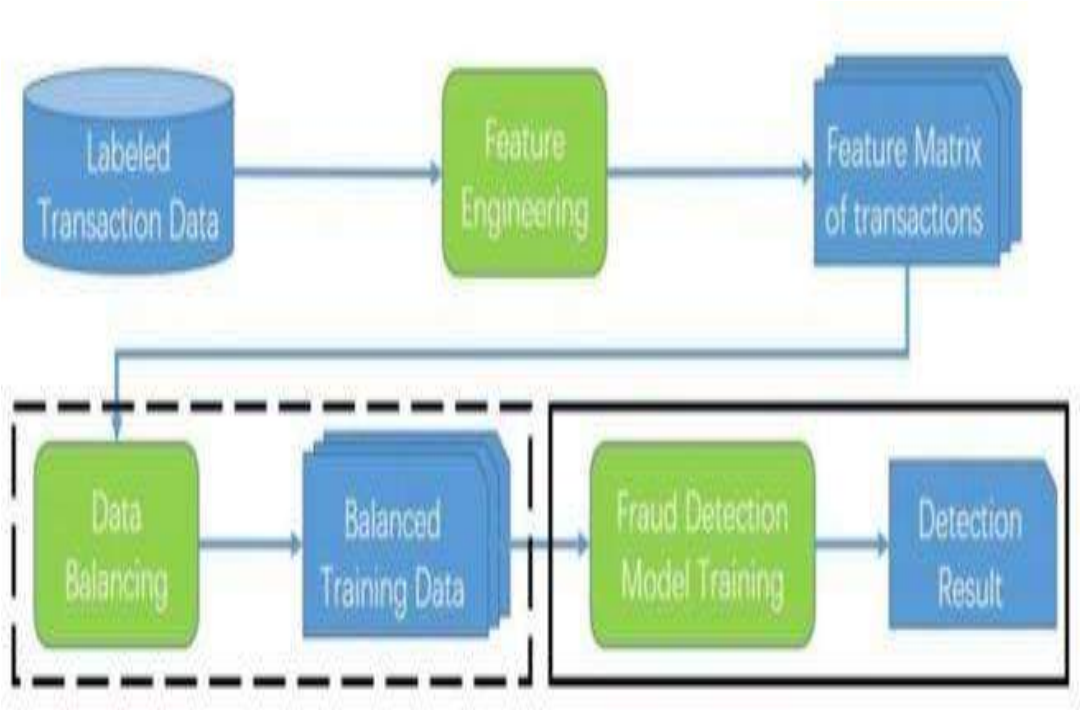


fig (1). background and terminology of a transaction data

Transaction frauds means any kind of financial loss of assets through individual or any public organizations which are trendy in todays market. Many kinds of frauds happen day-to-day through online payments by using third party applications and other through thefts and wire tranfers. For instance, in 2022, global credit card fraud losses amounted to an estimated **$32.04 billion**, with projections suggesting this number could rise to **$38.5 billion by 2027**.

Due the rapid rise of digital payments and through various websites and the transaction frauds have been rise. And other activities include online shopping through various websites and apps such as Flipkart, Amazon and various other foreign countries applications with give rise to transaction frauds through online payment by fetching the account number and bank details and personal details such as card number and the type of card being used and various other factors includes such as withdrawing or depositing large amount of data make the fraudsters become more smarter to hack the individuals account.

Meanwhile, apprehending credit card scammers often relies on the availability and quality of data. Law enforcement agencies and financial institutions utilize transactional data, along with advanced machine learning algorithms, to identify suspicious patterns indicative of fraud [6].

Deep Learning is the sub branch of Machine Learning uses various Artificial neurons with many layers and many hidden layers which has the ability to solve various complex datasets. A neural Network is a model inspired by the human brain which consists of interconnected Neurons. These Neurons process input data, applying weights and biases to identify relationships and make predictions. The convolutional neural network is a well-known deep learning architecture with wide applications in image recognition [7], [8], [9], achieving state- of-the-art performances, and has recently been applied in several cCCFD models [10], [11].

Additionally, the **complexity of modern financial fraud** schemes, including sophisticated attack methods like **synthetic identity fraud** or **botnet attacks**, often requires advanced techniques that can capture subtle variations in behavior. Deep learning models, by leveraging their ability to handle vast amounts of high-dimensional data, are better suited for such tasks than traditional approaches.

CLASSIFICATION OF LITERATURE

Supervised Learning

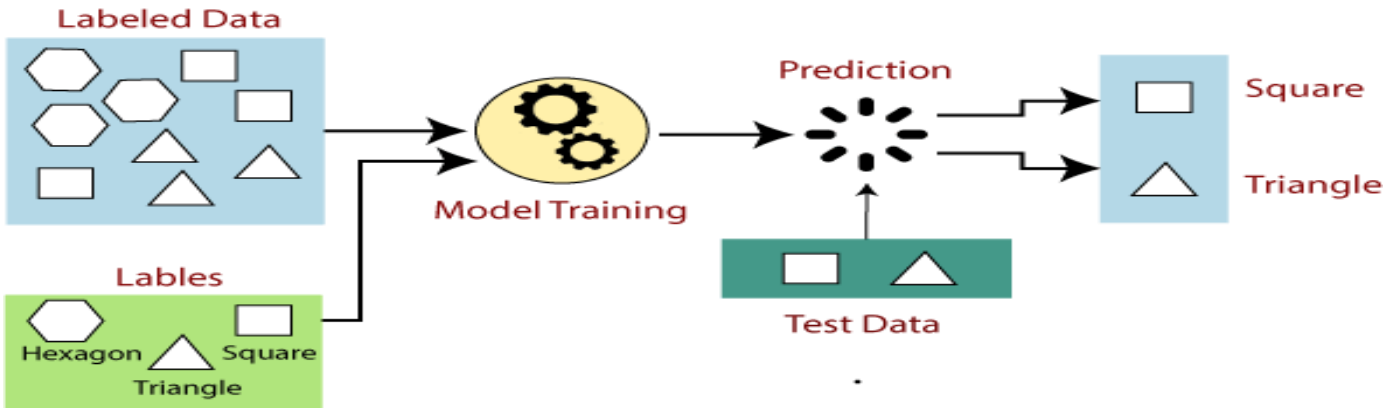


fig (2). supervised learning

ML algorithms fall into one of four categories: reinforcement learning, supervised, unsupervised, or semi-supervised [12]. The supervised learning (SL) approach is the most used machine learning technique for detecting credit card fraud [13]. Training an ML algorithm with a dataset in which every data point has a label is known as supervised learning. The data point's label specifies the particular class to which it belongs, such as fraud or non fraud. The link between the output labels (dependent variables) and the input characteristics (or independent variables) is often learned by SL approaches [14].

Deep learning techniques like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Supervised models provide higher accuracy predictions and up-to-date data for easy analysis. This Supervised learning is completely data dependency and relies on large datasets. If the data is not labelled then the performance and accuracy gained is very poor and even the fraud patterns accuracy gained is poor. They are even evaluated using metrics like precision and recall. Supervised models can be deployed for real-time fraud detection in live transaction systems, offering immediate insights to prevent ongoing fraudulent activities. Since fraudulent transactions are much rarer than legitimate ones, supervised models can become biased toward the majority class, leading to poor performance in fraud detection unless proper techniques (e.g., **resampling**) are applied.

Unsupervised Learning

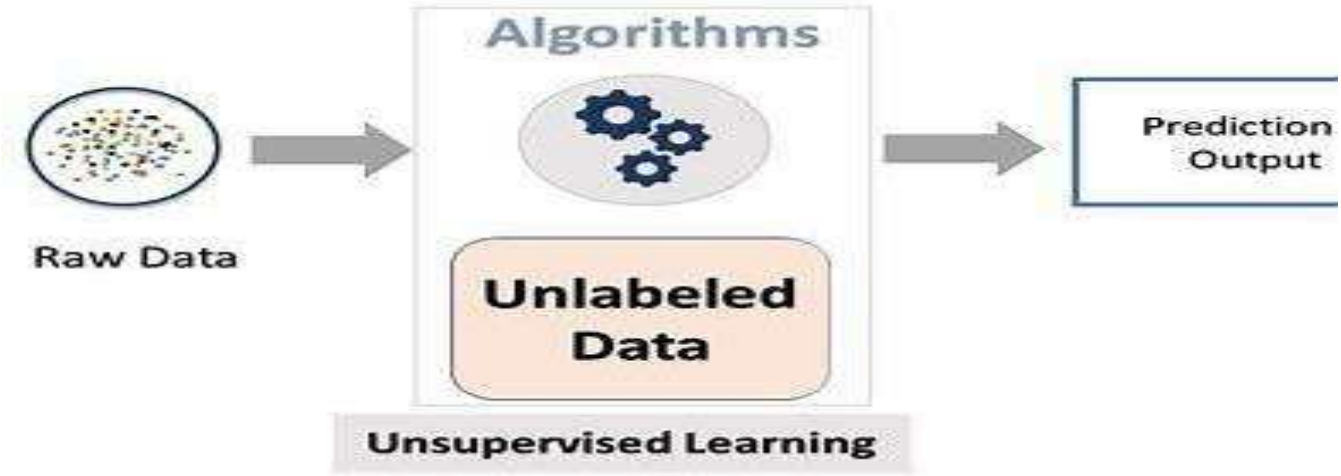
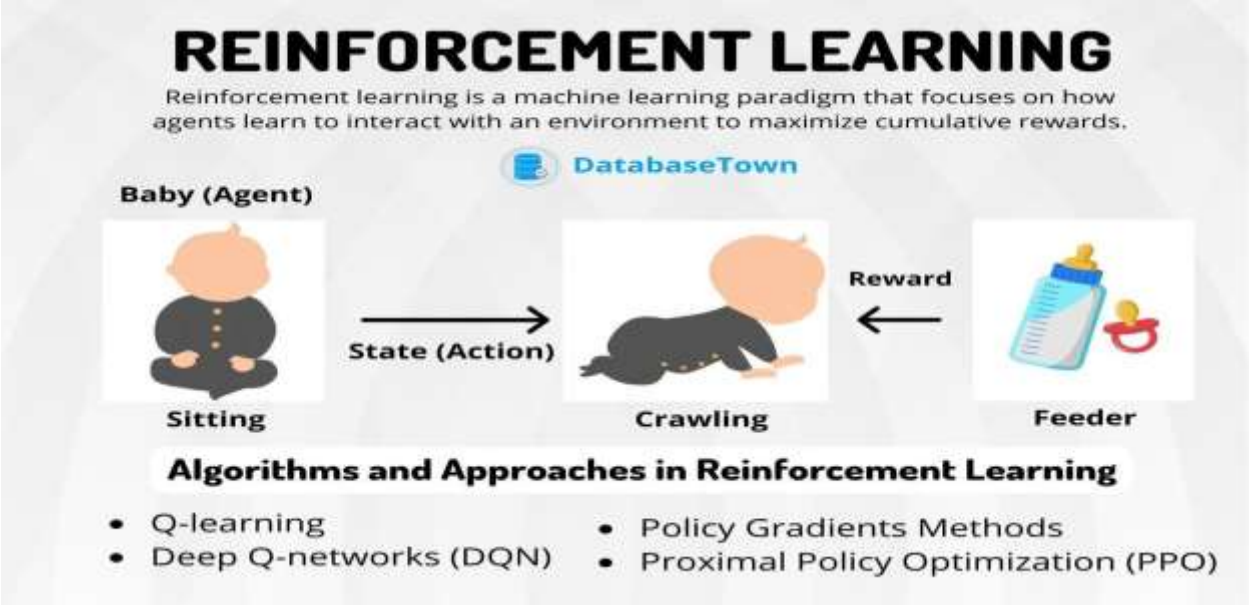


fig (3). unsupervised learning

The unsupervised learning technique is opposite to supervised learning technique in which the neural networks contain unlabelled datasets. the common algorithms used in these unsupervised techniques are K-means clustering, Convolutional Neural Networks, Linear Regression. The performance and accuracy gained by this unsupervised learning technique is very complex compared to supervised learning model as there are no predefined labels. As there no labels the accuracy of the model is indirectly measured by clustering and various clustering algorithms. The performance of these models is measured using Dimensionality reductions such as Principal Component Analysis.

The algorithms made for this model are very complex as the machine should recognise based on the patterns and various other patterns and complex datasets to identify the online transaction frauds. The machine should be capable to identify the frauds using various. But comparing this model with the unsupervised learning model the accuracy gained is poor than supervised learning models and algorithms.

Reinforced Learning



fig(4).reinforcement learning

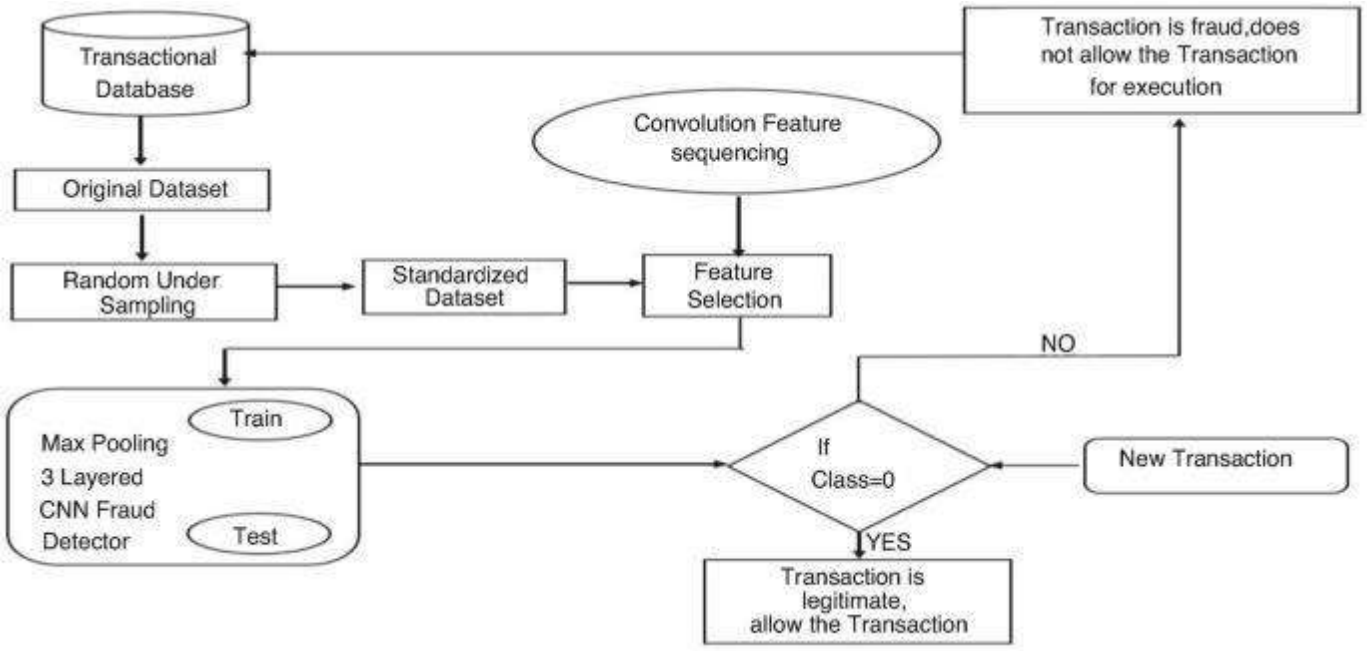
Reinforcement learning (RL) uses a dynamic, adaptive approach to improve fraud detection. By interacting with its environment, an RL system learns to take actions that maximize the accuracy of detecting fraud while minimizing false positives. While deep learning models are great at spotting patterns in large datasets, they typically require labelled data (e.g., marking transactions as fraudulent or legitimate) and rely on supervised learning. In contrast, reinforcement learning is more flexible, enabling systems to continuously adjust and improve as fraud tactics evolve over time.

What sets reinforcement learning apart from traditional machine learning is its focus on an "agent" that interacts with its environment and learns through feedback, which comes in the form of rewards or penalties. In fraud detection, for example, the RL agent might flag a transaction as potentially fraudulent and then receive feedback on whether that decision was correct. Over time, the system refines its strategies to make better, more accurate predictions.

DETAILED REVIEW OF LITERATURE

Supervised Learning in Transaction Fraud Detection

Neural networks have been shown in numerous studies to be capable of detecting fraudulent transactions in intricate credit card data [14], [15]. A neural network is a kind of machine learning that may be either supervised or unsupervised and has a learning process that resembles the human brain [16]. Neural networks, on the other hand, are made up of weighted connections between neurons. By adding up its weighted inputs, the neuron transforms its input into a single output using a non-linear activation function [15].Supervised learning techniques are widely used in credit card fraud detection because they can learn from past transaction data that is already labeled as either fraudulent or legitimate. This allows the system to recognize patterns that distinguish normal transactions from potentially suspicious ones. By training on these labeled examples, the model becomes better at identifying fraud in real-time, even when faced with new, unseen transactions. Essentially, supervised learning provides the ability to predict future fraud based on what has been observed in the past, making it a powerful tool for detecting unusual activity.



fig(5). flow chart of a transaction fraud detection

One of the techniques used in fraud detection is "convolutional neural networks (CNNs). While CNNs are more commonly associated with image recognition,they can also be applied to transactional data to spot hidden patterns. In a study by Zhang et al. (2022), CNNs were used to analyze the relationships between different features of transactions—like amounts, locations, and times—which could indicate fraudulent behavior. CNNs are good at picking up on these complex patterns, leading to high accuracy in detecting fraud. However, the downside is that CNNs require a lot of computational power, meaning they might not be practical for systems with limited resources or for applications that need to process transactions in real time.

Another approach involves recurrent neural networks (RNNs), which are particularly useful for analyzing sequences of data. This makes them a natural fit for fraud detection, where the order of transactions matters. Fraudulent activity often follows a sequence or pattern over time—such as a sudden spike in spending or the use of a credit card in several different locations within a short window. RNNs, and specifically long short-term memory (LSTM) units, are designed to track these types of sequential patterns. Chen et al. (2022) demonstrated that RNNs with LSTM units can better capture the relationships between transactions over time, improving fraud detection accuracy. The challenge with RNNs, however, is that they require large amounts of labeled data to train on, which can be a limitation in cases where fraud is rare or where labeled data is scarce.

Then there are Feedforward Neural Networks (FNNs), which are simpler models compared to CNNs and RNNs but can still be effective in fraud detection, especially when trained on carefully selected features, such as transaction amounts and the frequency of purchases. Liu et al. (2021) showed that FNNs can classify transactions as fraudulent or legitimate when given the right data. While FNNs are easier to implement and more computationally efficient, they don't capture the temporal relationships between transactions as well as RNNs do. This means that FNNs might miss fraud patterns that unfold over time, like a string of small transactions that add up to something suspicious.

In the end, each supervised learning method— whether it’s CNNs, RNNs, or FNNs—has its strengths and limitations. CNNs are excellent for detecting complex patterns but require heavy computational resources. RNNs, with their ability to analyze sequences of transactions, are great for spotting fraud that develops over time, but they depend on having lots of labeled data. FNNs are simpler and more efficient but aren't as

effective at detecting fraud that involves time-based patterns. All of these models rely on high-quality labeled data to train, and their success in detecting fraud ultimately depends on the richness and variety of that data, as well as the complexity of the fraud behaviors they're trying to identify .

Unsupervised Learning Techniques

Unsupervised learning techniques are gaining traction in fraud detection because they can find unusual patterns or anomalies in data without needing labeled examples of fraud. This makes them particularly useful for identifying new types of fraud that might not have been seen before, or even fraud that has evolved in response to existing detection systems.

One of the key unsupervised methods used is autoencoders, which are a type of neural network designed to learn the normal behavior of transactions. The way it works is simple: the autoencoder is trained on legitimate transaction data and learns to "compress" and then "reconstruct" this normal pattern. When a new transaction deviates from this reconstructed pattern, it's flagged as a potential fraud. Gupta et al. (2024) used this approach to detect fraud by identifying transactions that don't fit the usual patterns. An autoencoder is a genuine neural network, according to Raghavan [16]. Additionally, an autoencoder can encrypt data in the same manner that it decrypts it. This approach is effective in identifying irregularities, but it does need some fine-tuning.Without careful adjustments, the model might end up flagging too many legitimate transactions as fraud, which can create unnecessary alarms and increase operational costs. The trick is finding the right balance between catching fraud and minimizing false positives.

Another useful unsupervised technique is clustering, where transactions are grouped based on their similarities, like spending habits, transaction amounts, or geographic locations. Senator et al. used unsupervised clustering algorithms to detect money laundering [17]. K- means and DBSCAN are common clustering algorithms used for this purpose. The idea is that fraudulent transactions might form distinct clusters that don't align with the typical behavior of legitimate transactions. Zhao and Singh (2021) applied this technique to group transactions and identify clusters of fraudulent activity. Clustering is powerful because it can identify patterns in data that aren't immediately obvious. However, the downside is that it can struggle when dealing with very large datasets. As the volume of transactions grows, clustering can become slow and less effective. For example, K-means requires the number of clusters to be pre-defined, which can be tricky when fraud patterns are constantly changing. Similarly, DBSCAN might have difficulty handling datasets with varying levels of transaction density, making it harder to spot fraud when the data isn't neatly grouped.

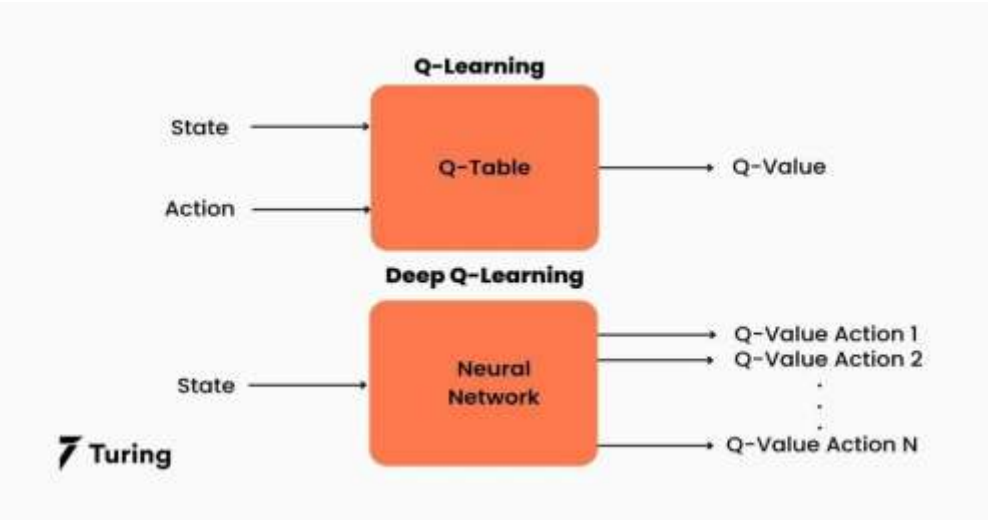
Generative adversarial networks (GANs) represent a more sophisticated unsupervised technique that can generate synthetic data that replicates actual fraudulent occurrences. GANs are the underlying class of deep learning models [18], [19], and the most promising path for DL advancement is the perception of development that they can provide. GANs consist of two parts: the generator, which creates fake fraudulent transactions, and the discriminator, which tries to figure out whether the transaction is real or fake. These two networks are trained together, with the generator getting better at creating realistic fraudulent data while the discriminator becomes better at distinguishing between the two. The advantage of using GANs for fraud detection is that they can generate additional examples of fraudulent transactions to help balance training data—something That's especially helpful when fraud is rare compared to legitimate transactions. By training models with both real and synthetic data, fraud detection systems become more robust. However, GANs come with challenges: they are computationally expensive and can take a lot of time to train properly. If the generator is not well-trained, the synthetic fraud data it produces might not be useful for improving the model.

In summary, unsupervised learning methods like autoencoders, clustering, and GANs are powerful tools for fraud detection because they can uncover hidden patterns of fraud without needing pre- labeled data. Autoencoders are great for spotting anomalies in transaction behavior but need to be tuned carefully to avoid false alarms. Clustering methods can group similar transactions and highlight unusual ones, but they can struggle with large datasets. GANs offer the ability to generate synthetic fraud data, helping to balance imbalanced datasets, but they require significant computational resources. Despite these challenges, these unsupervised techniques are crucial for detecting new and evolving forms of fraud, especially when traditional methods may not be able to keep up with rapidly changing fraudulent behaviors.

Reinforcement learning approaches to fraud detection

Reinforcement learning (RL) is becoming an increasingly popular method for fraud detection, thanks to its ability to learn and adapt in real-time. Unlike traditional supervised or unsupervised learning methods, which rely on historical data to identify patterns, RL involves agents that learn by interacting with their environment. As these agents take actions, they receive feedback—either rewards or penalties—that helps them refine their strategies over time. This makes RL particularly well-suited for fraud detection, where patterns are constantly evolving and systems need to adapt quickly.

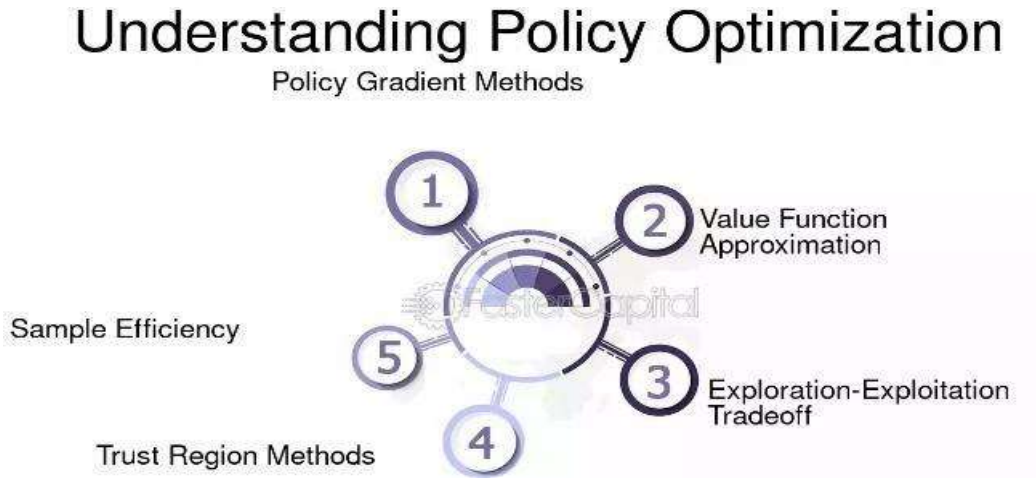
One common RL technique used in fraud detection is Q-learning, which is designed to help an agent learn the best possible actions in a given environment. In the context of fraud detection, Q- learning can be used to decide the optimal actions for classifying transactions. For example, a Q- learning model could assign rewards for correctly identifying fraudulent transactions and penalties for false positives (legitimate transactions flagged as fraud). This type of feedback loop allows the model to continuously improve its decision- making process. Singh et al. (2023) applied Q- learning to develop an RL model for fraud detection, where the agent dynamically adjusted its strategy to improve its accuracy. While this approach is effective, it does come with some challenges, particularly in terms of computational expense. " Training an RL model on transactional data can be resource-intensive and time- consuming, requiring large amounts of data and extensive computation to refine the model.



fig(6). q-learning neural network

Another advanced approach is Deep Q-Networks (DQN), which combines the power of Q-learning with deep neural networks. DQN is designed to handle high-dimensional data, such as the complex patterns found in

financial transactions. Lee et al. (2023) applied DQN to credit card fraud detection, where the model learned to take actions (such as flagging or approving transactions) to maximize fraud detection accuracy. The addition of deep learning allows DQN to handle much more complex, high-dimensional data compared to traditional Q-learning, making it a more powerful tool for fraud detection. However, the trade-off is that DQN models still require significant computational resources, particularly when training on large datasets, which can be a barrier for some organizations.



fig(7). optimization policy

Finally, policy gradient methods in RL take a slightly different approach by allowing agents to directly optimize their actions. Instead of learning a value for each possible action (like Q-learning), policy gradient methods aim to directly improve the policy—the strategy that determines the agent's actions. Rushin et al. used deep learning algorithms (Autoencoders) in fraud detection and found that the results produced were better than gradient boosted trees and logistic regression [20] This makes policy gradients particularly useful for complex environments like fraud detection, where the best action might not be immediately clear and the system needs to adjust based on a variety of different transaction scenarios. Li et al. (2022) used policy gradient algorithms to build an adaptive fraud detection system that learns the most effective decision-making strategies in different situations. While policy gradient methods offer greater flexibility and adaptability, they also have their challenges. They tend to require high-quality data and are often sensitive to the choice of hyperparameters (the settings that control the learning process). Finding the right balance can take time and experimentation.

In summary, reinforcement learning approaches like Q-learning, Deep Q-Networks, and policy gradient methods offer powerful, adaptable solutions for fraud detection. They can learn and improve over time, making them particularly well- suited to dynamic environments where fraud patterns constantly change. However, these methods also come with some challenges, such as high computational costs, the need for extensive training data, and sensitivity to model settings. Despite these hurdles, RL holds great potential for creating more accurate and adaptive fraud detection systems that can stay one step ahead of increasingly sophisticated fraudulent activities.

ANALYSIS AND DISCUSSION

The variety of deep learning techniques being applied to credit card fraud detection shows just how fast the field is evolving. Supervised learning methods like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are particularly effective at recognizing fraud when there are clear patterns in the data and labeled examples to learn from. However, these models struggle when confronted with new fraud tactics that haven't been seen before, making them less adaptable in the face of emerging fraud schemes. Additionally, since these methods rely heavily on labeled data (where transactions are pre-marked as fraudulent or legitimate), the scarcity of such labeled examples can create challenges. Plötz, Hammerla and Olivier used RBMs for activity recognition in context-aware computing applications [21]. Limited labeled data can lead to overfitting, where the model becomes too specialized in recognizing only the types of fraud it has seen before, making it less capable of identifying new, unseen fraud patterns.

Unsupervised learning methods, on the other hand, offer an advantage because they don't require labeled data. Techniques like autoencoders and clustering algorithms can help uncover hidden or unusual patterns in the data, allowing them to identify outliers and detect potential fraud. These models are especially useful when fraud patterns are constantly changing or evolving, as they don't rely on predefined labels. However, unsupervised learning techniques aren't perfect. One of the biggest issues is that they often result in high false positive rates—where legitimate transactions are mistakenly flagged as fraud. This is a significant concern for financial institutions, as excessive false positives can disrupt the user experience, frustrate customers, and erode trust in the system.

Then there's reinforcement learning (RL), which offers a fundamentally different approach. Rather than just learning from static historical data, RL allows models to interact with their environment and learn through experience. The model takes actions, receives feedback in the form of rewards or penalties, and adjusts its behavior accordingly. On the other hand, because of its remarkable performance and capacity to retain data over lengthy periods, LSTM is ideally suited for detecting credit card fraud [22].

This dynamic learning process gives RL a major advantage in fraud detection, particularly in environments where fraud patterns are constantly evolving. RL's ability to make decisions based on cumulative rewards makes it well-suited for handling real-time fraud detection in complex scenarios. The more data and feedback the RL model receives, the better it can adjust its strategies over time. However, RL also presents several challenges. First, it requires significant computational resources and often large amounts of training data to be effective.

Moreover, designing the right reward structure is tricky: if the rewards aren't set properly, the model might learn to optimize for the wrong things—like flagging too many legitimate transactions (leading to false positives) or missing actual fraud cases. While RL offers many advantages, there are also practical and ethical considerations. Since RL models are often data-hungry, they raise concerns about privacy, especially when they need to continuously interact with sensitive user data to make real-time decisions. Balancing the need for data with the protection of user privacy is a critical challenge. In addition, the complexity of RL models can make them harder to interpret. In the financial world, stakeholders—including customers, auditors, and regulators—need clear, understandable explanations for why a model has flagged a transaction as fraud or not. Without transparency and interpretability, it becomes difficult to trust the system, which is a key issue for widespread adoption in financial applications.

In conclusion, while supervised, unsupervised, and reinforcement learning techniques each have their unique strengths, they all come with limitations. Supervised methods are great at detecting known fraud patterns but struggle with new ones. Unsupervised methods can detect emerging fraud patterns but often lead to high false positives. Reinforcement learning offers a dynamic, adaptive approach but requires significant computational resources and careful model design. The future of fraud detection likely lies in combining the best aspects of

these techniques—merging the adaptability and continuous learning of RL with the pattern recognition strengths of deep learning. This could lead to models that are not only more accurate and scalable but also more capable of evolving alongside new and sophisticated fraud strategies.

Future Research Directions

Advancing credit card fraud detection through deep learning and reinforcement learning (RL) presents exciting opportunities, but it also requires overcoming several significant challenges. These challenges are key areas for future research and could ultimately push the boundaries of what's possible in fraud detection systems.

Improving Real-Time Detection and Response: One of the most pressing challenges is optimizing RL models for real-time fraud detection. For image processing, the purpose of using a CNN is to minimise processing without losing key features by reducing the image to make predictions [23], 24]. To prevent fraudulent transactions before they're completed, the system needs to be incredibly fast and accurate. This means reducing the time it takes to process data and make decisions low-latency processing is essential. Enhancing the speed and computational efficiency of RL methods could be achieved by simplifying neural network architectures or using edge computing, where data is processed closer to the source (e.g., on users' devices) rather than relying solely on distant servers. This approach could significantly speed up the detection process and make real-time fraud prevention more feasible.

Making Reinforcement Learning Models More Interpretable: While RL models are powerful, they are often criticized for being "black boxes." This means that, even though the model may make accurate fraud predictions, it can be difficult to understand why a particular decision was made. This lack of transparency is a problem for financial institutions and regulators, who need clear explanations for why transactions are flagged as fraudulent. Research into developing explainable RL models is crucial. This might involve creating architectures that are inherently interpretable or developing new techniques, like visualization tools, to help explain the model's decision-making process. These explanations would be critical for building trust in RL-based fraud detection systems and ensuring they meet regulatory standards.

In April 2017, an article by consulting firm McKinsey concluded that Deep Learning presented a promising solution to the problem of financial fraud detection by enabling institutions to make optimal use of all of their historical customer data as well as real-time transaction details that are recorded at the time of the transaction [25]. Leveraging Transfer Learning for Evolving Fraud Patterns: Fraud tactics are always evolving, and fraudsters are constantly finding new ways to bypass detection systems. Transfer learning could help solve this issue by enabling models to transfer knowledge from one set of fraud data to another. This means that models trained on historical fraud data could adapt to new, unseen fraud patterns with less training time. If applied to RL, transfer learning could allow models to quickly adjust to new data, making them more resilient to changing fraud tactics. This could be a game-changer in maintaining high detection accuracy in an ever-evolving fraud landscape.

Reducing Computational Costs and Resource Demands: One of the major barriers to scaling RL-based fraud detection is the significant computational resources required. Training RL models can be resource-intensive, and not all institutions have the infrastructure to support it. Future research needs to focus on making RL techniques lighter and more efficient. This could involve developing methods like model compression, where the size of the model is reduced without sacrificing performance, or quantization, which simplifies the model's calculations to save on processing power. Another promising solution is federated learning, which allows models to be trained across decentralized devices without needing to centralize data. This not only helps save on resources but also has the added benefit of enhancing privacy.

Fine-Tuning Reward Structures for Fraud Detection: One of the most crucial aspects of RL is how rewards are structured. In fraud detection, this is a delicate balancing act: the model must maximize detection rates while minimizing false positives (legitimate transactions incorrectly flagged as fraud). Future research should focus on developing more sophisticated reward functions that take into account the complexities of fraud detection. For instance, rewards could be adjusted dynamically based on factors like transaction type the risk level of a transaction, or the user's history. This would help fine-tune the RL models, ensuring they are more aligned with the nuanced needs of fraud detection in real-world scenarios.

Aurna et al. [27] suggested a CCFD method based on federated learning (FL) to safeguard private credit card information..Ensuring Privacy in Data- Intensive Models: Privacy is a critical concern in fraud detection, particularly given the sensitive nature of user transaction data. As RL models become more data-hungry, it's essential to address privacy concerns to protect users. Research into privacy-preserving techniques like differential privacy (which adds noise to data to prevent identification of individual users) or federated learning (which allows models to be trained without sharing raw data)—could provide solutions. These techniques allow models to learn from large datasets while still safeguarding individual privacy, making them ideal for use in financial services where strict data protection regulations must be followed.
In conclusion, while the potential of deep learning and reinforcement learning in credit card fraud detection is immense, there are still key challenges to address. Optimizing for real-time detection, improving model interpretability, adapting to evolving fraud patterns, reducing computational demands, fine-tuning reward structures, and ensuring privacy are all critical areas for future research. By tackling these challenges, we can move closer to developing fraud detection systems that are faster, more accurate, adaptive, and privacy-conscious—ensuring that they remain effective in an ever-changing landscape of fraud threats.

Conclusion

As digital transactions continue to surge, credit card fraud detection has become an urgent priority for financial institutions. Traditional fraud detection methods often struggle to keep up with the complexity and ever-evolving nature of fraudulent activities. This is where deep learning, especially when combined with reinforcement learning, offers a promising solution. These advanced models have the ability to adapt in real time, learning from new fraud patterns as they emerge, and adjusting their strategies to prevent fraud more effectively. Reinforcement learning, in particular, enables fraud detection systems to continuously improve by interacting with data, helping to minimize both missed fraud cases and false positives.

However, despite the potential of these technologies, there are still significant hurdles to overcome. L algorithms fall into one of four categories: reinforcement learning, supervised, unsupervised, or semi-supervised [26]. Reinforcement learning models, although powerful, are resource-intensive. They require vast amounts of training data and substantial computational power to function effectively. Additionally, fine-tuning the reward structures within these models is critical, as poorly designed rewards can lead to suboptimal performance. Beyond technical challenges, there are also concerns about the interpretability of these models. In financial contexts, where decisions must be transparent and understandable, the "black box" nature of some deep learning models can be a barrier. Privacy issues are another major concern, as sensitive financial data must be protected while these models are being trained and deployed.

Looking ahead, the future of fraud detection will depend on addressing these challenges. It's not just about developing more accurate models—it's about creating solutions that are scalable, interpretable, and in full compliance with privacy standards. Financial institutions need systems that not only detect fraud effectively but also operate in a way that is transparent to both regulators and customers.

In conclusion, the key to advancing credit card fraud detection lies in a balanced, holistic approach that combines the power of deep learning and reinforcement learning with a focus on privacy, interpretability,

and scalability. By overcoming the current limitations and continuing to innovate in these areas, future fraud detection systems will be better equipped to protect both financial institutions and their customers, paving the way for safer, more secure digital transactions.

References

[1] J. Wang, W. Liu, Y. Kou, D. Xiao, X. Wang, and X. Tang, ‘‘ApproxSMOTE federated learning credit card fraud detection system,’’ in Proc. IEEE 47th Annu. Comput., Softw., Appl. Conf. (COMPSAC), Jun. 2023, pp. 1370–1375.

[2] A. A. El-Naby, E. E.-D. Hemdan, and A. El-Sayed, ‘‘An efficient fraud detection framework with credit card imbalanced data in financial services,’’ Multimedia Tools Appl., vol. 82, no. 3, pp. 4139–4160, Jan. 2023. [

[3] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, ‘‘Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,’’ IEEE Access, vol. 10, pp. 39700–39715, 2022.

[4] P. Wang, E. Fan, and P. Wang, ‘‘Comparative analysis of image classification algorithms based on traditional machine learning and deep learning,’’ Pattern Recognit. Lett., vol. 141, pp. 61–67, Jan. 2021.

[5] I. D. Mienye and Y. Sun, ‘‘A deep learning ensemble with data resampling for credit card fraud detection,’’ IEEE Access, vol. 11, pp. 30628–30638, 2023.

[6] S. Gold, ‘‘The evolution of payment card fraud,’’ Comput. Fraud Secur., vol. 2014, no. 3, pp. 12–17, Mar. 2014.

[7] S. S. Yadav and S. M. Jadhav, ‘‘Deep convolutional neural network based medical image classification for disease diagnosis,’’ J. Big Data, vol. 6, no. 1, pp. 1–18, Dec. 2019.

[8] J. Naranjo-Torres, M. Mora, R. Hernández-García, R. J. Barrientos, C. Fredes, and A. Valenzuela, ‘‘A review of convolutional neural network applied to fruit image processing,’’ Appl. Sci., vol. 10, no. 10, p. 3443, May 2020.

[9] I. D. Mienye, P. Kenneth Ainah, I. D. Emmanuel, and E. Esenogho, ‘‘Sparse noise minimization in image classification using genetic algorithm and DenseNet,’’ in Proc. Conf. Inf. Commun. Technol. Soc. (ICTAS), Mar. 2021, pp. 103–108.

[10] R. San Miguel Carrasco and M.-Á. Sicilia-Urbán, ‘‘Evaluation of deep neural networks for reduction of credit card fraud alerts,’’ IEEE Access, vol. 8, pp. 186421–186432, 2020.

[11] K. Fu, D. Cheng, Y. Tu, and L. Zhang, ‘‘Credit card fraud detection using convolutional neural networks,’’ in Neural Information Processing, Kyoto, Japan. Cham, Switzerland: Springer, 2016, pp. 483–490.

[12] S. Dong, Y. Xia, and T. Peng, ‘‘Network abnormal traffic detection model based on semi-supervised deep reinforcement learning,’’ IEEE Trans. Netw. Service Manag., vol. 18, no. 4, pp. 4197–4212, Dec. 2021.

[13] E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, ‘‘A systematic review of literature on credit card cyber fraud detection using machine and deep learning,’’ PeerJ Comput. Sci., vol. 9, p. e1278, Apr. 2023

[14] Ibomoiye Domor Mienye , (Member, IEEE), and Nobert Jere, "Deep learning for Credit Card fraud detection: A Review of Algorithms, Challenges, and Solutions," IEEE Access, Department of Information Technology, Walter Sisulu University, Buffalo City Campus, East London 5200, South Africa, 11 July 2024.

[15] B. Yuen, M. T. Hoang, X. Dong, and T. Lu, ''Universal activation function for machine learning,'' Sci. Rep., vol. 11, no. 1, p. 18757, Sep. 2021.

[16] J. Kim, H.-J. Kim, and H. Kim, ''Fraud detection for job placement using hierarchical clusters-based deep neural networks,'' Int. J. Speech Technol., vol. 49, no. 8, pp. 2842–2861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[17] Senator, T.E., Goldberg, H.G., Wooton, J., Cottin,i M.A., Khan, A.U., Klinger, C.D., Llamas, W.M., Marrone, M.P., Wong, R.W. (1995). Financial Crimes Enforcement Network AI System (FAIS) Identifying Potential Money Laundering from Reports of Large Cash Transactions. AI magazine, 16(4), 21.

[18] I. Benchaji, S. Douzi, and B. E. Ouahidi, ''Credit card fraud detection model based on LSTM recurrent neural networks,'' J. Adv. Inf. Technol., vol. 12, no. 2, pp. 113–118, 2021, doi: 10.12720/jait.12.2.113-118.

[19] H. Zhou, H.-F. Chai, and M.-L. Qiu, ''Fraud detection within bankcard enrollment on mobile device based payment using machine learning,'' Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1537–1545, Dec. 2018, doi: 10.1631/FITEE.1800580.

[20] Rushin, G., Stancil, C., Sun, M., Adams, S., & Beling, P. (2017, April). Horse race analysis in credit card fraud—deep learning, logistic regression, and Gradient Boosted Tree. In Systems and Information Engineering Design Symposium (SIEDS), 2017 (pp. 117- 121). IEEE.

[21] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, ''A neural network ensemble with feature engineering for improved credit card fraud detection,'' IEEE Access, vol. 10, pp. 16400–16407, 2022.

[22] Plötz, T., Hammerla, N. Y., & Olivier, P. (2011, July). Feature learning for activity recognition in ubiquitous computing. In IJCAI Proceedings-International Joint Conference on Artificial Intelligence (Vol. 22, No. 1, p. 1729).

[23] A. O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ''Performance analysis of feature selection methods in software defect prediction: A search method approach,'' Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.

[24] J. Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szelg,, and R. Słowiński, ''Auto loan fraud detection using dominance-based rough set approach versus machine learning methods,'' Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[25] Corbo, J., Giovine, C., & Wigley, C. (April 2017). Applying analytics in financial institutions' fight against fraud. In McKinsey Analytics Retrieved February 8, 2018, from mckinsey.com/businessfunctions/mckinsey-analytics/our-insights/applying-analytics- infinancial-institutions-fight-against-fraud.

[26] S. Dong, Y. Xia, and T. Peng, ''Network abnormal traffic detection model based on semi-supervised deep reinforcement learning,'' IEEE Trans. Netw. Service Manag., vol. 18, no. 4, pp. 4197–4212, Dec. 2021.

[27] N. F. Aurna, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, ''Federated learning-based credit card fraud detection: Performance analysis with sampling methods and deep learning algorithms,'' in Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR), Jul. 2023, pp. 180–186