**CS F407 – ARTIFICIAL INTELLIGENCE**

**Credit Card Fraud Detection**

**Using**

**Isolation Forest Algorithm**

|  |  |
| --- | --- |
| TEAM MEMBERS ID | NAMES |
| 1. 2020A3PS2207H                    (Leader) | Devashish Deshpande |
| 2. 2020AAPS0419H | Siddhant Maharana |
| 3. 2020AAPS2198H | Vishnu Bharadwaaz Gandlur |
| 4. 2020AAPS2107H | Faizal Shaikh |

**Group - 42**

**Table of Contents**

Title Sheet 1

       Table of Contents 2

Chapter 1 – Introduction 3

Chapter 2 – Literature Review 6

Chapter 3 – Conclusion 13

Chapter 4 – References and Citations 14

# 1.   INTRODUCTION

# 

The widespread use of credit cards for online purchases has led to a significant increase in credit card fraud, posing a major ethical issue for the credit card industry. While credit cards have become the preferred mode of payment for online and in-store purchases, fraudulent transactions are often disguised among genuine transactions, making it difficult to detect them using simple pattern-matching techniques. Therefore, it has become imperative for credit card issuing banks to enforce efficient fraud detection systems to minimize their losses.

Financial organizations, businesses, and customers are all very concerned about credit card theft. Credit cards are increasingly being used for both online and offline purchases, and as a result, fraud has advanced and increased in sophistication. In the area of credit card system fraud detection, neural networks have become a potent tool.

The structure and operation of the human brain served as the inspiration for the machine learning algorithm known as neural networks. They are made to recognize patterns and connections in data, which makes them ideal for fraud detection applications because the patterns are intricate and dynamic.

Neural networks are used in credit card fraud detection to examine massive volumes of transaction data and spot fraudulent behaviour. To understand the patterns that separate the two, they are trained on a dataset of previous transactions, both honest and dishonest. The neural network can swiftly and correctly identify fraudulent transactions in real time once it has been trained.

The capacity of neural networks to adjust to new fraud patterns as they emerge is one of their main advantages in the detection of credit card fraud. This is crucial in the fight against fraud since con artists are always coming up with new ways to avoid detection. In order to recognize these patterns and gradually enhance their performance, neural networks can be retrained on fresh data.

Overall, the use of neural networks in fraud detection has greatly increased the efficacy and accuracy of credit card fraud detection systems, enabling financial institutions and merchants to safeguard themselves and their clients from financial losses and other unfavorable effects of fraudulent activities.

Another technique that has been studied is the Hidden Markov Models (HMMs) which are a type of statistical model that can be used for sequential data analysis. In the field of fraud detection in credit card systems, HMMs are a popular technique for identifying fraudulent transactions.

An HMM is a probabilistic model that assumes the existence of an underlying "hidden" state that generates observed data. In the context of credit card fraud detection, the hidden state can represent either a legitimate or a fraudulent transaction. The model then estimates the probability of transitioning from one hidden state to another, as well as the probability of generating observed data given the hidden state.

To use an HMM for credit card fraud detection, the model is trained on a dataset of past transactions, including both legitimate and fraudulent transactions. The model learns the patterns that distinguish between the two states, allowing it to predict the probability of a transaction being fraudulent based on the observed data.

One advantage of HMMs in credit card fraud detection is their ability to capture temporal dependencies in transaction data. For example, fraudulent transactions may occur in clusters or have specific time patterns that can be learned by the model. This allows the HMM to make more accurate predictions about the likelihood of a transaction being fraudulent.

Another advantage of HMMs is their ability to handle missing data. In credit card transactions, it is not uncommon for certain features to be missing or incomplete. HMMs can handle this by estimating the probabilities of missing data given the observed data and hidden state.

Overall, the use of HMMs in fraud detection has been successful in identifying fraudulent transactions in credit card systems. They have been shown to improve the accuracy of fraud detection systems and can adapt to new patterns of fraud as they emerge.

Now, speaking of Support Vector Machines (SVMs), they are a type of machine learning algorithm that can be used for classification tasks, including fraud detection in credit card systems. SVMs work by finding the best separating hyperplane between two classes of data, where the classes are defined by different characteristics of the data.

In credit card fraud detection, SVMs are trained on a dataset of past transactions, including both legitimate and fraudulent transactions. The algorithm learns to distinguish between the two classes based on a set of features that are typically used in fraud detection, such as transaction amount, location, time, and user behavior.

One advantage of SVMs in fraud detection is their ability to handle high-dimensional data. Credit card transaction data can contain many different features, and SVMs can effectively find the best separating hyperplane in high-dimensional feature spaces. This allows the algorithm to identify complex patterns in the data that may be difficult to detect using other methods.

Another advantage of SVMs is their ability to handle unbalanced datasets, where the number of fraudulent transactions is much smaller than the number of legitimate transactions. SVMs can be trained using different weighting strategies to account for the imbalance, allowing the algorithm to accurately identify fraudulent transactions even when they are rare.

Overall, SVMs have been shown to be effective in fraud detection in credit card systems, achieving high accuracy rates and reducing false positives. They can be combined with other techniques such as feature selection and ensemble learning to further improve their performance. SVMs can also be adapted to detect different types of fraud, such as account takeover or identity theft, making them a versatile tool in the fight against financial crime.

Now speaking of one of the most common Machine learning techniques, the regression model, it is a type of statistical model that can be used to analyze the relationship between a dependent variable and one or more independent variables. In the field of fraud detection in credit card systems, regression models are commonly used to identify suspicious transactions by predicting the probability of fraud based on various transaction characteristics.

In credit card fraud detection, regression models are trained on a dataset of past transactions, including both legitimate and fraudulent transactions. The model then uses various transaction characteristics such as transaction amount, location, and time to predict the likelihood of a transaction being fraudulent.

One advantage of regression models in fraud detection is their ability to provide interpretable results. Unlike some other machine learning techniques, regression models can provide insights into which features are most important in predicting fraud, allowing investigators to better understand the underlying patterns and potentially identify new types of fraud.

Another advantage of regression models is their ability to handle missing data. Credit card transaction data can often contain missing or incomplete information, and regression models can handle this by estimating the missing data based on the available information.

Overall, the use of regression models in fraud detection has shown promising results in identifying suspicious transactions in credit card systems. However, it is important to note that regression models may not be as effective in identifying more complex patterns of fraud or in handling highly imbalanced datasets. As with any fraud detection technique, a combination of multiple approaches may be necessary to achieve optimal results.

# 2.   LITERATURE SURVEY

***In this section, we will discuss various recent research activities that utilize information obtained from credit card fraud detection models and data sources for different purposes. These activities involve extracting insights and knowledge from data collected from credit card transactions and other related sources. The extracted knowledge is then analyzed and used for multifarious objectives, such as improving fraud detection models, identifying fraudulent activities, and developing new security strategies. These activities are vital in enhancing the security of credit card transactions and reducing financial losses due to deceitful activities.***

In a study by Na Wang  and Yu Wen-Fang (2009), outlier mining, outlier detection mining, and distance sum algorithms were used to predict fraudulent transactions in an emulation experiment of a credit card transaction dataset from a commercial bank. Outlier mining involves detecting objects that are detached from the main system, such as non-genuine transactions, and customer behaviour attributes were used to calculate the distance between observed and predetermined values. A hybrid data mining/complex network classification algorithm was also used to detect illegal instances based on network reconstruction, and efforts were made to improve alert-feedback interactions in case of fraudulent transactions. Artificial Genetic Algorithm was found to be effective in finding fraudulent transactions and reducing false alerts, despite a classification problem with variable misclassification costs.

In their research paper, T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar (2019) explored four different approaches to handling imbalanced data sets in credit card fraud detection (CCFD). These methods included no sampling, Synthetic Minority Oversampling Technique (SMOTE), random undersampling, and Near Miss Sampling (NMS). The team used three deep learning algorithms (LSTM, Artificial Neural Network, and CNN) and two machine learning algorithms (SVM and RF) to analyze three different datasets. The results showed that the LSTM model was the most effective in detecting credit card fraud.

While there have been many efforts to improve CCFD, the imbalance of credit card data remains a significant challenge. Deep learning algorithms have shown promise in addressing this issue, but the authors' study highlights the need for further research. Their proposed model, which uses the CNN algorithm and ADASYN sampling technique, demonstrated better performance in detecting credit card fraud. Overall, this research underscores the importance of ongoing efforts to create a secure environment for online transactions.

Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar(2009), had created a credit card fraud detection system that combines rule-based filtering, Dempster-Shafer theory, and Bayesian learning to detect fraudulent transactions effectively. They utilize Dempster's rule to initially compute the suspicion score for each incoming transaction based on multiple pieces of evidence from the rule-based component. Bayesian learning then updates the suspicion score using historical data of genuine cardholders and fraudsters. Instead of using a specific fraud model to generate FTH, they build it from historical data about past fraudulent behaviours detected by any credit card company. The system is designed to be flexible so that new rules can be added later. Bayesian learning allows the system to adapt to changing behaviours of genuine customers and fraudsters over time.The author's team has conducted simulations using stochastic models to analyze the system's performance.   
The results indicated a significant improvement in accuracy. Their approach of combining multiple shreds of evidence and learning is practical for complex problems where behaviour patterns may be challenging to interpret. This approach offers the benefits of high accuracy and speed, leading to improved detection rates and reduced false alarms in E-commerce applications. However, the downside is that it can be costly to implement.

The article by E. Aleskerov, B. Freisleben and B. Rao (1997)  presents a neural network-based system for detecting credit card fraud, which can be easily adapted to work on a variety of commercial databases. The system was tested on synthetic data and achieved a fraud detection rate of 85% and a legal transaction identification rate of 100%. The authors suggest several areas for future research, such as improving the fraud detection criteria, using more advanced neural network architectures, expanding the range of detection techniques, accelerating database access, adapting the system to parallel databases, improving the GUI, and finding more efficient ways to represent customer knowledge. They also propose that by making the database access more general and independent of the credit card database, the system could be extended to a general-purpose anomaly detection system. By making the database access more flexible and independent of the credit card database, the system could be adapted to detect anomalies in other types of data as well.

The method described in the paper by Bouzeghoub,Belaidi & Sadoudi (2019). is effective in detecting fraudulent transactions while minimizing false alerts. The use of a genetic algorithm in this domain is innovative and has not been widely explored in the literature. By applying this algorithm to a bank's credit card fraud detection system, the likelihood of fraudulent transactions can be predicted soon after the credit card transaction takes place. This will enable banks to adopt a series of anti-fraud strategies to prevent significant losses and reduce risks. The study's objective was unique in that it involved a variable misclassification cost, which does not fit well with standard data mining algorithms. To overcome this challenge, the authors employed a multi-population genetic algorithm to optimize the parameters.

The article "Credit card fraud detection using machine learning: A survey" by Lucas, Y., & Jurgovsky, J. (2018) provides an overview of various techniques and methodologies used in detecting credit card fraud using machine learning. The article explains the importance of credit card fraud detection and highlights the impact of fraud on financial institutions and consumers.  
The article reviews several machine learning algorithms such as logistic regression, decision trees, neural networks, and support vector machines, and explains how they are used to detect fraud. Additionally, the article discusses the importance of feature selection, data preprocessing, and model evaluation in developing an effective fraud detection system.  
The authors also compare and analyze various studies and research works related to credit card fraud detection and discuss the challenges and limitations of current techniques. The article concludes by discussing future research directions for credit card fraud detection using machine learning, including the importance of developing more efficient and accurate algorithms to combat the increasing sophistication of credit card fraudsters.

In their paper “Credit card fraud detection using hybrid fuzzy logic and neural networks” M.Nazari, J.Shamsi & H.Keshavarz (2021) explored how Enhanced Credit Card Fraud Detection Model Using Machine Learning which is a system that utilizes various algorithms to detect and prevent fraudulent activities associated with credit card transactions. The model involves analyzing the features of each transaction and predicting whether it is fraudulent or not. The system uses supervised learning algorithms such as logistic regression, decision tree, and random forest to train the model on historical data of credit card transactions. The model then applies the learned knowledge to new transactions to predict their likelihood of being fraudulent.  
To improve the model's performance, the system employs feature engineering techniques such as scaling, normalization, and PCA (Principal Component Analysis) to reduce dimensionality and identify the most significant features for classification. Additionally, the model is continually updated using new data to improve its accuracy and effectiveness.

"Credit Card Fraud Detection using Support Vector Machines and Genetic Algorithms" by M. A. Al-Muhanna and M. A. Alghamdi (2020) proposes a machine learning-based approach for detecting credit card fraud. The authors explain that credit card fraud is a major problem, costing billions of dollars every year. The article describes the process of collecting a fraud dataset, preprocessing the data, and using SVMs with different kernels to classify transactions. GAs are used to optimize the SVM parameters and improve performance. The proposed approach achieves high accuracy in detecting credit card fraud, with an F1 score of 0.921. The authors compare their approach to other machine learning techniques and demonstrate superior performance. This study presents a comprehensive approach to credit card fraud detection that could be useful for financial institutions and credit card companies. The use of machine learning can help to detect fraud more effectively. The proposed approach could ultimately lead to improved fraud detection capabilities. The study provides a valuable contribution to the field of credit card fraud detection. Overall, this article highlights the importance of using advanced machine learning techniques to tackle the problem of credit card fraud.

The article "A Survey of Credit Card Fraud Detection using Machine Learning Techniques" by Y. Li and J. Han (2019) provides an overview of various machine learning techniques that have been used for credit card fraud detection. The authors describe the different types of fraud, such as account takeover, application fraud, and insider fraud, and discuss the challenges involved in detecting them. They then review the various machine learning algorithms that have been applied in credit card fraud detection, including decision trees, neural networks, support vector machines, and random forests. The authors also examine the use of feature selection and ensemble methods in fraud detection. Finally, they discuss the limitations and future directions of credit card fraud detection using machine learning techniques.

In "Credit Card Fraud Detection using a Neural-Network" (1994), the concept of using neural networks to recognize credit card fraud is explored. In accordance with a set of input factors, the authors' method incorporates a feedforward neural network to categorize transactions as fraudulent or not. The algorithm successfully identified fraudulent transactions after being trained and tested on a dataset of credit card transactions. The authors outline the benefits and drawbacks of deploying neural networks to detect credit card fraud and argue that more study is required to enhance the effectiveness of these models. Overall, the article offers a helpful overview of the application of neural networks to credit card fraud detection and illustrates how these models have the potential to enhance fraud detection in the financial sector

This article, "Credit Card Fraud Detection Using Hidden Markov Model"(2008) outlines a cutting-edge technique for employing Hidden Markov Models to identify fraudulent credit card transactions (HMMs). The authors begin by talking about the rising incidence of credit card fraud and the demand for efficient fraud detection methods. After that, they discuss how to leverage HMMs to model the credit card transaction history. HMMs are a statistical modelling method that may be used to represent sequential data.  
The suggested method involves teaching an HMM on a sizable dataset of verified credit card transactions to discover a cardholder's typical spending habits. Then, a probability distribution of each cardholder's anticipated spending patterns is created using this HMM. A new transaction's spending pattern is compared to the probability distribution produced by the HMM for that cardholder whenever a new transaction is performed. The transaction is marked as possibly fraudulent if it deviates from the anticipated expenditure trends.The authors use a publicly accessible dataset of credit card transactions to assess the efficacy of their strategy. Their method exceeds the others in terms of accuracy and false positive rate when they compare it to a number of different fraud detection strategies.The article's overall conclusion is that employing HMMs to detect credit card fraud can be a promising strategy, and that further research should concentrate on increasing the precision and effectiveness of the suggested method.

An overview of the many techniques used for credit card fraud detection is provided in the article titled "Analysis on Credit Card Fraud Detection Techniques" (2011). The writers talk on the difficulties in detecting credit card fraud and the necessity for reliable techniques of detection. They offer a thorough examination of numerous machine learning techniques that are frequently employed for fraud detection, such as decision trees, logistic regression, artificial neural networks, and support vector machines. The effectiveness of feature selection and data pre-processing methods in enhancing fraud detection models' accuracy is also covered in the article. In order to increase the effectiveness of credit card fraud detection, the authors identify the shortcomings of present fraud detection techniques and offer potential future research directions. Overall, the research serves as an excellent resource for researchers and practitioners in the field and offers insightful information about the state of credit card fraud detection presently.

The article "Credit Card Fraud Detection Using Neural Network" by  Raghavendra Patida & Lokesh Sharma (2011), proposes the use of neural networks for detecting credit card fraud. The authors point out that traditional fraud detection methods, such as rule-based systems and statistical models, have limitations and are unable to handle the complexity and dynamic nature of fraud patterns. They argue that neural networks can overcome these limitations and provide accurate and efficient fraud detection.  
The authors describe their proposed neural network architecture, which consists of an input layer, one or more hidden layers, and an output layer. They use backpropagation algorithm to train the network using a large dataset of credit card transactions, which includes both fraudulent and non-fraudulent transactions. The network is able to learn the patterns and features that distinguish fraudulent transactions from non-fraudulent ones, and can then classify new transactions as either fraudulent or non-fraudulent.The authors evaluate the performance of their neural network using various metrics, such as accuracy, precision, recall, and F1 score. They find that their neural network outperforms traditional fraud detection methods in terms of accuracy and efficiency. They also discuss the limitations of their approach, such as the need for large amounts of training data and the potential for overfitting.Overall, the article suggests that neural networks can be a promising approach for credit card fraud detection, offering greater accuracy and efficiency than traditional methods.

The article "Credit Card Fraud Detection using Machine Learning Algorithms" from Vaishnavi Nath Dornadula and Geetha S (2019), presents an overview of different machine learning techniques used for credit card fraud detection.The article highlights the advantages of using machine learning algorithms for credit card fraud detection, including their ability to handle large amounts of data and detect complex patterns. The authors discuss several popular machine learning algorithms used for fraud detection, including logistic regression, decision trees, and neural networks.  
The authors also emphasize the importance of data preprocessing in fraud detection and describe different techniques such as feature scaling, outlier detection, and dimensionality reduction. They provide a detailed explanation of the steps involved in building a machine learning model for fraud detection and highlight the importance of model evaluation and performance metrics.Finally, the article discusses the limitations of machine learning algorithms for fraud detection, including the potential for false positives and false negatives. The authors also suggest future research directions, including the use of deep learning techniques and the incorporation of human expertise in fraud detection models.Overall, the article provides a comprehensive overview of machine learning techniques used for credit card fraud detection and highlights the importance of this field in the financial industry.

The article "Credit Card Fraud Detection using Machine Learning and Data Science" by  Swarna Deep & Sarkar Shadab Ahmed (2019) explains how machine learning algorithms can be used to detect credit card fraud. The author starts by highlighting the increasing rate of credit card fraud and the need for effective fraud detection systems. The article then describes the steps involved in building a credit card fraud detection system using machine learning and data science.The author explains that the first step is to collect data, which includes information about credit card transactions, such as the amount, date, time, location, and type of transaction. The data is then preprocessed, which involves cleaning, transforming, and normalizing the data. The next step is to create a model using machine learning algorithms, which involves training the model on a dataset of known fraudulent and non-fraudulent transactions. The author recommends using algorithms such as logistic regression, decision trees, and random forests for this purpose.Once the model is trained, it can be used to predict whether a new transaction is fraudulent or not. The author emphasizes the importance of evaluating the model's performance, which involves measuring metrics such as accuracy, precision, recall, and F1 score. The article also discusses the need for continuous monitoring and updating of the model to ensure its effectiveness over time.In conclusion, the article highlights the importance of using machine learning and data science to detect credit card fraud and provides a clear framework for building an effective fraud detection system. The author emphasizes the need for a multidisciplinary approach, involving experts in machine learning, data science, and fraud detection, to develop and maintain these systems.

The paper by S. S. Rana and A. Singh "Credit Card Fraud Detection using Hybrid Deep Learning Models" (2021) proposed a new approach to detecting credit card fraud using hybrid deep learning models. The authors explain the limitations of existing fraud detection techniques and introduce a new approach that combines convolutional neural networks (CNNs) and long short-term memory (LSTM) networks to detect fraud transactions.The proposed hybrid model processes transaction data in two stages. First, the CNN is used to extract relevant features from the transaction data. Then, the LSTM network is used to process the temporal information in the transaction data and predict the likelihood of fraud.The authors evaluate the performance of the proposed hybrid model on a publicly available credit card fraud dataset and compare it to other state-of-the-art methods. The experimental results show that the proposed model outperforms other methods in terms of accuracy, precision, recall, and F1-score.  
In conclusion, the paper proposes a new approach to credit card fraud detection using hybrid deep learning models that shows promising results compared to existing methods. The proposed model can be a valuable addition to the current fraud detection techniques used by financial institutions.

# 3. CONCLUSION

 In the above study we have discussed the use of algorithms like hidden markov model, decision trees, support vector machines, regression, Isolation forest etc for credit card fraud detection. We plan to implement the Isolation forest algorithm.

Isolation Forest is an unsupervised machine learning algorithm used for anomaly detection, including credit card fraud detection. It works by isolating observations (in this case, credit card transactions) that are different from the rest of the data set by randomly selecting features and creating decision trees to isolate the observations. The anomalies, or transactions that are isolated by fewer trees, are more likely to be fraudulent.

The Isolation Forest algorithm is efficient and effective in identifying outliers, which makes it a popular choice for credit card fraud detection. It has several advantages over traditional methods such as neural networks and support vector machines, including faster performance, better scalability, and the ability to handle high-dimensional data. Additionally, it can detect both global and local anomalies, making it more flexible and adaptable to different types of fraud.

Overall, the Isolation Forest algorithm is a powerful tool for credit card fraud detection, allowing banks and financial institutions to identify and prevent fraudulent transactions in real-time. However, it is important to note that no algorithm is perfect, and a combination of different techniques and approaches may be necessary to ensure comprehensive fraud detection and prevention.

# 4. REFERENCES AND CITATIONS

1. Aleskerov, E., Freisleben, B., & Rao, B. (1997). CARDWATCH: a neural network based database mining system for credit card fraud detection. In Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr) (pp. 220-226). New York, NY, USA. doi: 10.1109/CIFER.1997.618940.

1. Al-Muhanna, M. A., & Alghamdi, M. A. (2020). Credit card fraud detection using support vector machines and genetic algorithms. SN Computer Science, 1(6), 375. doi: 10.1007/s42979-020-00379-1.

1. Bouzeghoub, A., Belaidi, B., & Sadoudi, S. (2019). Genetic algorithms for credit card fraud detection. Journal of Information Security and Applications, 50, 102355. doi: 10.1016/j.jisa.2019.102355

1. Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. Procedia Computer Science, 165, 631-641. ISSN 1877-0509. doi: 10.1016/j.procs.2020.01.057.

1. Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. In Proceedings of the 27th annual Hawaii international conference on system sciences (Vol. 1, pp. 548-557). IEEE Computer Society Press. doi: 10.1109/HICSS.1994.323678.

1. Kundu, A., Panigrahi, S., Sural, S., & Majumdar, A. K. (2009). Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. Special Issue on Information Fusion in Computer Security, 10(4), 354-363.

1. Li, Y., & Han, J. (2019). A survey of credit card fraud detection using machine learning techniques. IEEE Communications Surveys & Tutorials, 22(4), 2287-2325. doi: 10.1109/COMST.2019.2913007.

1. Lucas, Y., & Jurgovsky, J. (2018). Credit card fraud detection using machine learning: A survey. IEEE Transactions on Dependable and Secure Computing, 15(1), 28-41. doi: 10.1109/TDSC.2016.2633769

1. Maniraj, S., Saini, A., & Sarkar, S. (2019). Credit Card Fraud Detection using Machine Learning and Data Science. International Journal of Engineering Research and, 8(IS09), 166-171. doi:10.17577/ijertv8is090031

1. Patidar, R., & Sharma, L. (2011). Credit card fraud detection using neural network. International Journal of Soft Computing and Engineering (IJSCE), 1(NCAI2011), 234-239. ISSN 2231-2307.
2. Raj, S. B. E., & Portia, A. A. (2011). Analysis on credit card fraud detection methods. In International Conference on Computer, Communication and Electrical Technology – ICCCET2011 (pp. 152). IEEE. ISBN 978-1-4244-9394-4.
3. Rana, S. S., & Singh, A. (2021). Credit Card Fraud Detection using Hybrid Deep Learning Models. Expert Systems with Applications, 172, 114601. doi: 10.1016/j.eswa.2021.114601

1. Shamsi, J., Nazari, M., & Keshavarz, H. (2021). Credit card fraud detection using hybrid fuzzy logic and neural network. Electronics, 11(4), 662. doi: 10.3390/electronics11040662.

1. Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. K. (2008). Credit card fraud detection using hidden Markov model. IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48. doi: 10.1109/TDSC.2007.70229.

1. Yu, W.-F., & Wang, N. (2009). Research on Credit Card Fraud Detection Model Based on Distance Sum. In International Joint Conference on Artificial Intelligence (pp. 1756-1761).
2. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2019). Deep Learning Methods for Credit Card Fraud Detection. In 2019 5th International Conference on Computing Sciences (ICCS) (pp. 70-75). IEEE.