International Journal of Research in Engineering, Science and Management
Volume 9, Issue 1, January 2026
www.ijresm.com | E-ISSN: 2581-5792 | RESAIM Publishing | www.resaim.com

Credit Card Fraud Detection: Use of Artificial Intelligence

Minul Mindula Subasinghe*
Independent Researcher, Hatfield, United Kingdom

***Abstract*: According to Minchin (2025) fraud is UK's biggest financial threats, which includes over 2 million cases reported between January and July in 2025 alone. This sums up to over £620 million lost just in the first half of 2025. With regards to its origins, over 70% of fraud incidents starts online, and about 17% over a simple telephone call. However, banks and financial institutions introduce new tactics to reduce fraud incidents daily. Minchin (2025) also explains that UK banks were able to reimburse 98% of victims caught up in fraud incidents where criminals had gained access to their accounts or cards and had stolen money. Whereas, through authorized push payments methods, or APP for short, which ideally means that the victims were on the phone with criminals who had tricked then into sending them money through bank transfers. Banks were able to identify the genuineness of these cases as was able to return money of approximately 62% of such victims. On this paper, fraud and scams pertaining to credit cards are explained and how artificial intelligence and machine learning models, and even generative AI, can be used to identify and prevent such fraudulent activities are discussed.**

***Keywords*: Fraud, Scam, Artificial Intelligence, Machine Learning, Credit Cards, Banking and Finance Industry, Finance Security.**

1. Introduction

A. Background of the Study

It is becoming difficult to detect cybercrime, using just the traditional rule-based detection systems, which depends on a certain pattern identification or manual interferences. Since, criminals use artificial intelligence and generative AI models to find new tactics to commit credit card fraud, the best response is to create a solution using artificial intelligence or machine learning to detect and tackle credit card fraud. An AI system can be designed which can automatically identify suspicious activities and report relevant authorities which can rapidly enhance transaction security.

B. What is Fraud?

Fraud is a deliberate act of deception carried out to gain an unfair or illegal advantage. This usually involves in misleading or lying to someone on purpose to gain profits. Fraud is not categorized as an honest mistake, as it involves in an intentional and designed false impression to trick someone into giving you money. Even though fraud might start off online, however, this is not always the case. A fraud incident can originate in areas such as during a business transaction, in a healthcare setting or even online platforms – social media platforms.

Mentioned under the Fraud Act (2006) there are three sections of fraud;

a) Fraud by False Representation,
b) Fraud by Failing to Disclose Information, and
c) Fraud by Abuse of Position.

As it continues, if a person is guilty of fraud in breach of the above, is liable to imprisonment or a fine depending on the decision of the magistrate's court.

Below is a list of types of fraud mentioned and explained by (Office of the Comptroller of the Currency, 2025)

1. Check fraud
2. Consumer product and retail fraud
3. Credit card and debit card fraud
4. Debt collection fraud
5. Elder financial exploitation
6. Financial and investment fraud
7. Identity theft
8. Mortgage fraud

C. What is Scam?

A scam is something that has been set up to trick and manipulate an individual. This can include giving away personal information, sending money to someone or sharing sensitive information such as your bank details, passwords, or identification information (BBC, 2025).

BBC (2025) has shown several ways in which we can spot a scam. We should always be informed and alerted of these ways to keep ourselves safe from scamming criminals.

HSBC (2025) explains the most common types of scams sweeping across the UK.

1. Authorised push payment (APP) scams
2. Purchase scams
3. Investment scams
4. Gold purchasing scams
5. Cryptocurrency scams
6. WhatsApp/SMS scams
7. Impersonation scams
8. Romance scams
9. Payment diversion scams
10. Money mules
11. Rogue trader scams

*Corresponding author: minulmindula11@gmail.com

12. Pension scams
13. Holiday scams
14. QR code scams
15. AI or cyber scams

In technical terms, fraud and scam is similar to each other, which involves in tricking someone to gain a financial profit.

2. Aims And Objectives

A. Aim

The aim of this study is to evaluate on an AI-driven fraud detection models which can be used to successfully identify credit card transactions to find out any anomalies within the transactions to detect fraud.

B. Objectives

- To find out any limitations or challenges related to credit card fraud detection and any challenges that can be faced when integrating AI.
- To propose new techniques to an AI-driven system in detection credit card fraud.
- To compare AI-based fraud detection models with old traditional rule-based systems.
- To study upon different techniques and systems based on deep learning, machine learning, and neural-networks, pertaining to fraud detection.

3. Problem Statement

The loss concerning credit card fraud is mentioned to be billions, which is becoming a huge threat to the financial industry. Currently available fraud detection systems, which uses classic techniques are becoming outdated and outsmarted by many criminals and their improved fraud systems around the world. This rapid improvement through artificial intelligence needs to be resolved using the same. Traditional techniques can no longer detect new fraud cases and are too slow to perform quick account retrievals or card blocks to prevent fraud.

Using a proper custom-built model, which can be fed a large amount of data to train, can be used to detect not only pre-defined incidents, but also identify and capture new techniques used by criminals. The use of AI models can drastically help financial institutions keep their customer safe from criminals committing credit card fraud.

4. Literature Review

A. Overview

Several organisations, including banks and other financial institutions are in a never-ending battling to keep the public safe from these criminals. However, with the rapid growth of technology and now AI, it is quite difficult, even for high-stake banking algorithms to tackle with such criminals.

When it comes to credit card fraud it is one of the most common and the quickest ways an individual can lose money. Financial institutions used a few different tactics to prevent credit card fraud, and they are listed as below.

1. Machine learning models – machine learning models or many algorithms are trained to spot potential patterns in unusual activities. These include overseas purchases or multiple small test transactions. The models are also trained to adapt to new fraud incidents as it happens.
2. Rule-based systems – most merchants often has set a limit on transactions and immediately blocks any transaction which maybe over a set threshold. Rules can also be set to identify any mismatches on billing and shipping addresses which in turn can help identify a potential fraud.
3. Behavioural analytics – Websites are designed to keep an eye on consumer behaviour. For example, the use of a single website can differ among two different people. The way I navigate through a certain website might be different from someone else navigating through the same website. Hence, cookie can be set or other parameters are set on websites to track individual user movements and behaviours to identify possible changes. Which can lead to a possible potential fraud incident.
4. Authentication layers – security tools such as tokenization, 3DS, or biometric verification provides an extra layer of authentication to prevent unauthorised access.

Currently credit card networks, such as Visa, Mastercard or American Express has developed certain security features embedded to credit cards. Below mentioned features are embedded and integrated with credit cards to prevent fraudulent activities,

1. Address Verification Service (AVS) – this feature involves in verifying if the entered customer billing address is the same as the one registered with the account number.
2. 3-D Secure (3DS) – various card operators use this feature which prompts the user to enter a code to complete a transaction.
3. CVV (Card Verification Value) – a three-digit number for Visa or Mastercard, and a four-digit number for Amex, often found in the back of a credit card, is used to confirm a purchase through an online transaction. However, to enhance customer experience, huge e-commerce websites, such as Amazon, waive the request for the CVV, hoping to make it easier for customer to quickly checkout. This may often lead to a high risk for credit card fraud.

B. Machine Learning and Deep Learning Approaches in Fraud Detection

Certain machine learning techniques and approaches can be used to observe patterns or anomalies in transaction data. A trained model can identify any suspicious changes in spending behaviour of a certain individual which can raise a red flag in being compromised.

Long Short-Term Memory (LSTM) networks can be used in fraud detection as they can effectively capture substantial dependencies and discrepancies in transactions. These

networks often win against classic machine learning models over accuracy and reduce in false positives (Nerella, 2021). Several predictive algorithms are being developed which can distinguish between real and fraud transactions. Machine learning model can be trained using previous transactional information, which are already categorized as fraud or real. The system can be taught the difference and can be used to calculate and identify fraud in new cases, having the potential to reduce the risk for clients of being targeted by criminals.

There are three generally introduced categories of machine learning: mixed approach, unsupervised and supervised approaches. According to Ahmad & Chen (2020) supervised learning is involved in a dataset which is used to train a particular model is given instructions of labelled data. This approach requires the intervention of a human to label the transaction data as fraud or real. This would further help the model to categorize among the two. Whereas, unsupervised approach involves in analysing the transaction behaviour, looking for suspicious and unprecedented patterns within the transactions to find anomalies. This approach can often be used to identify new fraud cases, which are yet to be found and investigated.

Both of these approaches can be used together to get a more accurate detection of potential fraud incidents in credit card use. The use of both approaches can be utilized, for instance, a system can identify suspicious trends and patterns in transactions using unsupervised methods and then use supervised methods to categories these transactions as fraudulent or not. This multi-faceted approach can be utilized to detect fraud with higher accuracy level with fewer false positives (Sizan, et al., 2025).

5. Proposed Methods of Data Collection

A. Dataset Overview

After constructing custom machine learning models, datasets with and without data anomalies must be uploaded and used as training and testing data for these models. This is a crucial part in model construction and is essential before using this model to actual detect fraud incidents. Strictly for practical and research purposes, multiple datasets, are available in Kaggle, which can be used for this purpose. Furthermore, sample data can be used from various sources including financial institutions, and real-life can be used for further training and for real-world use of the system.

Both historic and real-time datasets must be used to train the models, as this can help the model to identify any potential changes in fraud trends and behaviours overtime. A few transactions information which can be used in these datasets can be, value, merchant category, location, payment channel and timestamps. The model can be trained to identify a single credit card spending pattern. Which can easily detect an anomaly if the spending habit changes instantly.

B. Data Preprocessing

According to Sizan, et al. (2025), the data that has been uploaded to the model has a few steps to follow before it can be used for training and testing. The model needs to be built in such a way that I can only read a certain format of information, which is easier for it to identify any changes. Hence, the datasets used, whether real-time, historic or even sample, needs to first be cleaned. This involves in deleting missing values and outliers. This would rather improve the integrity of the data. Secondly, feature engineering should be implemented to encode categorical features and transform them into numerical values, and these values should be normalized to maintain consistency, which can then be used within machine learning algorithms. The preprocessing of the data in such a way described helps develop a stronger background for the development of a reliable and effective fraud detection model in credit card transactions.

6. Conclusion

When we look at the numbers from 2025, it's rather clear that we are not only dealing with a rise in crime, but also witness a shift in how financial threats work.

References

[1] T. Ahmad and H. Chen, "A review on machine learning forecasting growth trends and their real-time applications in different energy systems," *Sustain. Cities Soc.*, vol. 50, p. 101721, 2019.

[2] BBC, "How to spot a scam," *BBC Bitesize*, 2025. [Online]. Available: https://www.bbc.co.uk/bitesize/articles/zgg6cxs.

[3] *Fraud Act 2006*, c. 35, United Kingdom, 2006. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/35/section/1.

[4] HSBC, "Common Scams," *HSBC Security Centre*, 2025. [Online]. Available: https://www.hsbc.co.uk/help/security-centre/fraud-guide/common-scams/.

[5] B. Luthi, "The 10 Most Common Types of Fraud," *Experian Blog*, 2025. [Online]. Available: https://www.experian.com/blogs/ask-experian/most-common-types-of-fraud/.

[6] L. Minchin, "Over £620 million lost to fraud in first half of 2025," *BBC News*, 2025. [Online]. Available: https://www.bbc.co.uk/articles/c74j00lzdpvo.

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[8] A. Nerella, "Approaches to fraud detection on credit card transactions using artificial" *SSRN*, 2021. [Online]. Available: https://download.ssrn.com/2025/6/2/5278257.pdf.

[9] Office of the Comptroller of the Currency, "Consumer Fraud Awareness and Prevention," *OCC*, 2025. [Online]. Available: https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html.