Manuscript ID:
IJEBAMPSR-2026-030213

Volume: 3

Issue: 2

Month: April

Year: 2026

E-ISSN: 3065-9140

Submitted: 06 Mar. 2026
Revised: 11 –Mar. 2026
Accepted: 11-Apr. 2026
Published: 30-Apr -2026

Address for correspondence:
Mohammed Abdullah Khairullah
Al Baha Private College of Science, Saudi Arabia
Email: basel@bpcs.edu.sa

DOI: 10.5281/zenodo.22338339

DOI Link:
https://doi.org/10.5281/zenodo.22338339

Detection of Fraud in Customer Credit Card Transaction Using Artificial Neural Network Algorithm Alanoud

Alanoud[1], Mohammed Abdullah Khairullah[2]
[1,2]Al Baha Private College of Science, Saudi Arabia

Abstract

Since the world is rapidly moving towards dealing with financial transactions without cash, and since the use of credit cards has become a necessity. The fraudulent activities associated with it are increasing dramatically leading to huge loss for the financial institutions. Therefore, we need to observe and detect these transactions and determine whether the transactions are fraudulent or not. In this project, we present a working for the most famous machine learning algorithms: "ANN" algorithm. It Used to analyze operations and detect fraud using the Python language

Keywords: *Credit Card Fraud Detection, Artificial Neural Network (ANN), Machine Learning, Fraudulent Transactions, Financial Security, Credit Card Transactions*

Introduction

Credit card is one of the most widely used financial resources designed to make purchases like food, electronic devices, travel, etc. Also, many agencies require the person to have a credit card for themselves, which is an easy way to complete any purchase. However, the existence of the impostor is beyond doubt According to the census survey, about 41.3% of netizens have started buying products online, and it is not surprising that the percentage will increase in the coming years. With the increase in online commerce, and as the world moves towards cashless transactions, the number of credit card users has increased exponentially, and as a result, the number of fraudulent operations associated with these cashless transactions will be increase.

Definition Of Fraud:

Fraud It can be loosely defined as:

"Any conduct that intends by means of a person to obtain an unfair advantage from another person." In other words, fraud is an act that aims to obtain illegitimate gain, either by concealing the truth or otherwise. as bank fraud is defined as "the unauthorized use of an individual's confidential information, or the theft of funds from his account.

Credit Card Fraud Is:

Credit card fraud, an act committed by a person with intent to defraud, whereby he uses another person's credit card to obtain anything of value. Using a credit card number without having possession of the actual card is also
a form of credit card fraud

Numer Of Categories Noted For Credit Card Fraud

1. **Lost or stolen cards:**

It is considered one of the most common types of fraud and occurs when the card is lost or stolen. The thief may steal the card from the victim or steal it from an unsecured location. The card will then be used for unauthorized transaction, To minimize the damage from this type of theft, you must report your stolen card. To prevent suspicious transactions.

2. **Commercial forgery:**

It is another type of fraud that aims to "launder" merchant receipts that make large sums by showing illegal transactions that never occurred. Often, during accepted transactions, legal information from these transactions is stolen and used to produce illegal card copies to perform illegal transactions.
Here the trader is a "compromise point" in the process.

How to Cite this Article:
Alanoud, & Khairullah, M. A. (2026). Detection of Fraud in Customer Credit Card Transaction Using Artificial Neural Network Algorithm Alanoud. International Journal of Economic, Business, Accounting, Agriculture and Management Towards Paradigm Shift in Research, 3(2), 72–77. https://doi.org/10.5281/zenodo.22338339

3. **No card fraud:**
The criminal can use the stolen card data even if he or she does not physically carry the card.
For example, it may access the card number and account holder's name by stealing some documents. Where he gets enough information to make purchases online or over the phone. These unauthorized transactions may not be noticed until the customer's bank statement is issued.
4. **Account Take over:**
The fraudster takes control of the account and begins the fraud.
5. **False fraud on the site:**
Fraud may start from the fictitious work on the websites.
6. **Application fraud:**
Customer's credentials are stolen by the fraudster, then he creates a fake account, and the transactions takes place.
7. **Card Forgery:**
All the data from the magnetic strip and copied so that it looks like the real card.

Historical Money Losses Due To Fraud In Credit Card Transactions
1. **UK - £17 million**
"The biggest instance of credit card fraud in the UK occurred in the mid-2000s when a gang of eastern European criminals used the stolen and cloned details of 32,000 credit cards to illegally acquire more than £17 million.
Over the course of a few years, they stole the money and transferred it to various accounts based in various countries before being arrested and imprisoned in 2007.
They were ultimately caught when one member of the gang was investigated as part of a routine anti-terror check. The investigating police officer's suspicions were raised and when they looked further into the man, they unraveled a wide scale fraudulent operation."
2. **USA - $200 million**
"The largest credit card fraud in the United States is far ahead of the United Kingdom. The scam, which was eventually thwarted in 2013, involved 18 gangs of criminals based in New York who stole a total of $200 million.
Their scheme was relatively complex as it involved creating many fake identities. They then hired undercover agencies to create perfect credit records for their fake identities so they could apply for high-limit credit cards and high-value loans.
The money earned was laundered through a bunch of fake and unscrupulous real companies and transferred to accounts all over the world."

3. Research Idea
Credit card fraud is constantly increasing and has become a major problem in the financial sector.
Because of this fraud, card users are reluctant to make purchases
In this project, it is proposed to apply:
(Artificial Neural Network "ANN") algorithm, which is one of the most popular machine learning algorithms to detect credit card fraud more accurately.
In the project, we will explain how it works to detect credit card fraud and compare its performance with previously used machine learning algorithms.
We hope that the experimental results will show great performance as an accurate algorithm that can be widely used in the future to detect credit card fraud in the real world.

4. Problem Statement
Today we live in a world where we can achieve different results with a touch.
In recent years, we have become more dependent on mobile phones and web applications where we can book flights, buy electronics, get recommendations, and order food to our home. This was a major reason for the increase in the number of online payment transactions. It is completely related to card fraud and has resulted in the loss of millions in revenue for financial institutions globally and has increased the concern of credit card users.
Approximately 20.48 billion cards (including credit, debit and all prepaid cards) were in circulation worldwide in 2017.
Also, today we rely on many ML applications without realizing it. One of the most popular of these applications is credit card fraud detection systems using machine learning techniques that make our payment processing more secure and robust.
Fraudsters use various techniques to obtain funds from the stolen card. In this project, we will present a proposal to apply Artificial Neural Network (ANN) algorithm to detect credit card fraud more accurately and apply it using Python language to demonstrate its efficiency.

5. Research Objective
Credit card fraud has been a huge problem throughout history, although there are systems that fight against this fraud. However, there are still various ways in which criminals can trick people and credit card companies out of huge sums of money.
Especially with the increasing use of credit cards by people to purchase goods that they desperately need. Fraud related to it is on the rise, so we need a model that predicts it with higher accuracy.
The main aim of the research is:
1. Clarifying the professionalism of the fraudulent operations.
2. Finding fraudulent in credit card transactions more accurately.

Research Field

The research aims to enhance the protection of credit cards by analyzing transactions, depending on the time between one transaction and another.

Structure of Research

The first chapter includes:

Introduction to the research, clarifying the idea of the research and its aim, describing, and clarifying the research problem.

In addition to a questionnaire to measure the extent of knowledge of the risk of fraud in bank card transactions

In the second chapter:

We talked about the background of research and previous studies that were in the same field of our research.

In the third chapter:

In the third chapter, we talked about what the analysis is, what the methodology is, and the difference between the current systems and the proposed system, in addition to the mechanism of the proposed system's work.

Gathring Sample And Studying

The study, questionnaires, and surveys were posted on social media links. Which indicated below.

https://docs.google.com/forms/d/1BOL0bbQwRaXNYfh8h7gGYmWwCZOeKKI5-gHk2_Ib3M0/edit?pli=1

Research Bachground

With the increasing reliance on credit payment, credit card fraud can be very serious and professional. However, most people do not know how dangerous this scam is. It is therefore imperative that everyone takes the necessary steps to avoid the risks of credit card fraud.

The scams vary from card theft, account takeover, fraud, to email/phone order (MO/TO scams) and more. The banking sector has taken various steps towards preventing credit card fraud. Therefore, our goal is to make the systems more professional and accurate in detecting fraud in bank card transactions.

Previous Studies

According to The American Heritage dictionary, second college edition, fraud is defined as a deception deliberately practiced in order to secure unfair unlawful gain. Fraud detection is the recognition of symptoms of fraud where no prior suspicion or tendency to fraud exists.

Recent global payment fraud statistics indicate the seriousness of the credit card fraud problem. In the United Kingdom, in 2009 alone, losses from plastic (debit and credit) card fraud according to the report by the Financial Fraud Action UK (FFA) were $US696 million (Financial Fraud Action UK, 2010).

In the same year, the Australian Payments Clearing Association (APCA) recorded losses of $US144 million from credit and charge card fraud perpetrated on Australian issued cards (Australian Payments Clearing Association, 2010).

Some relevant studies conducted by several researchers are described in this section.

A study appeared in 2010 and states that Many credit card fraud perpetrators are now better organized than before, resulting in losses greater than their crime.

As some of the proceeds of this economy are used to finance other crimes, this requires that fraud prevention tools and systems become more regulated. Countries such as the United States and the United Kingdom are improving their fraud prevention strategies by strengthening their coordination.

The study indicates that the main areas of resource allocation in credit card fraud prevention within a payments system are:

1. Understanding of the real problems.
2. Fraud prevention policy.
3. Fraud awareness.
4. technologybased protection.
5. Identity management.
6. And legal deterrence.

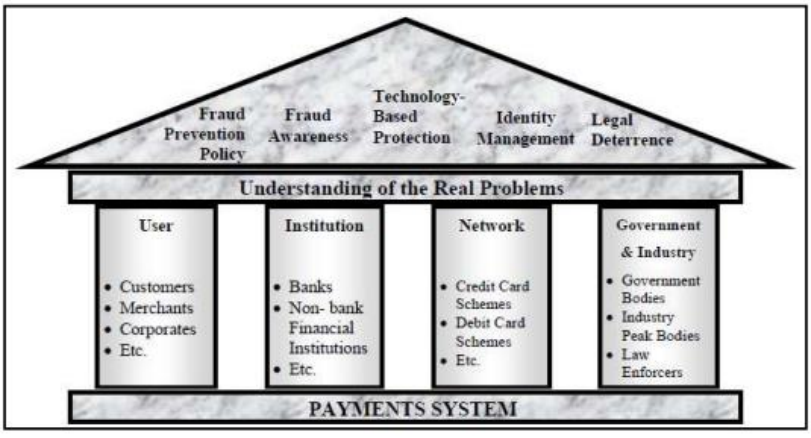


Fig.1

These areas are mainly supported by four pillars: *user*; *institution; network;* and *government and industry* [1]

And in 2020 the researchers Etab Al-Tahar Taha and Sarif Jamil Mulberry described that the gradual increase in electronic commerce made the use of credit cards more common. The fraud rate also increased.

They used an enhanced optical gradient enhancement device, the LightGBM enhancement machine.

In this approach they used two sets of public data set:

1. "Real data" consisting of fraudulent dataset
2. Non-fraudulent transactions.

Their system yields an accuracy of an accuracy of 97.34%[2].

The Researchers C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan proposed a new process with multiple stages.

First, they collect the transactions made by the cardholder into a file. Then the coefficients of behavioral patterns are collected, after which the data is classified, and then the model is trained, and the model is tested. If any abnormal behavior appears, feedback is given to the system about the abnormal behavior through a feedback mechanism [3].

In 2019 the researchers Debachudamani Prusti and Santhnu Kumar Rath designed an application with applied machine learning approaches such as Decision tree (DT), k-nearest algorithm (kNN), Extreme learning machine (ELM), Multilayer perceptron (MLP) and support vector machine (SVM) to detect the accuracy in fraud identification.

They proposed a model by hybridizing the DT, SVM and KNN techniques. They used two web-based protocols.

Such as simple object access protocol (SOAP) and Representational state transfer (REST) for efficient exchange of data across multiple heterogeneous platforms.

They compared five results from a machine learning algorithm based on a measure of accuracy.

SVM performed better than other algorithms by 81.63% but the hybrid system they proposed has higher accuracy 82.58% [4].

Researcher Muhammad Zamini and Golamali Montazar proposed an unmoderated credit card fraud detection system using autoencoder-based aggregation. “They used three hidden layers, and the k method of clustering was used and tested on a European data set which performed very well compared to other existing system.”[5].

Iman Sadeqly, Nawal Sayel and Fouzia Ben Abbou describe the current banking transactions like credit card transactions, mobile phone transactions etc." are gaining popularity" because all people prefer digital and paperless transactions. And all of them were exposed to fraud. Many researchers have analyzed, designed, and developed the model for fraud detection using machine learning. They made a comparison of all machine learning algorithms to determine which model is best for detecting fraud in a credit transaction [6].

1. Data Analysis

Data analysis is a procedure to examine it and find out the appropriate way to deal with it and to determine a specific algorithm and system for it to be more accurate. Data analysis has different methods that differ according to the goal used by the researcher, and we will explain it in the following points.

2. Methodology

Methodology is the study of research methods. Another definition can refer to the methods themselves or to the philosophical discussion of the associated background assumptions. Or an organized procedure to achieve a specific goal. In this chapter there is an explanation of how the proposed system works and the programming language proposed to be used in the implementation with an explanation of some libraries that serve. In addition to the algorithms that will be applied in the proposed system.

3. How Machine Learning Working In Fraud Detection?

To detect fraud, the machine learning model first needs to collect data. Then it analyzes all the data collected, segments, and extracts features from this data. Next, the machine learning model receives training sets that teach it how to predict the probability of fraud. Finally, it creates machine learning models for fraud detection.

Fig (2)

4. Current Sustems

In most of the current systems, machine learning algorithms such as Random Forests, Naïve Bayes, are use random data, and it Requires huge processing time and having small number of columns, so it gives a low fraud detection rate when we compared it with the proposed system .

5. The Proposed System

In the proposed system, we will use an Artificial Neural Network (ANN) to detect fraud in credit card transactions.

And classification algorithm such as Support vector machine (SVM) is used to build a credit card fraud detection model.

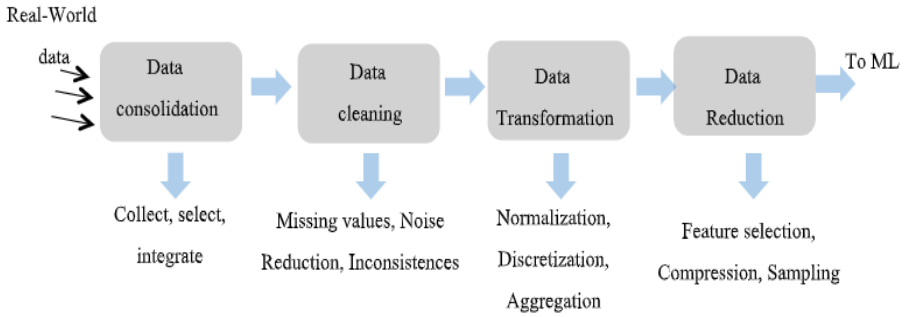
We compared between their work and saw that artificial neural networks predict better.

Advantages Of Proposed System

- Provides high accuracy.
- It has many columns and it useful for increasing the accuracy of fraud detection.
- Added layer of safety

Data Preprocessing

in proposed system the algorithm starts working from loading the dataset, then data pre-processing carried out that includes cleaning and normalizing the data and Dataset is separated into two dataset one for train data and the second for test and model is trained and tested to measure the accuracyFinally, system predicts whether transaction is fraud or non-fraud.



Feature Extraction

It is the method of reducing the input variable by using only relevant data and getting rid of noise in data.

Programming Language Used:

We will use Python as the programming language. Python is a beginner's language, which offers diverse applications. It is easy to use, interpretable, object-oriented, high-level, has the advantage of scripting, and provides rich packages and libraries used in machine learning files.

Libraries Used

Some of the python library used in proposed system are as follows:

1. NUMPY

NUMPY is a python library. Abbreviation of NUMPY is numerical python library. NUMPY package is used for multidimensional arrays and linear algebraic operations.

2. Pandas

Pandas is a python library. Pandas is used for data analysis and data manipulation tool. It is used to read the dataset and load the dataset. It is fast, flexible when working with data.

3. SCIKITLEARN

A python package which is suitable for statistical model and machine learning models. A best suited python package for machine learning modeling.

4. KERAS

KERAS is mainly used while implementing deep learning algorithms such as CNN, RNN because its user friendly, modularity, and easy to extensibility. It runs on both CPU and GPU. In the experiment of finding the fraud or nonfraud credit card.

5. MySQL

MySQL is database which is used for storage purpose. In the experiment of fraud identification in card transaction we had used MySQL for storing the user details namely username, password, email-id and phone number.

6. TKINTER

TKINTER is python library which is used for Graphical User interface (GUI). It can be used on both Unix and Windows platform. We can create it by importing TKINTER module then GUI is created, and one or more widgets are added finally, called in loop.

7. MLxtend

MLxtend is a library that implements a variety of core algorithms and utilities for machine learning and data mining. The primary goal of MLxtend is to make commonly used tools accessible to researchers in academia and data scientists in industries focusing on user friendly and intuitive APIs and compatibility to existing machine learning libraries.

Classification Techniques:

The following algorithms are used in proposed system:

1. Support Vector Machine.
2. Artificial Neural Network.

Data Set

"It is important that credit card companies can recognize fraudulent credit card transactions so that customers are not charged for items that they did not purchase."

The proposed system makes use of the dataset downloaded from

Kaggle website, the dataset contains European cardholder transactions that occurred over two days.

feature descriptions- Time - the seconds elapsed between each transaction and the first transaction in the dataset V1, V2, …, V28 -principal components obtained through dimensionality reduction (PCA) Amount - the transaction amount Class - the response variable, indicating whether a transaction was fraudulent or not.

System Requirments

Hardware:

- Internet connected computer.

Software:

- Windows10 Microsoft
- Microsoft Office Word 2019
- Google Chrome
- Microsoft PowerPoint.
- Google forms creator.
- Kaggle: is a platform for data science and machine learning that allows data scientists to share and analyze code using the Python languages and it is helps in building your own system.

Acknowledgment

I would like to express my sincere gratitude to all those who contributed to the successful completion of the research paper titled “Detection of Fraud in Customer Credit Card Transactions Using Artificial Neural Network Algorithm.” I am deeply thankful to my supervisor, professors, and faculty members for their valuable guidance, continuous support, and constructive suggestions throughout the course of this study. Their expertise and encouragement played a vital role in shaping this research.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Financial Fraud Action UK. (2010). Fraud the Facts 2010. Retrieved December 27, 2010, from Financial Fraud Action UK: https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Prabowo%20card%20fraud.pdf
2. A.A. Taha, S.J. Malebary, an intelligent approach to credit card fraud detection using an optimized light gradient boosting machine, IEEE Access 8 (2020) 25579–25587, doi:10.1109/ACCESS.2020.2971354.
3. C. Jiang, J. Song, G. Liu, L. Zheng, W. Luan, Credit card fraud detection: a novel approach using aggregation strategy and feedback mechanism, IEEE Internet Things J. 5 (5) (Oct. 2018) 3637–3647, doi:10.1109/JIOT.2018.2816007.
4. D. Prusti, S.K. Rath, Web service-based credit card fraud detection by applying machine learning techniques, in: Proceedings of the TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 492–497, doi:10.1109/TENCON.2019.8929372.
5. M. Zamini, G. Montazer, Credit card fraud detection using autoencoders based clustering, in: Proceedings of the 9th International Symposium on Telecommunications (IST), Tehran, Iran, 2018, pp. 486–491, doi:10.1109/ISTEL.2018.8661129.
6. Sadgali, N. Sael, F. Benabbou, Fraud detection in credit card transaction using neural networks, in: Proceedings of the 4th International Conference on Smart City Applications (SCA ’19). Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–4, doi:10.1145/3368756.3369082. Article 95.
7. G. Singh, R. Gupta, A. Rastogi, M. D. S. Chandel, A. Riyaz, "A Machine Learning Approach for Detection of Fraud based on SVM", International Journal of Scientific Engineering and Technology, vol. 1, no. 3, pp. 194-198, 2012, ISSNISSN: 2277-1581.