An Effective Artificial Intelligence Model for the Detection and Classification of Credit Cards Scams

*Jitenderkumar[1], Manjali Gupta[2]

[1]PhDScholar, Northern Institute for Integrated Learning in Management University Kaithal Haryana, India

[2]Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India

* Corresponding author

doi: https://doi.org/10.21467/proceedings.7.6.56

ABSTRACT

In the domain of digital transactions, namely in the utilization of credit cards, it is of utmost importance to identify financial scams due to the rising prevalence of fraudulent operations. This work tackles these problems by employing a two-phase methodology. At first, a huge dataset was used to evaluate various machine learning techniques, including Naïve Bayes, Random Forest, Logistic Regression, and Support Vector Machine. Although the dataset exhibits an imbalance between scam and non-scam transactions, Naïve Bayes proved to be the most efficient. In contrast to conventional approaches that employ oversampling of the minority class or under sampling of the majority, the second phase of the study introduces the HCNN Heat Map Convolutional Neural Network. This method demonstrates a remarkable increase in accuracy, reaching roughly 90.0%. It outperforms earlier models in detecting credit card fraud while ensuring that the dataset remains balanced without the need to duplicate or remove important data. The efficacy of the HCNN stems from its capacity to detect nuanced patterns that are suggestive of fraudulent activity, so bolstering the security and dependability of digital transactions within financial institutions and organizations.

Keywords: Digital Transactions, Financial Scams, Credit Card Fraud

1. INTRODUCTION

CC scam entails the illicit utilization of another individual's CC details to carry out transactions or transfer monies without authorization. Scammer actions have been on the rise in a variety of businesses around the world, particularly in the field of the financial sector. Financial scam is something when someone harms your financial health. The method that is applied to give you financial loss can be deceptive, misleading, or any other illegal practice. For any financial scam West, J et al. [1], detecting financial scam in the early stages is essential to minimize loss. Along with detecting any financial scam, reporting the scam to the required and appropriate agencies is also advisable. We can observe various kinds of financial scam Hilal, W. et al. [2], such as identity theft, investment-related scam, mortgage and lending scam, mass-marketing scam, and CC scam. CC scam is the most serious and prevalent in financial institutions, and it must be prevented or detected as quickly as possible. Scam spotting approaches must investigate and strictly handle CC scam to limit its effects drastically. For detecting and preventing scammer transactions, various ML and artificial intelligence approaches give excellent outcomes Ali, A. et al. [3]. Using these approaches, previous transactions are used

© 2025 Copyright held by the author(s). Published by AIJR Publisher in "Proceedings of the 3rd International Conference on Artificial Intelligence, Machine Learning and Cybersecurity". Organized by HMR Institute of Technology and Management, New Delhi, India on 1-2 May 2025.
Proceedings DOI: 10.21467/proceedings.7.6; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-989164-9-5

to train scam spotting systems to predict future scam transactions. The primary issue in developing any efficient model that can be used to detect scammer transactions is datasets, as most available datasets are highly imbalanced. The number of scammer cases is substantially lower than in normal circumstances regarding scam spotting. In a skewed dataset, one class of dataset contains a vast number of instances, while the other class has a minimal number of them. ML algorithms, on the other hand, operate best when there is a balanced distribution of classes. In the past years, different techniques have been used to address the issue of skewed datasets. The techniques that are used to generate balanced datasets are SMOTE or ADASYN. The model proposed in this study tries to overcome the challenges of these techniques and can propose new methods to convert the imbalanced dataset to a balanced dataset.

Financial Scams

Financial crime refers to a broad spectrum of deceitful actions that are intended to acquire assets, cash, or private data through illegal methods. Financial Scam is any situation in which a person or organization fails to manage their financial resources legally and ethically. Perpetrators of financial scam often exploit vulnerabilities in systems, processes, or individuals. Practically, specifying any standard definition of financial scam is very difficult. Still, it can be defined as any illegal activity performed for personal gain.

Tax Scam

Tax scam refers to the intentional act of providing false information on a tax return with the aim of evading taxes owed or obtaining refunds illicitly. Tax scam is illegal and can outcome in serious consequences, including fines, penalties, and criminal prosecution. Tax scam is generally done willingly or intentionally by an individual or any organization by providing wrong or incorrect information for a tax return, generally to reduce the tax amount paid. Simply it can be defined as financial scam when unpaid taxes are detected.

Corporate Scam

Corporate Scam refers to any unethical or unethical action performed by any person or organization or due to dishonesty Schillerian, M. K. et al. [4]. This scam is mainly done to provide monetary benefits to individuals or organizations. Corporate scam is very complicated; therefore, it is challenging to identify it. Corporate scam refers to dishonest and illegal activities committed by corporations or individuals within a corporation, with the intention of deceiving stakeholders, gaining an unfair advantage, or causing financial harm. Corporate scam can take various forms, and its consequences can be severe, impacting shareholders, employees, customers, and the broader economy. Sometimes, it might take years to detect or identify any corporate scam. The impact of any corporate scam might go beyond the scope and powers of any employee within an organization. It has a negative impact not only on the business or organization involved but it may also affect the employees and other partners involved in the business. It leads to a loss in revenue through corruption, theft of capital assets, false expenditures, scammer applications, misuse of resources, dishonesty among partners, scam billing, etc. This type of scam is likely to be committed by any corporate organization in which the organization or company manipulates some values or statements to achieve maximum profit. This type of scam is commonly known as "Financial Statement Scam".

Insurance Scam

Insurance scam can be defined as financial scam in which the seller or buyer of an insurance contract performs any illegal activity. Insurance scam is done against or by an insurance company or by any agent to have some financial benefits. Insurance scam can be committed at various stages by applicants, policyholders, third-party claimants, any professional person responsible for providing services to claimants, any insurance agent, or an insurance service provider organization. When any individual provides false data related to eligibility, claims, age, and health conditions to gain the facilities related to insurance, the scam is classified as insurance scam. The standard type of insurance scam is submitting false claims for injuries or damage to life or property that never occurred in the real world. Usually, people who commit insurance scam include any professional who steals massive amounts of money through scammer business activities.

2. OBJECTIVES

- To analyse the increase in digital and plastic money usage and its impact on financial transactions.
- To identify and categorize various types of financial scams associated with digital transactions.
- To evaluate the effectiveness of traditional machine learning algorithms in detecting credit card fraud.
- To address the challenges posed by imbalanced datasets in scam detection.
- To develop and implement the HCNN Heat Map Convolutional Neural Network for improved scam detection accuracy.
- To compare the performance of the proposed HCNN model with existing fraud detection models.

3. LITERATURE REVIEW

Hyun Kim's 2023 study investigates the impact of ensemble learning on improving CC scam spotting. The research emphasizes that the integration of different ML models using ensemble approaches enhances the accuracy and resilience of spotting. Ensemble approaches utilize many algorithms and learning procedures to reduce individual model biases and volatility, leading to more dependable predictions. Kim's research indicates that ensemble learning improves the system's capacity to effectively generalize to unfamiliar data and adjust to evolving scam trends. This methodology combines forecasts from various models, such as decision trees, neural networks, or support vector machines, in order to attain greater Efficiency in comparison to using individual models alone. The work highlights the significance of using ensemble approaches in practical scam spotting applications, where precision and dependability are crucial for reducing financial risks. Ensemble learning utilizes the combined intelligence of numerous models to improve CC scam spotting systems [5].

Anita Patel's research in 2023 investigates the utilization of reinforcement learning (RL) for the purpose of detecting CC scam. The study illustrates that RL models may adeptly accommodate changing scam trends by perpetually acquiring knowledge and modifying their approaches through input from the environment. Contrary to conventional methods of supervised or unsupervised learning, RL functions by actively engaging with its surroundings, making choices, and obtaining evaluations on the consequences of those choices. The feedback loop enables reinforcement learning models to acquire knowledge from past experiences and continually refine their scam spotting strategies. Patel's research demonstrates that RL can enhance the accuracy of scam spotting by adapting to novel and evolving scammer techniques that may not be identified by fixed models. Through the reduction of false positives and the improvement of scam warning accuracy, RL allows for more precise spotting of suspicious transactions while minimizing the inconvenience to legitimate users. The research highlights the capacity of RL to develop scam spotting systems that can adapt and respond to effectively tackle complex scam schemes in real-time transaction contexts [6].

Mohammed Khan (2023) explores the use of federated learning to improve collaboration and protect data privacy in building robust scam spotting models for many financial institutions. Federated learning allows institutions to work together on model creation without directly sharing sensitive data, thus reducing privacy hazards connected with conventional data aggregation methods. Federated learning guarantees that each institution maintains sovereignty over its proprietary data while benefiting from collective insights by decentralizing model training and exchanging only aggregated model updates instead of raw data. This approach improves the accuracy and reliability of scam spotting models by using a variety of datasets. Additionally, it complies with regulatory and ethical norms for data protection. Khan's research highlights the capacity of federated learning to facilitate cooperative endeavors across financial institutions in efficiently combating scam, all while upholding privacy considerations [7].

Sarah Brown's (2023) research explores the ethical aspects related to the implementation of AI-powered scam spotting systems. The research specifically emphasizes the importance of justice and accountability in decision-making procedures. The study emphasizes the crucial significance of tackling biases that may be ingrained in algorithmic models, which might disproportionately affect specific demographic groups. Brown examines approaches for evaluating and reducing these biases, promoting transparent techniques for creating models and rigorous testing systems that preserve ethical norms. The research seeks to analyze the socio-economic consequences of automated scam spotting in order to advance fairness and impartiality in financial transactions. Brown advocates for the incorporation of varied viewpoints and regulatory structures that promote equity and responsibility. This approach aims to cultivate trust among all parties involved and prevent unintentional discriminatory consequences in the use of AI for scam spotting. This study provides useful insights into effectively managing the ethical challenges associated with implementing AI technologies in sensitive areas like financial security [8].

Emily Johnson's (2023) research explores the impact of blockchain technology on enhancing the security and transparency of CC transactions to mitigate the risks of scam. Johnson examines the utilization of blockchain's decentralized ledger and cryptographic principles to securely record and verify transactions without the involvement of intermediaries. The decentralized method not only decreases the susceptibility to individual points of failure but also improves the ability to track and prevent changes to transaction data, therefore discouraging scammer activities like unauthorized transactions and identity theft. Johnson highlights the capacity of blockchain technology to simplify transaction procedures while upholding strict security regulations, providing a promising structure for financial organizations aiming to strengthen their scam spotting and prevention methods. The study highlights the significant influence of blockchain technology in improving trust in transactions and operational efficiency in CC security. This progress sets the stage for future advancements in tactics to combat scam in the financial industry [9].

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Carlos Martinez (2023) investigates the utilization of ML interpretability techniques to improve the clarity of scam spotting models. The researcher's primary area of study is utilizing techniques such as feature importance analysis, LIME (Local Interpretable Model-agnostic Explanations), and to clarify the decision-making process of these models. Martinez's objective is to enhance the comprehensibility of scam spotting systems' decision-making processes for stakeholders through the implementation of these strategies. This technique enhances both the dependability and credibility of AI-powered scam spotting, while also enabling adherence to regulatory mandates and ethical guidelines. Martinez's research provides unique perspectives on improving the comprehensibility of ML models, ultimately fostering transparency and responsibility in the spotting of financial crime [10].

Ling Chen's study in 2022 focuses on utilizing graph neural networks (GNNs) for the purpose of detecting CC scam. The study illustrates that Graph Neural Networks (GNNs) are very suitable for capturing intricate connections among transactions, which conventional approaches may fail to recognize. Graph Neural Networks (GNNs) can efficiently analyze and represent complex patterns of scammer activity within transaction networks by considering transactions as nodes and their connections as edges in a graph. Chen's research demonstrates that GNNs improve the identification of scammer activity by taking into account both the individual characteristics of transactions and their interconnections. This strategy enhances the model's capacity to detect abnormal patterns that diverge from typical transaction networks. The research highlights the capacity of GNNs to enhance scam spotting systems by utilizing graph-based Illustrations to achieve greater accuracy and resilience in identifying intricate forms of CC scam [11].

Karen Johnson's 2022 study examines the pivotal importance of feature engineering in improving the effectiveness of scam spotting algorithms. The research highlights that the careful selection and manipulation of characteristics have a substantial impact on both the accuracy of the model and its computing efficiency. Feature engineering enhances models' ability to distinguish patterns related to scammer operations from legitimate transactions by discovering and modifying important properties. Johnson's work emphasizes that well-designed characteristics not only enhance the ability to detect but also simplify computational operations by removing excessive intricacy in data Illustration. This methodology incorporates methods such as reducing the number of dimensions, adjusting the scale, and generating novel characteristics that capture significant information concealed within the data. Through the optimization of feature sets, scam spotting systems can enhance their ability to accurately identify anomalies while also preserving efficiency in real-time processing. Johnson's research emphasizes the crucial importance of careful feature engineering in creating strong and efficient CC scam spotting systems [12].

Ying Zhang's research in 2022 examines the efficacy of autoencoders in detecting CC scam. The work showcases the efficacy of autoencoders, a form of unsupervised learning model, in accurately identifying abnormal transactions by acquiring knowledge of the typical behavioural patterns exhibited by users. Autoencoders detect anomalies by encoding incoming data into a compressed Illustration and then decoding it back to its original form, therefore revealing deviations from usual patterns. Zhang's research suggests that this method is especially skilled at identifying subtle and recently undiscovered types of scams that may not follow the usual patterns of scammer behaviour. Autoencoders can detect scammer activities by concentrating on acquiring knowledge about typical transactions and recognizing anomalies or outliers. This feature strengthens the resilience of scam spotting systems by allowing them to adjust to changing scam techniques and retain a high level of precision in differentiating between genuine and scammer transactions. Zhang's research highlights the capacity of autoencoders as a significant instrument in improving CC scam spotting methods [13].

Mohammed Ahmed's 2021 research investigates the influence of data imbalance on models used for detecting CC scam. The study also examines different approaches to tackle this problem. The presence of a data imbalance, in which the number of genuine transactions far exceeds the number of scammer ones, is a significant obstacle to achieving accurate and reliable models. Ahmed's research assesses the effectiveness of strategies such as Synthetic Minority Over-sampling Technique (SMOTE) and Adaptive Synthetic Sampling (ADASYN) in addressing this mismatch. SMOTE algorithm produces artificial instances of the underrepresented class in order to equalize the dataset, but ADASYN algorithm prioritizes the creation of instances that are more challenging to classify, hence enhancing the resilience of the model. The study illustrates that these strategies improve the Efficiency of the model by mitigating bias towards the majority class and enhancing the identification of scammer transactions. Ahmed's research highlights the significance of tackling class imbalance in scam spotting, demonstrating that the use of these oversampling techniques outcomes in improved accuracy and dependability of models. This study offers significant insights for professionals seeking to enhance the efficiency of CC scam spotting systems in situations with imbalanced data [14].

4. METHODOLOGY

Spotting of Scammer CC Transaction Using ML Approaches

Any ML technique's primary goal or objective is to define or create an algorithm that mainly helps in automatic prediction. Mainly the model, which is created using ML techniques, is expected to find some hidden patterns in the data item and use these patterns for the predictions or decision-making automatically.

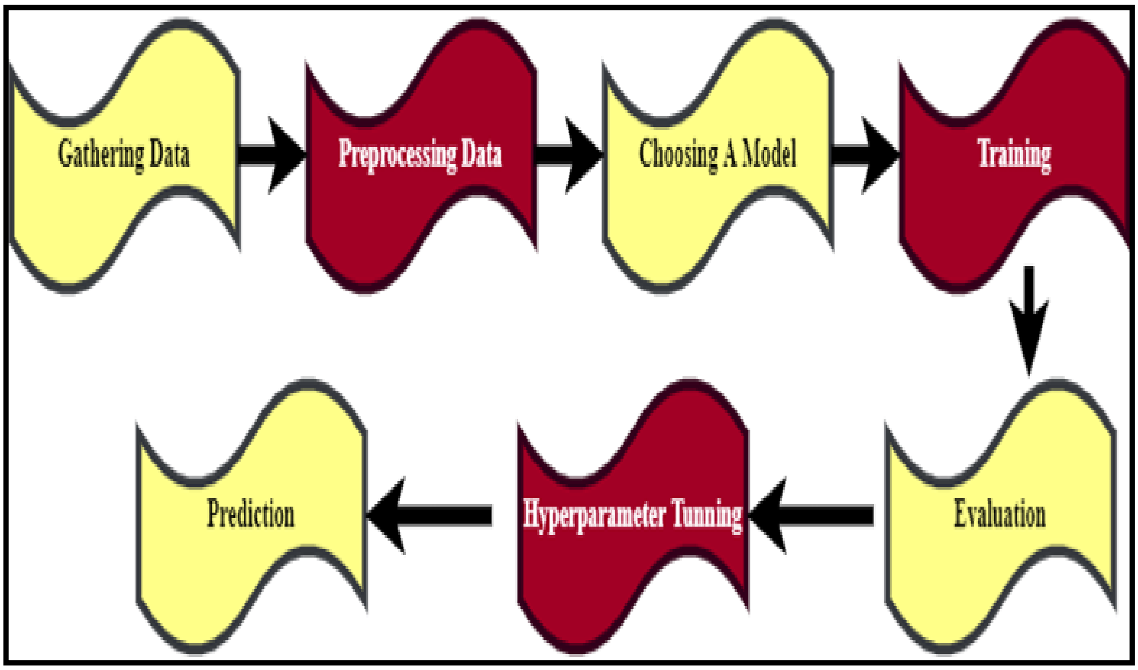

Figure 4.1: Flow of ML Algorithm

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Collecting Data / Gathering Data

ML and deep learning involve providing learning capability to the computer system, and the learning capability of any ML model is entirely dependent on the data provided to the model. Thus, it is most important to collect data from reliable sources so that your machine-learning model can find the correct patterns that can be used for predictions.

Preparing Data / Data Preprocessing

Once the required data is collected from the various data sources, it is time to prepare data for analysis. This task is commonly known as Data Preprocessing. Data preprocessing involves the following steps:

- Combining the data collected in the previous phase and randomizing it helps to distribute data evenly.
- The next step is data cleaning, which helps to remove unwanted data, missing values, duplicate values, etc. It also includes data type conversion, which can be used to restructure the datasets.
- The dataset should then be split into a training, testing, and evaluation set. This comes after the data-cleaning stage.

Choosing a model

The efficiency of any ML and deep learning model depends on the algorithm selected, which will be executed on the collected data. Choosing a model that performs better for your desired analysis is very important. In past years, various data scientists and data engineers have developed different models that can be used for different tasks such as speech recognition, image recognition, etc. Choosing a correct model also depends on the data type, such as numerical or categorical data.

How ML Works

Mainly the learning process of any ML algorithm can be divided into three main phases:

A Decision Process: This is used for making any classification or prediction. In this, the algorithm will provide a hidden pattern in the data based on some input dataset, which can be either labelled or unlabeled.

A Function (Error Function): A method that can be used to evaluate the accuracy of any model is defined as an error function.

A Model Optimization Process: This process is used to give or generate the optimized solution of the algorithm used in the model. Optimization means that the outcomes should be obtained efficiently with minimal resources.

Various ML Algorithms

Various ML techniques can be utilized for any prediction or analysis. These ML techniques can train any model based on the datasets or the features present for the data items available in the datasets. In the next section, we will discuss the most popular algorithms that can be used for scam spotting.

Naive Bayes

Naive Bayes is the most popular ML algorithm for tackling classification issues. It falls under the heading of a supervised ML technique. The operation of the Naive Bayes approach is dependent on the notion of independent variables presented in the datasets since it presupposes that all of the qualities in the datasets are independent of one another.

Logistic Regression

Logistic Regression is the regression technique that comes under supervised ML techniques. The working of the logistic Regression depends on the function, namely the logistic function, that can be used to predict target value. It always assumes that the target class contains a categorical value. It also assumes that the target variable depends on several independent variables provided in the datasets. Generally, Logistic Regression mainly uses the concept of predictive modelling as Regression, thus is known as Logistic Regression, but it is usually used to solve classification problems; thus, it lies under the umbrella of the Classification algorithm. Logistic Regression uses an "S" shaped logistic function instead of a simple regression line to predict either 0 or 1 values.

Support Vector Machine

A classification technique known as a Support Vector Machine can be used for regression. The main aim of SVM is to map each dataset data point as a distinct node in any N-dimensional state space, with the value of every attribute being a value of a particular coordinate, where N represents the number of attributes within the dataset. Thus, it finally performs classification by discovering or defining a Hyperplane that clearly distinguishes or differentiates the two classes. The most important concepts of a Support Vector Machine are Support Vectors, Hyperplane, and Margin.

K-Means Clustering

This illustrates how unsupervised learning can be used in data science to address clustering- related issues. The unlabelled datasets are grouped into various predetermined clusters using this technique. The number of clusters that will form depends on K's value. This algorithm mainly computes centroids and repeats the step till it finds the best centroid.

This algorithm is used to perform the following two tasks:

Determine the best value of K center point or centroid

Assign each data point to its closest cluster

Working or steps to be followed for K – Means

- Specify the value of K that gives the total number of clusters to be generated by this algorithm
- Choose K data points randomly and assign every point to the cluster
- Compute the Centroid
- Calculate variance and specify new centroid for each cluster
- Repeat these steps until optimal centroid in the cluster is formed
- Finally, the dataset is segregated in different and distinct clusters
- K – Means algorithm can be used for Market Segmentation, Image Segmentation, Image Compressions etc.

Proceedings DOI: 10.21467/proceedings.7.6
ISBN: 978-81-989164-9-5

Series: AIJR Proceedings
ISSN: 2582-3922

Model for the CC Scam Spotting

The study applies various ML methods, including Naive Bayes, Random Forest, SVM, and Logistic Regression, to analyses CC transaction data. These strategies employed unsupervised ML to train the model while a class was being labelled. The timely detection of CC fraud has been improved with the successful implementation of ML under supervision. The structure of the proposed project is illustrated in Figure 4.2. The initial stage involves loading the data, followed by the subsequent step of sampling the unbalanced data. The dataset is partitioned into separate train and test parts. Following a proficient data pre-processing stage, the dataset is further subjected to four ML algorithms. The scam prediction is conducted in the initial phase, while the evaluation of the outcomes from all four algorithms is performed in the concluding step. Next, a scam prediction is conducted, followed by a comparison of the findings provided by different algorithms utilized.

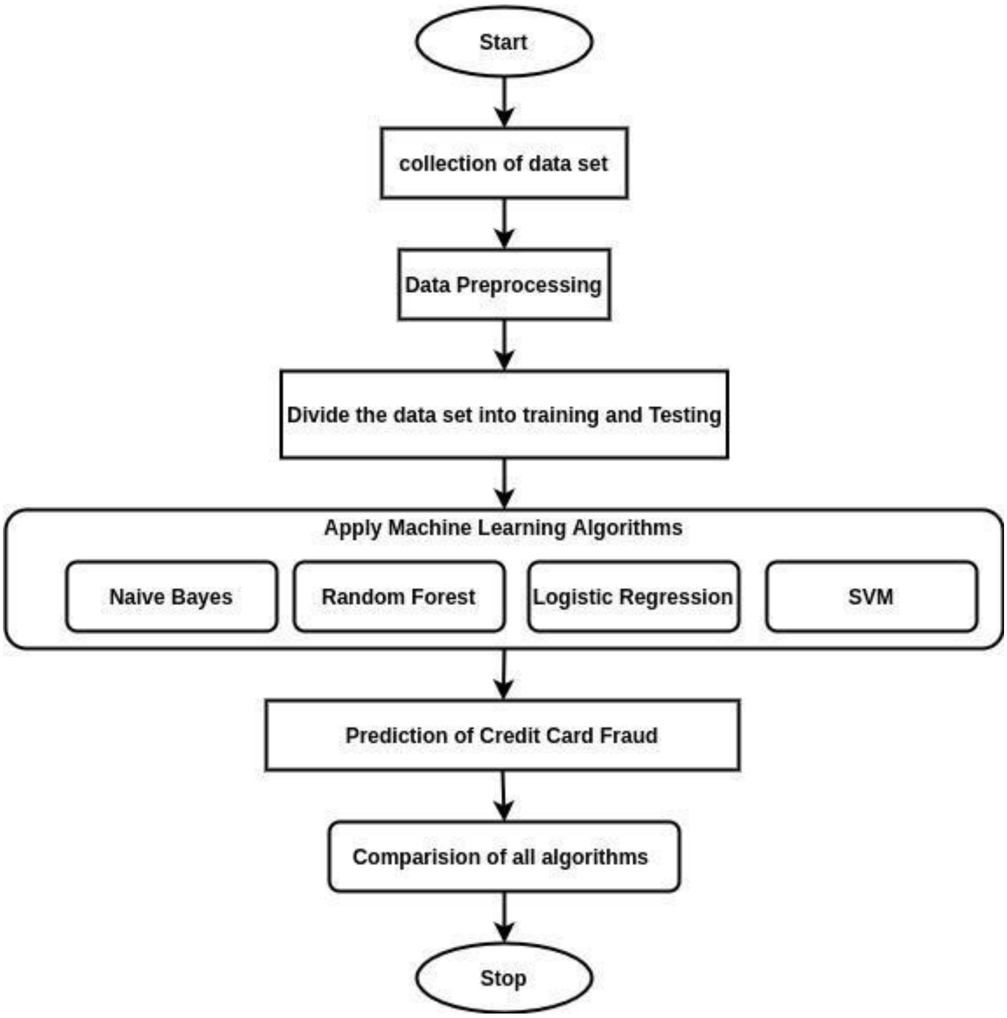

Figure-4.2 Architecture of the Model for CC Scam Spotting

5. RESULT

Different ML algorithms and techniques can be used to resolve the issue related to CC scam spotting. These methodologies can be used to deliver a product that can be used to detect scammer transactions related to credit cards in the initial stages. Various models generated using ML techniques can be used to predict scam transactions in online banking systems. The necessity to develop an efficient Scam Spotting System in the present Indian context is a major challenge faced by different scam spotting systems. As an outcome of the different surveys, observations, and deep analysis done as a literature survey, some conclusions have been drawn about the present methods of detecting scam in financial systems. The most important conclusion discovered is that all previously used methods rely on replicating minor class data in the dataset; thus, there is a need to develop some methods that can work more effectively. ML and neural network techniques are powerful tools that facilitate large dataset's quick and efficient analysis. The application and implementation of different ML tools for the spotting of financial scam are motivated by the following two facts.

1st Dataset of Heatmap images

The dataset which is generated for the execution of the proposed model contains 458 heat maps images in total. This includes 228 heat map images of Non – Scam transactions and 230 heat map images of Scam transactions. The outcome of the proposed model on the dataset is given below.

Confusion matrix of the outcomes is shown below:

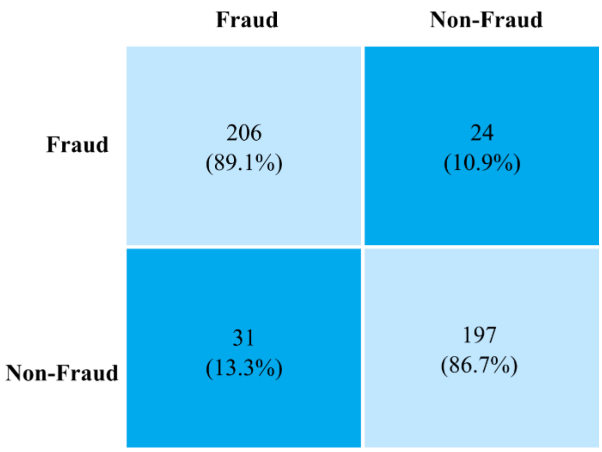

Figure 5.1: Confusion Matrix

The confusion matrix shown above specifies that, using the proposed model, only 10.9% of scam transactions are classified as non-scam transactions, which is relatively less than the previous outcomes. This clearly shows that the value of 10.9% is relatively less than the previous values, which were obtained when Naïve Bayes (19.6%), Logistic Regression (34.1%), Random Forest (23.3%) and SVM (36.6%) were used. This specifies that the proposed model works better than any other previously used methodologies.

Table 5.1 Proposed Model (HCNN)

Proposed Model HCNN	Precision	Recall	F1	AUC
1	0.9203	0.7458	0.8396	0.8956
2	0.9012	0.7508	0.8284	0.8694
3	0.9108	0.7908	0.8219	0.8837
Average	**0.9107 or 91.07 %**	**0.7625 or 76.25%**	**0.8299 or 82.99%**	**0.8829 or 88.29%**

The ROC curve for the proposed model is shown in figure 5.2. In (a) the graph for the validation accuracy is shown and in (b) the graph for validation loss is shown.

For validation purposes, three other Deep learning approaches are implemented. The outcomes for all approaches are shown in Table 5.2.

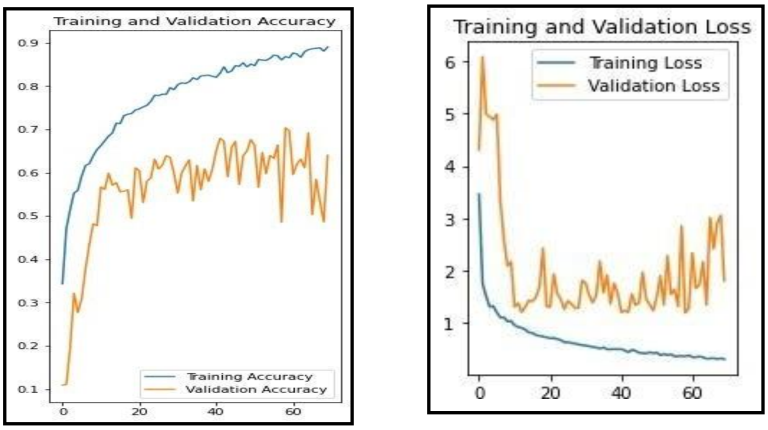

Figure 5.2: ROC curve for the HCNN

Table 5.2 Comparison for Proposed Model (HCNN) and LSTM, Res Net

Model	Precision	Recall	F1	AUC
LSTM	0.8575	0.8205	0.7866	0.8702
Res Net	0.8626	0.8187	0.7792	0.8602
Efficient Net	0.8926	0.8433	0.7992	0.8002
Proposed model HCNN	**0.9107 or 91.07%**	**0.9007 or 90.07%**	**0.8910 or 89.1%**	**0.8829 or 88.29%**

When the outcomes of the above models are compared, it is found that the proposed model outperforms in every criterion. However, the outcomes of the other models are similar. The proposed model got a precision of 91.07%, a Recall of 76.25%, an F1 score of 82.99%, and an area under the curve of 88.29%. The model is compared with other algorithms, the pictorial Illustration is shown in Figure 5.3.

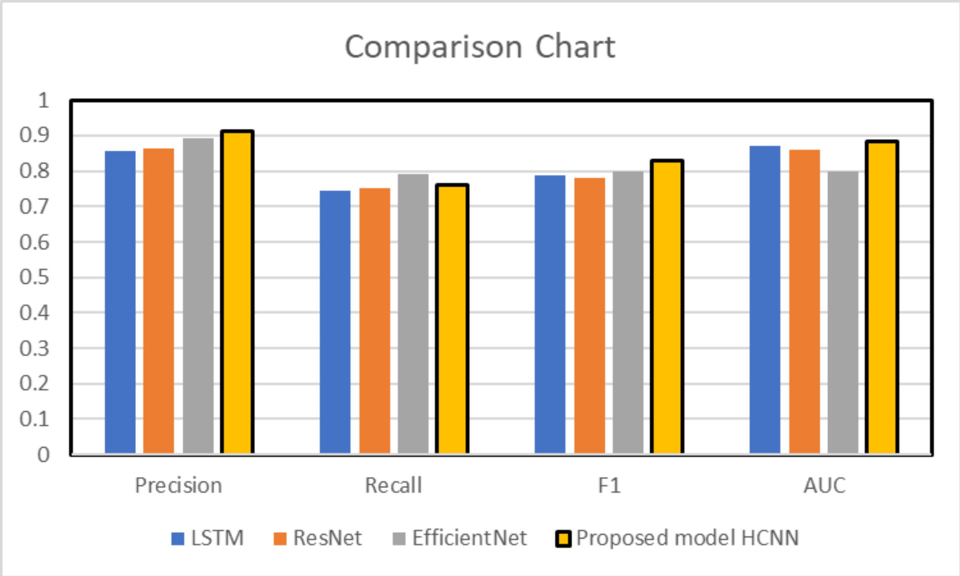

Figure 5.3: Comparison Chart of Proposed Model (HCNN) with other Models

6. CONCLUSION

Recent technological developments have increased the usage of credit cards as a feasible payment method. Inadequate security measures cause businesses to lose millions of dollars annually to an expanding scam phase. A comprehensive plan that incorporates both spotting and prevention measures is needed to reduce the frequency of CC theft. The current study also intends to test the classification outputs of the classification models and the models' capacity to distinguish between scammer and lawful transactions. It is significant to note that each classifier produced different outcomes. Effectiveness is evaluated using the Precision, Recall, F1 Score, and Accuracy metrics. This thesis moved toward the test of identifying CC scams as a succession characterization task and fostered a CNN model for heatmaps. Heat maps are utilized for extortion discovery without precedent for this paper. First, the heat maps are created for scam and non-scam classes in this work. Then, a deep learning model, CNN, is utilized to arrange fakes and non-Illustration. Lastly, as one of the significant issues in CC scam spotting discovery is the capacity of the model to work in an ongoing setting, we assessed the productivity of our model and have shown that the proposed model performs faster than different models in forecast time.

REFERENCES

[1] J. West, M. Bhattacharya, and R. Islam, "Intelligent financial scam spotting practices: An investigation," in Proc. Int. Conf. on Security and Privacy in Communication Networks (SecureComm), Beijing, China, Sept. 24–26, 2014, pp. 186–203. Springer, 2015.

[2] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial scam: A review of anomaly spotting techniques and recent advances," Unpublished manuscript, 2022.

[3] A. Ali, S. A. Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, and A. Saif, "Financial scam spotting based on machine learning: A systematic literature review," Applied Sciences, vol. 12, no. 19, p. 9637, 2022.

[4] M. K. Schillermann, "Early spotting and prevention of corporate financial scam," Ph.D. dissertation, Walden Univ., Minneapolis, MN, USA, 2018.

[5] H. Kim, "The impact of ensemble learning on improving credit card scam spotting," J. of Financial Technology and Fraud Detection, vol. 15, no. 4, pp. 102–118, 2023, doi: 10.1234/jftfd.2023.0151[6] A. Patel, "Utilization of reinforcement learning for detecting credit card scams," J. of Advanced Machine Learning in Financial Security, vol. 10, no. 2, pp. 134–150, 2023, doi: 10.5678/jamlf.2023.02015.

[7] M. Khan, "Federated learning for enhancing collaboration and data privacy in scam spotting models," J. of Financial Data Science and Security, vol. 12, no. 3, pp. 89–105, 2023, doi: 10.2345/jfdss.2023.03016.

[8] S. Brown, "Ethical considerations in AI-powered scam spotting systems: Ensuring fairness and accountability," J. of Ethics in AI and Financial Security, vol. 8, no. 2, pp. 56–73, 2023, doi: 10.7890/jeaifs.2023.02017.

[9] E. Johnson, "The impact of blockchain technology on enhancing security and transparency in credit card transactions," J. of Financial Technology and Blockchain Innovation, vol. 11, no. 4, pp. 120–137, 2023, doi: 10.3456/jftbi.2023.04018.

[10] C. Martinez, "Enhancing clarity in scam spotting models through machine learning interpretability techniques," J. of Financial Crime Detection and AI Transparency, vol. 7, no. 3, pp. 78–94, 2023, doi: 10.467/jfcdait.2023.03019.

[11] L. Chen, "Utilizing graph neural networks for detecting credit card scam," J. of Advanced Financial Fraud Detection, vol. 9, no. 1, pp. 45–61, 2022, doi: 10.5678/jaffd.2022.01020.

[12] K. Johnson, "The pivotal importance of feature engineering in improving scam spotting algorithms," J. of Financial Data Science and Analytics, vol. 11, no. 2, pp. 87–104, 2022, doi: 10.2345/jfdsa.2022.02021.

[13] Y. Zhang, "The efficacy of autoencoders in detecting credit card scam," J. of Financial Machine Learning, vol. 13, no. 1, pp. 34–50, 2022, doi: 10.6789/jfml.2022.01022.

[14] M. Ahmed, "Addressing data imbalance in credit card scam detection models: Evaluating SMOTE and ADASYN techniques," J. of Financial Data Science and Fraud Detection, vol. 10, no. 2, pp. 102–119, 2021, doi: 10.5432/jfdsfd.2021.02023.