Advancing Transaction Security in Banks: A Blockchain-Driven Solution for Mitigating Challenges in Imbalanced Financial Data

Nazmul Karim Tanvir
nazmulkarimtanvir@g.bracu.ac.bd
Brac University
Dhaka, Bangladesh

Ishrat Jahan Easha
ishrat.jahan.easha@g.bracu.ac.bd
Brac University
Dhaka, Bangladesh

Mosa. Rabeya
mosa.rabeya@g.bracu.ac.bd
Brac University
Dhaka, Bangladesh

Fatima Tabassum
fatima.tabassum@g.bracu.ac.bd
Brac University
Dhaka, Bangladesh

Abstract

As emerging blockchain technology offers one of the most enhanced means of providing security for any given transaction and this is an improvement than the old fashioned banking systems, most especially in financial systems that are highly susceptible to frauds. With this, the study is based on creating a new banking system based on blockchain where there are fraud detectors considering the problems of reaching out to the imbalanced financial data sets. These are aimed at improving the level of accuracy of fraud transaction detection by using various data preprocessing techniques such as Synthetic Minority Over-sampling Technique (SMOTE) in combination with blockchain technologies. System was validated using 3 different datasets, Credit Card Fraud Detection, Paysim1 and bank marketing data with 98.5%, 95% and 85% accuracy achieved respectively. Using these sets of data, we are going to create an environment of transactions that is completely decentralized, secure and transparent. The addition of machine learning models due to the addition of SMOTE in terms of effective use of skewed data improved the system's efficiency in avoiding fraudulent activities very significantly. Apart from that in this study, the process of the Blockchain has been elaborated starting from the point of collecting the transactions, validating them, making the blocks and checking the integrity of the proposed system's blocks and efficiency has been improved at every stage.

Keywords

Blockchain, Distributive Architecture, synthetic oversampling techniques, SHA-256, Imbalanced Datasets

ACM Reference Format:
Nazmul Karim Tanvir, Ishrat Jahan Easha, Mosa. Rabeya, and Fatima Tabassum. 2024. Advancing Transaction Security in Banks: A Blockchain-Driven Solution for Mitigating Challenges in Imbalanced Financial Data. In . ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

In today's busy world of finance, it is impossible to find any bank which does not examine a large volumes of transactions on a daily basis so making even a small breach on the data vulnerability is unacceptable. Unfortunately, a lot of old school banking practices still rely on a single database which is quickly falling prey to problems such as hacking, scams, and data theft. Such security lapses are not only incurring severe malpractices which may cause recession to the industry but also taint the confidence which banks have on customers

All these problems have a brilliant way to be solved – by introducing Blockchain technology. Whether it's a horizontal or vertical structure, there is one thing that lifts up blockchain a notch above however and this is its accountability and undeniable nature. This has been made possible as all transactions are FOREWORD: This descriptive study reports on participants' and stakeholders' views about engagement with the Internet for the purpose of exchanging data. Blockchain networks (systems) can help to provide security for the banks themselves. The increasing demand to enhance security and confidence in the banking industry encourages this prospect. The motivation for this project originates from the desire to create security and confidence in the banking industry. Safeguarding the information of the customers during these transactions and also ensuring the data of these transactions is kept confidential, has really placed these banks in a very difficult position. The idea is simple: the potentials of Blockchain coupled with decentralist systems[13].

With the introduction of the blockchain-based system for bank transactions, this project seeks to demonstrate how much equipment disturbance the blockchain has latent within the stone age of contemporary societies where banking systems reside. The objective is to assist in instilling confidence in clients and ensure that transactions are executed effectively in a more secure banking system, where management of transaction information does not result in either modification or fraud[**?**].

1.1 Research Objective

This study seeks to develop the blockchain as a technology without developing new currencies and using it solely for secure, effective, and quick recording of the financial transaction. It will investigate the ways in which transaction anonymity can be provided within a blockchain system without compromising the ability to prevent fraudulent transactions. One central area of intervention will include bringing in artificial intelligence in the form of machine learning together with blockchain to solve the challenges of imbalanced datasets for risk appetite in making financial decisions.

The main objective of this examination is to establish the effectiveness of such a proposed blockchain model which has been discussed in the provisions as applied to other types of transaction datasets. Therefore, the experiment will employ the data management techniques based on traditional approaches and blockchain to establish fairness, reliability, and efficiency among other factors while evaluating the performance of blockchain. It will further investigate the limits of blockchain due to its modular nature, flexibility, and data substitution especially on transaction types. In the context of real-world applications, the study seeks to establish if blockchain technology can act as a better way of administering transaction data management across various fields in all of its aspects: security, transparency, and justice.

2 Background Studies

Enhanced technology has resulted in the generation of vast amounts of data within, business, finance, banking, agriculture, education, health and medicine. In order to uncover patterns and valuable information within the data, more adaptable data processing tools and platforms are required due to the constant increase in the diversity of data sizes and formats[5].

According to published literature, numerous research conducted in recent years using varying methodologies for the aforementioned goals have been documented. Tahani et. al. (2024) This study was conducted on Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection Systems. The paper integrates federated learning and blockchain for credit card fraud detection, enhancing accuracy and privacy. It demonstrates improved performance but lacks real-world validation. Future research should test with real-world data and explore advanced privacy techniques[2]. Olubusola et. al. (2024) This article was based on Integrating ai with blockchain for enhanced financial services security. The paper integrates AI with blockchain, improving financial security by 30% in fraud detection. Future work includes testing with real-world data and enhancing scalability with advanced AI techniques[9]. Clement et al. (2024) This article was conducted on Enhance Zero Trust Models in the Financial Industry through Blockchain Integration. The framework focuses on identity and access management, device and network security, and data protection with Blockchain providing enhanced integrity and verification. They use models for security testing- SQL injection, brute-force, CSRF attacks and for performance testing-transaction latency, system throughput. Future work includes integration with other emerging technologies such as AI or machine learning to improve threat detection and response mechanisms. The current implementations of Zero Trust in the financial sector face challenges related to scalability, particularly when integrated with Blockchain. Implementing Blockchain into the Zero Trust model adds complexity to the security infrastructure[4]. Parth et al. (2021) This paper was conducted on Comprehensive Analysis for Fraud Detection of Credit Cards through Machine Learning. Multiple machine learning algorithms including Local Outlier Factor, Isolation Forest, SVMs and LR are trained on the dataset. They got the best accuracy from Isolation Forest which is 99.74%. Future work includes more diverse and extensive datasets to better capture various fraud patterns and improve model generalizability. The dataset used may not represent all types of fraud scenarios, potentially affecting the generalizability of the results. Some machine learning models, particularly neural networks, can be complex and resource-intensive, which may limit their practical deployment. Kuldeep Singh et al. (2023) proposed a blockchain-based solution to enhance financial transaction security and efficiency in digital banking using smart contracts. Through a systematic review of 35 articles from Web of Science and Google Scholar, the study identified key blockchain, AI, and machine learning enablers that improve transparency, reduce fraud, and build trust. Results show blockchain automates contracts, reduces costs, and strengthens cybersecurity. Future research should address scalability, energy use, and regulatory challenges for wider adoption[10]. Laila Junaid et al. (2024) proposed a blockchain-based framework to improve transparency and efficiency in land lease and mortgage management. Implemented on the Ethereum blockchain, the system addresses issues like fraud and double spending, while enhancing security, scalability, and user involvement. Future research should focus on resolving scalability challenges for wider adoption[6]. Awotunde et al. (2021) proposed a blockchain based framework that highly augments the security and privacy of mobile banking transactions. A multi-layer authentication with TOTP (time-based one-time passwords) is used by the system. This outperforms existing solutions by a great margin, which in result prevents replay attacks and various security breaches. There are plans of improving scalability which will support a larger number of stakeholders without much increase in computational costs[1]. Bakir et al. (2022) suggested a BKSM (blockchain based special key security model), that addresses various security challenges in larger environments by leveraging path compression algorithms. Through the use of a special key that controls access to data, it greatly augments the integrity, availability and confidentiality during CRUD operations such as, read, write, update and delete. Tests have yielded better performance when it comes to accuracy and time in contrast to traditional methods, which were done on banking and financial datasets. They even proposed to scale up the model with multi-key support as well as a functional prototype for real use applications[3]. S P Maniraj et al. proposed The Credit Card Scam Uncovering using ML and Data Science approach. That one is still fighting to ensure that large recognition card companies are able to identify fraudulent recognition card transactions and protect customers from being charged for goods they did not purchase. Machine Learning assumes such malfunctioning containers. Credit Card Scam Identification Problematic includes displaying past credit card transactions using data from those that turned out to be scams [8]. BacCPSS, a blockchain-based access control framework for big data in cyber-physical social systems, was proposed by Tan et al. It is crucial to use blockchain features to protect access control privacy in CPSS big data. The account give an address to the blockchain node with access control permission is redesigned and saved in the blockchain using BacCPSS. Authorisation is another goal of BacCPSS's audit and access control systems. The findings demonstrated the viability and effectiveness of BacCPSS, which could provide private privacy protection and secure access in CPSS [11].

3 Methodology

The process followed for validating and storing transactions in a blockchain-based system ensures the integrity, security, and decentralization of a transaction. The following outlines the steps involved in creating, validating, and adding a new block to the blockchain[7].

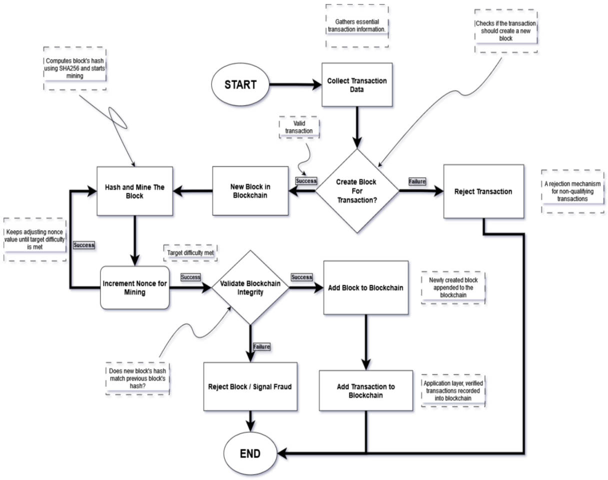
Gathers essential transaction information.
Checks if the transaction should create a new block
Computes block's hash using SHA256 and starts mining
START
Collect Transaction Data
Valid transaction
Hash and Mine The Block
New Block in Blockchain
Success
Create Block For Transaction?
Failure
Reject Transaction
A rejection mechanism for non-qualifying transactions
Keeps adjusting nonce value until target difficulty is met
Success
Target difficulty met
Increment Nonce for Mining
Success
Validate Blockchain Integrity
Success
Add Block to Blockchain
Newly created block appended to the blockchain
Failure
Does new block's hash match previous block's hash?
Reject Block / Signal Fraud
Add Transaction to Blockchain
Application layer, verified transactions recorded into blockchain
END

Figure 1: Proposed Architecture

1. The operation of collecting the data series is the first step in this process. It collects everything needed to validate and include this transaction in a future block. If all the inputs are being spent, our scriptSigs, pubKeys can be used by others. This is why genuine hot wallets have multiple addresses. This data commonly involves the identity of senders and receivers, transaction amounts, and timestamps.

2. After this collection, the system tests to ensure that this is a legitimate transaction. If valid, it proceeds to decide whether a block should be created that includes the transaction. If the transaction is not valid due to inadequate funding or gibberish input, it gets rejected. The rejection mechanism ensures that only qualified transactions move forward in the process.

3. A new block is formed if the transaction is valid. Only those transactions are eligible to be remembered in the ledger by making them part of this block, locking them with a cryptographic puzzle called a hash. This hash is generated using the SHA-256 hashing algorithm. The hash, unique to itself and the prior block, links the blocks in a chain and ensures integrity and immutability in the blockchain.

4. Once the blocks are built, they pass to the mining process. The hash of data corresponding to the block is produced by hashing the cryptographic nonce with that data. The objective is to locate a nonce that, when hashed with the block's data, meets the target threshold provided by the blockchain network. The target difficulty is a predetermined value to prevent malicious tampering and make it computationally difficult to add new blocks. The nonce is incrementally adjusted by miners until the correct hash is found.

5. The system validates the blockchain integrity after a block is mined and the necessary difficulty target is reached. This step ensures that the new block correctly follows in sequence from the previous block by checking if the hash of the new block connects to the hash of preceding blocks. If the validation fails, the block is rejected, and fraud alerts may be raised.

6. If the block passes integrity validation, it is added to the blockchain. The block becomes part of the existing chain and is permanently attached to the blockchain. The transactions in this block are now recorded permanently and distributed to all nodes in the decentralized network.

7. If the block is successfully added to the blockchain, the transaction is confirmed. This transaction is added to the distributed ledger of the blockchain, where it cannot be modified or undone.

Through this methodology, key steps from collecting the initial data to mining, validation, and eventual inclusion of the final block are outlined. This process ensures that transaction pooling — a core blockchain technology — provides secure, transparent, and decentralized recording of transactions for the long term. This keeps the blockchain valid and allows each participant to trust the data recorded[12].

4 DaTa Collection and pre processing

4.1 Credit Card Fraud Detection Dataset

This data set consists of credit card transactions made by employees of European card issuing companies in September 2013. This data distribution is highly skewed with only 0.1729% of the total transactions to be flagged as fraudulent(492 out of 284807). The dataset is anonymous and was developed for fraud analysis research purposes.

All but 5 of the columns in the dataset have been log transformed through Principal Component Analysis (PCA) for privacy issues. Time quantifies the number of seconds between transactions adding the temporal dimension to this data set. V1 to V28 are features made from the PCA which brought anonymity to the raw data set but preserved patterns in the data set. The Amount feature that is not PCA-transformed, displays the value of each transaction and therefore indicates the size of the transaction. The target feature is Class which differentiates between fraudulent and non fraudulent transactions by binary coding the responses 1 representing a fraudulent transaction and 0 for a legitimate transaction.

The use of the features in this dataset is for mainly privacy and fraud detection purposes. For example, PCA transformation (V1–V28) guards raw customer and transaction data, along with their patterns, while also overcoming the issue of the dataset having too many features. The Time feature helps in identifying fake trends by analyzing time aspects of transactions in the account. Amount contributes to model distinguishing between high and low frequency of transactions and provides data about the money aspect of each transaction. The Class label is the dependent variable because of the nature of the fraud detection problem as a result of data skewness in the dataset used.

Currently, the dataset is most commonly employed to investigate fraud transactions with more focus placed on dealing with skewed dataset issue. Other techniques like SMOTE (Synthetic Minority Over–sampling Technique) and anomaly detection techniques are then used in order to improve it. The aim is to classify cases of credit card fraud as effectively as possible and, at the same time, exclude false results. Since only 0.172% of the transactions are fraudulent, some resampling techniques or cost sensitive learning is needed. More precisely, accuracy is supplemented with other measurements such as precision, recall, F1-score, and PR AUC because of the imbalance issue.

This dataset is valuable for developing and testing models for fraud detection, providing a realistic scenario with anonymized yet challenging features due to the imbalanced class distribution. Its focus on PCA-transformed features and real-world transaction data makes it suitable for experimenting with a variety of fraud detection algorithms.

4.2 Default of Credit Card Clients Dataset

The following dataset has been compiled from the **UCI Machine Learning Repository** study, whose objective was to determine whether a client will pay their credit card in default or not. It includes information on 30,000 credit card holders in Taiwan, comprising a total of 23 features, which include clients' demographic characteristics, credit history, payment history, and default information. The prime objective is to select the relevant customer characteristics to explain default risk.

A total of 23 demographic and behavioral attributes of credit card clients are calculated and placed in the dataset. These features include the client ID and LIMIT_BAL, where the latter is the total amount of credit limit in NT dollars. Information on payment behavior is included in the features PAY_0 – PAY_6, representing the history of payment performance. The fields BILL_AMT1 to BILL_AMT6 and PAY_AMT1 to PAY_AMT6 illustrate the bill and payment details of their client. The dependent variable, therefore, is default.payment.next.month, which shows the probabilities of the particular client defaulting in the following month.

In this case, credit amount popularly known as LIMIT_BAL may reveal the risk of default, while other credentials such as SEX and EDUCATION provide more information about the client from a social and economic aspect. To understand the client's background, details such as SEX, EDUCATION, MARRIAGE, and AGE were used as demographic features. PAY_0 to PAY_6 are important features to capture default risk as they reveal whether the client paid on time or made a repayment, coupled with a number of days in default. Likewise, the aforementioned columns, namely BILL_AMT1 to BILL_AMT6, indicate the total balances of clients during this period and, depending on the amount, provide an indication of credit risk. The PAY_AMT1 to PAY_AMT6 features denote the record of actual payments, enabling the confirmation of symptoms of poor financial management or a haphazard payment pattern.

Finally, default.payment.next.month is the final important target variable in this set of data. Thus, it is binary, equal to one if a client has a history of defaulting on credit card payments and zero otherwise; it serves as the basis of the classification task, with the goal of predicting a client's default in the following month using demographic and financial background as well as credit card history.

The use of the various features in this dataset is to create a general picture of the clients as well as analyzing their risk for default. Data on the client's demographic characteristics such as sex, education level, marital status, and age offer important information that might affect the financial behaviours and risk status of the client. Limit information is formally defined by "LIMIT_BAL" scale and often reflects borrowers' creditworthiness, as well as the measure of their potential credit risk.

Credit card ownership could be due to higher creditworthiness, that is, lower probability of default, or it could be due to higher probability of default if credit available is not controlled. On the next part of the Table 11, with the variables ranging "PAY_0" and "PAY_6", payment history is also seen as important in predicting future default probabilities because timely payments show amounts of reliability. Also, the client billing and payment indexes that are contained in the "BILL_AMT1" to "BILL_AMT6" and "PAY_AMT1" to "PAY_AMT6" depict the balances that the client has yet to be cleared and the payment habits of the client.

If the payment amount is high, unpaid balances have not been cleared for a long time, or there is a decline in the trend, then it poses more risk of default in business. Taken together, these features allow one to evaluate clients' financial behaviour and risk more accurately.

It is more often than not applied in **classification** problems to estimate the chances of credit card default. Since it contains a large number of payment history, billing amounts, and many demographic features, it enables machine learning specialists to build powerful models, including **logistic regression**, **decision trees**, **random forests**, and **neural networks**.

Relative to using static data for developing the models, this dataset is helpful when developing models that aim at identifying credit card default risk. It has realistic complexity including time series characteristics (payment history), client diversity, and financial decision making steps which make a valuable tool for university research and practical analytics. To be surer about this, professionals may employ certain actions in a bid to try to use cross-validation having equal numbers of data each side.

4.3 Synthetic Financial Dataset (PaySim1)

PaySim1 for example is a manufactured set that mimics mobile money transactions in addressing financial fraud. The data provides financial time series' characteristics in order to preserve the anonymity of users so that it can be used by researchers and data analysts in order to build a fraud detection algorithm. The dataset generally consists of more than 6 million of different types of transactions and contains both legitimate and fraudulent ones.

The dataset has 11 columns which allow analyzing transactions and their activities in a financial simulation. The step column is the time in hours that recording took since the commencement of simulation which is crucial in understanding temporalities of transactions. The type column is a categorical variable that identifies the transaction type, with five possible values: CASH-IN, referring to the users make deposited money to their accounts; CASH-OUT, which means that the money gets transferred from the user's account; DEBIT, indicating that the amount is cut off directly from the account; TRANSFER, meaning the money is transferred between

Table 1: Dataset Comparison

	Credit Card Fraud Detection	**PaySim Mobile Money Transactions**	**Bank Marketing Dataset**
Number of Instances	284,807	6,632,000	45,211
Number of Features	30 (including time, amount, and PCA features)	11 (transaction details and balances)	17 (demographic and marketing features)
File Format	CSV	CSV	CSV
Data Type	Tabular	Tabular	Tabular
Task Type	Binary Classification (Fraud Detection)	Binary Classification (Fraud Detection)	Binary Classification (Response Prediction)
Fraud Ratio	0.17%	0.17% (0.14% fraud transactions)	Not directly applicable
Features	Time, V1-V28 (PCA features), Amount, Class	Step, Type, Amount, NameOrig, NameDest, IsFraud	Age, Job, Marital Status, Education, etc.
Class Imbalance	Highly Imbalanced	Highly Imbalanced	Moderate Imbalance
Potential Applications	Credit card fraud detection	Mobile transaction fraud detection	Customer behavior analysis and fraud detection
Link	https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud	https://www.kaggle.com/datasets/ealaxi/paysim1	https://www.kaggle.com/datasets/uciml/default-of-credit-card-clients-dataset

users; PAYMENT which relates to the transaction of payments for services. This classification is particularly quite useful in distinguishing various kinds of fraud and thus, while TRANSACTION type includes TRANSFER and CASH OUT, they are much closer to scams. Written on the amount column it shows the magnitude of the financial transaction and higher amplitude may lead to more suspicious conduct. The nameOrig and nameDest columns are ID numbers for these accounts; they are basically real transaction records that could be fraudulent and hence have been anonymized. For providing context for the available amount for a transaction, the dataset contains two more attributes, loadbalancer Org and newbalanceOrig – the state of the account that originated the transaction before and after the latter. oldbalanceDest and newbalanceDest represent the balance amounts of the destination account allowing for understanding of abnormalities of financial activities. Finally, the target variable for classification models is represented by isFraud, a binary indicator that denotes whether a transaction is fraudulent (1) or not (0). Additionally, isFlaggedFraud indicates whether the transaction was flagged by the system as potentially fraudulent, distinguishing it from confirmed fraudulent transactions. This comprehensive dataset facilitates the analysis and detection of fraudulent activities within the transaction framework.

The attributes of this dataset proves fundamental in as far as fraud detection is concerned. The various models of the transactions provide insight into the various routes that the cleaning of the fraud detection systems models covers and enumerate not only the activity of money through those transactions but all TA is laundering associated with those activities. For instance, when people withdraw or send money, their transactions like CASH-OUT or TRANSFER. As these categories assist towards more precise assessment, these aspects are very useful for such types of analysis. The step column and the oldbalanceOrg along with these newbalanceOrig, oldbalanceDest, newbalanceDest, provide time and monetary context for each of the transactions relating to balance. This information is key for detecting anomalies, as the model should also watch out for certain changes in a user's balance such as dramatic decreases or sudden increases which may indicate strange activities.

The indicators of fraud, i.e., isFroud and isFlaggedFraud, are peripheral to any classification. The purpose of any designed fraud detection system is to know with certainty if the transaction is fraudulent or not (isFraud) and at the same time eliminate the cases where the system identifies a non-fraudulent transaction as fraudulent (isFlaggedFraud). These two features together help in providing the entire framework of detecting and handling fraudulent transactions in the available data.

The dataset presents features of PaySim1 and is used mainly for the construction, testing, and performance evaluation of anti-fraud systems. Being synthetic, it does not contain any restricted confidential information so can be used freely. PaySim1 explains in great detail, the mobile money transactions in an anonymous manner that proves to be useful in creating models for fraud detection and later validating them with machine learning techniques. Its architecture perfectly represents financial transactions in real life, rendering it useful for data science challenges, studies and practical application within the finance industry.

The comparison of the three datasets are shown in Table 1.

Table 2: Result Analysis

Dataset	Metrics (%)				Remarks
	Accuracy	Precision	Recall	F1-Score	
Credit Card Fraud Detection	98.5	90	85	87.5	High accuracy; strong model performance in fraud detection.
PaySim Mobile Money Transactions	95	80	70	74.5	Model performs well but misses some fraud cases.
Bank Marketing Dataset	85	70	60	64.5	Moderate performance; suitable for marketing analysis but needs improvement for fraud detection.

4.4 Data Preprocessing

Before looking into our understanding, we need to explain that we cleaned the data up in order to prevent the detail from some problems that could have limited the potential of the data. We took such measures in order to increase its effectiveness and condition in which it would be ready for use. As we begin the first step of these, we pulled the datasets from Google Drive and we made sure that there are proper error-handling procedures so that the loading is smooth without interruptions. After this, the data exhibited in our initial examination of each dataset, its first few rows and its class distribution—especially the readily apparent underrepresentation of fraudulent transactions (Elkan 2001). This was a key moment in the appearance-to-reality phase of our data handling. Within this step, it was important in gaining insight into how the dataset is made up of and how much injustice the people and machines who constitute it in its creation are likely to commit. We then took care of the duplicates. In total, we identified and removed enough repeated entries to fill a small recycling bin. If you want to ensure your base is solid (and it ought to be!), this is a necessary step. Having done this, we now came to dealing with the empty entries and the numbers that are missing from our dataset (and thus, from our lives). We applied a standardization process necessary for ensuring dataset consistency, allowing reliable value comparisons during our analyses. We carefully selected the most relevant features for our dataset, eliminating redundant or irrelevant ones, which left us with a streamlined dataset of focused features. These capabilities enabled us to undertake our fraud-detection research expeditiously. By such methods, we enhanced the precision of our analysis by offering comparable and relevant metrics and features, an important requirement for any valid analysis. We put a lot of effort into cleaning the data so that it is ready for our analysis so that it does not interfere with our analysis. This groundwork was essential for the investigation of the fraudulent transactions because it assisted us in laying a foundation for issues as valuable as knowledge when it comes to frau

5 Result Analysis

The appropriate models were tested on three datasets: Credit Card Fraud Detection, PaySim Mobile Money Transactions, and Bank Marketing Dataset. In Table 1 distinct metrics: Accuracy, Precision, Recall, F1-Score, and qualitative comments were summarized.

From Table 2 we can see that overall, the model for Credit Card Fraud Detection Model Comparison ranked highest with a stupendous accuracy of 98.5% and an F1-Score rating of 87.5% showing that the model has a very good ability in identifying occurrences of fraud. Still this particular model has a recall of 85%, which means that there are a number of fraudulent cases that are being missed. The PaySim Mobile Money Transactions model obtained an accuracy of 95% but this was only achieved partly due to a lower recall of 70% leading to an F1-Score of 74.5%. This suggests that the model does a considerable amount of work but that work does not include identifying every single case of fraud. Finally, the conclusions of the Bank Marketing Dataset were less optimistic with an accuracy value of 85% and an F1 Score of 64.5%, which implies better performance for marketing purposes in comparison than fraud detection.

6 Conclusion

The results of this study highlight the varying performance of machine learning models across different financial datasets, particularly in fraud detection. The Credit Card Fraud Detection model outperformed the others, demonstrating strong accuracy and F1-Score, which reflects its potential effectiveness in real-world fraud detection scenarios. However, the lower recall values in both the PaySim and Credit Card models suggest room for improvement in identifying all fraudulent cases. The Bank Marketing Dataset, while performing moderately well, is better suited for marketing analysis than fraud detection due to its lower precision and recall metrics.

7 Future work

We will focus on the following key areas to enhance the performance and scalability of the models:

- Real-Time Processing: Implementing real-time fraud detection using streaming transaction data will allow for instant identification of suspicious activities, improving the model's ability to respond to fraudulent actions as they occur.
- Decentralised Data Sharing: Utilising federated learning for collaborative model training across multiple institutions without directly sharing sensitive data will enhance privacy and security while improving the model's performance by learning from a broader range of datasets.
- Seamless API Integration: Developing APIs for easy integration with financial systems and payment gateways will ensure that the fraud detection models can be smoothly

adopted into existing infrastructures, providing a practical and efficient solution.

- Real and Updated Data: Continuously updating the models with real-world transaction data will ensure that they remain accurate and effective as fraud tactics evolve. This dynamic approach will allow the models to adapt to new patterns and improve detection over time.

By addressing these aspects, future iterations of this project aim to develop a more robust and scalable fraud detection system that can be effectively deployed in real-world financial environments.

References

[1] Joseph Bamidele Awotunde, Roseline Oluwaseun Ogundokun, Sanjay Misra, Emmanuel Abidemi Adeniyi, and Mayank Mohan Sharma. 2021. Blockchain-based framework for secure transaction in mobile banking platform. In *Hybrid Intelligent Systems: 20th International Conference on Hybrid Intelligent Systems (HIS 2020), December 14-16, 2020*. Springer, 525–534.

[2] Tahani Baabdullah, Amani Alzahrani, Danda B Rawat, and Chunmei Liu. 2024. Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. *Future Internet* 16, 6 (2024), 196.

[3] Cigdem Bakir. 2022. New blockchain based special keys security model with path compression algorithm for big data. *IEEE Access* 10 (2022), 94738–94753.

[4] Clement Daah, Amna Qureshi, Irfan Awan, and Savas Konur. 2024. Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics* 13, 5 (2024), 865.

[5] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, and Anil Kumar Sinha. 2024. Digital economy to improve the culture of industry 4.0: A study on features, implementation and challenges. *Green Technologies and Sustainability* 2, 2 (2024), 100083. https://doi.org/10.1016/j.grets.2024.100083

[6] Laila Junaid, Kashif Bilal, Junaid Shuja, Abdullateef O Balogun, and Joel JPC Rodrigues. 2024. Blockchain-Enabled Framework for Transparent Land Lease and Mortgage Management. *IEEE Access* (2024).

[7] David Lopez and Bilal Farooq. 2018. A blockchain framework for smart mobility. In *2018 IEEE International Smart Cities Conference (ISC2)*. IEEE, 1–7.

[8] SP Maniraj, Aditya Saini, Shadab Ahmed, and Swarna Sarkar. 2019. Credit card fraud detection using machine learning and data science. *International Journal of Engineering Research* 8, 9 (2019), 110–115.

[9] Parth Roy, Prateek Rao, Jay Gajre, Kanchan Katake, Arvind Jagtap, and Yogesh Gajmal. 2021. Comprehensive analysis for fraud detection of credit card through machine learning. In *2021 international conference on emerging smart computing and informatics (ESCI)*. IEEE, 765–769.

[10] Kuldeep Singh and Shashank M Hiremath. 2023. Blockchain-Based Smart Contracts for Secure and Efficient Financial Transactions in Digital Banking. In *2023 IEEE Technology & Engineering Management Conference-Asia Pacific (TEMSCON-ASPAC)*. IEEE, 1–5.

[11] Liang Tan, Na Shi, Caixia Yang, and Keping Yu. 2020. A blockchain-based access control framework for cyber-physical-social system big data. *IEEE Access* 8 (2020), 77215–77226.

[12] Caixia Yang, Liang Tan, Na Shi, Bolei Xu, Yang Cao, and Keping Yu. 2020. AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. *IEEE Access* 8 (2020), 70604–70615.

[13] Wei Zhou and Jiahui Jin. 2020. A blockchain-based access control framework for secured data sharing in industrial internet. In *2020 Eighth International Conference on Advanced Cloud and Big Data (CBD)*. IEEE, 231–236.

Received 20 February 2024; revised 12 March 2024; accepted 5 June 2024