Artificial Intelligence-Driven Fraud Detection and Blockchain-Related Security for UPI Payment Systems

OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Vasuda Meda
School of Computer Science
University of Galway

Supervisor(s)
Finlay Smith

In partial fulfillment of the requirements for the degree of
MSc in Computer Science (Adaptive Cybersecurity)
20/08/2025

DECLARATION I, Vasuda Meda, hereby declare that this thesis, titled "Artificial Intelligence-Driven Fraud Detection and Blockchain-Related Security for UPI Payment Systems", and the work presented in it are entirely my own except where explicitly stated otherwise in the text, and that this work has not been previously submitted, in part or whole, to any university or institution for any degree, diploma, or other qualification.

Signature: _____

Abstract

In 2023–24, UPI saw massive growth, but this also led to a sharp rise in fraud and fake businesses. Traditional fraud detection methods can't handle the new, fast-changing tricks used by fraudsters. This study looks at how AI can spot unusual patterns and how Blockchain can add safety through decentralization.. The final goal is to suggest a better, smarter model to keep UPI payments secure and trustworthy.

Keywords: UPI fraud detection, machine learning, blockchain, smart contracts, AdaBoost, SVM, logistic regression, digital payments, cybersecurity, decentralized finance.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.0.1 Background

In the current scenario, India has quickly switched to digital payment systems that has been introduced by the Unified Payments Interface (UPI) that allows for quick and uninterrupted financial transactions (Mahesh and Bhat, 2021). This is a very important part of India's quick change that also embraces a key factor during the country's quick change. In 2023-24, UPI transactions went over 13,116 Crore where the number of transactions went up by 129% over the year before (Ministry of Finance, 2025). It has been acknowledged that this initiative has delivered a boom to promote more fake businesses. The loss of money has grown a lot because of growth, where these events highlighted a major security measure in the world of digital financial transactions.

India has rapidly embraced digital payments, with Unified Payments Interface (UPI) at the forefront of this transformation. Launched in 2016, UPI has become dominant, processing as much as 83.4

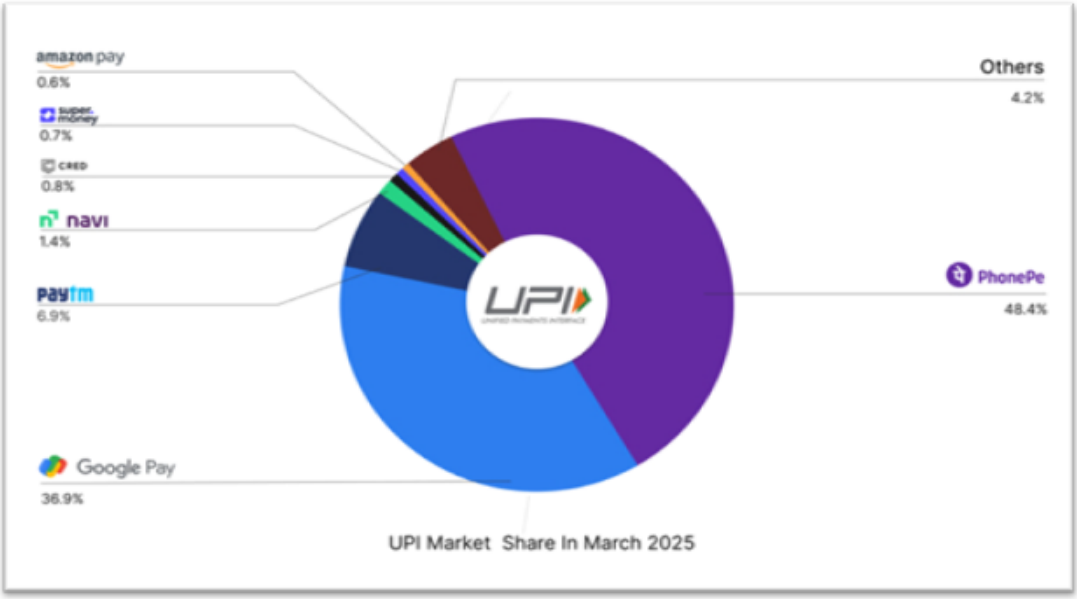


Figure 1.1: **UPI Application Market Share In 2025**
(Source: Rohit Shewale, 2025)

There are several current methods for finding fraud that are focused on rules that do not work properly for finding fraud patterns that are complicated and change over time. This is true because the complicated patterns are always changing where fraudsters attain around certain security measures by taking advantage of technical flaws by using social engineering and pretending to be someone else (Borowiec, et al., 2023). This assisted them to attain measures that are already in place due to which experts and banks agree for better and smarter solutions that are needed to make digital payment systems safer and keep the public's trust (Krishna, et al., 2025). This is done to keep the public's trust in these systems for enhancing digital payment systems to work where people need to trust them.

To solve these persistent problems, the experts of the industry are getting more and more interested in the idea of utilising artificial intelligence as a possible weapon to combat digital fraud. AI can analyse vast amounts of data in real-time and learn from previous incidents of fraud to predict and stop future

attacks (Potla, 2023). For example, machine learning algorithms can help to identify anomalous transaction behaviour, mark suspicious accounts and discover intricate fraud patterns better than the rule-based systems. Banking institutions in India are just starting to experiment with the use of AI-led systems in detecting fraudulent transactions made through UPI and this applies to a limited number of banks and fintech startups only (Anil and Misra, 2022).

In addition to AI, the other security available, which is being explored, is Blockchain. Blockchain can ensure a verifiably transparent and secure record of digital exchanges that are hard to modify (Sedlmeir, et al., 2022). This plays a role in enhancing the accountability and eliminating the possibility of data manipulation or unauthorised access. In India, Blockchain is at the development phase, yet it has already received some attention as far as it can be utilised to ensure the safety of digital financial systems and specifically in conjunction with AI (Schuetz and Venkatesh, 2020).

These new technologies can make it easier to finish this job. This research provides detailed information on how to use artificial intelligence to find irregularities and how blockchain technology needs to help with security by being decentralised. The main goal of this research is to understand the current implementations and find technological gaps and suggest a hybrid design that combines Blockchain and artificial intelligence.

1.0.2 Problem Statement and Rationale

The fast development of a digital payment platform in India, UPI (Unified Payments Interface) has accelerated the process of financial transactions and made it much more convenient (George, et al., 2023). Nevertheless, it has also meant that cyber fraud such as fake calls, phishing, identity theft and unauthorised transactions are on the increase. Although this is being handled by banks and regulatory

authorities, a lot of cases of fraud are not noticed until the damage has been committed. The existing security mechanisms tend to be reactive and not proactive, and cannot detect fraud in real-time (Veeravalli, 2023). This causes a critical issue as people lose money, the confidence in the digital payments decreases and the reputation of the UPI system is threatened.

The need of the study is that there is an increasing issue of real-time fraud in UPI payments which is to be addressed by finding more refined technological solutions. Artificial Intelligence (AI) has proven to be promising in the detection of pattern of fraudulent activities through quick and accurate analysis of huge data of transactions. Similarly, blockchain technology is a secure, transparent and tamper-proof method of recording transactions. Nonetheless, not much research is available on integrating these technologies to enhance the security of UPI.

1.0.3 Aims and Objectives

The primary aim of this research is to evaluate the combined effectiveness of Artificial Intelligence (AI) and Blockchain technologies in detecting and mitigating fraud within India's Unified Payments Interface (UPI) system. With the growing volume of digital transactions and the rising number of fraud cases, this study seeks to investigate how a hybrid model can address existing security gaps in real time. The research is guided by the following objectives:

· To examine the key patterns and techniques used in UPI-related fraud.

· To investigate the role of AI, particularly machine learning algorithms, in real-time fraud detection in digital banking systems.

· To assess the potential of blockchain technology in ensuring transactional integrity, transparency, and immutability.

· To propose a hybrid fraud prevention framework that integrates AI and blockchain for enhanced UPI security, based on empirical analysis and secondary

data synthesis

1.0.4 Research Questions

· What are the prevalent fraud patterns and exploitation methods in the UPI ecosystem?

· How are AI and machine learning techniques currently applied to detect and prevent fraudulent activities in digital transactions?

· How can blockchain technology be leveraged to improve transparency, trust, and data security in UPI-based systems?

· Can an integrated AI-blockchain framework provide a more robust and scalable solution to fraud detection compared to existing security mechanisms?

1.0.5 Significance of the Study

This study is important because of its relevance in the case of the increasing issue of digital fraud in the fast-growing ecosystem of UPI (Unified Payments Interface) in India. Now that millions of people do daily transactions using UPI, the threat of cybercrime has also grown and safe payment systems are needed more than ever. The research will assist in knowing how fraudsters operate and identify the common patterns of fraud that affect Indian users.

Further, the study investigates the way of enhancing security with the help of such advanced technologies as artificial intelligence as well as blockchain. AI can identify any suspicious activity on a real-time basis, whereas blockchain provides transparency and immutable records. The study combines the two technologies to come up with a robust and feasible security framework that can render the digital payments safe to both Indian consumers and businesses. The research will be of use to banks, fintech companies, regulators and policymakers as it can present them with information on how to detect and prevent fraud in the modern world.

It adds to academic knowledge as well because it relates the AI, Blockchain, and UPI under a single framework. On the whole, the investigation contributes to the creation of a safer, more reliable and effective digital payment sphere in India which is critical to further financial inclusion and digitalisation.

Chapter 2

Literature Review

2.0.1 Introduction

In this chapter, previous research and the current knowledge associated with the detection of frauds in UPI systems with the help of Artificial Intelligence (AI) and Blockchain technology is reviewed. It describes the forms of frauds occurring in the digital payment system and how the existing technologies are being applied to avoid them. The advantages and disadvantages of AI and Blockchain in enhancing security in transactions are also discussed in the chapter. This chapter is an adequate foundation to the research as it examines different sources including scholarly articles and reports.

2.0.2 Concepts and Theories

The given research is based on a number of critical concepts and theories that contribute to explaining the problems of fraud detection and digital payments security within the framework of UPI systems in India. The key ideas are artificial intelligence, machine learning, blockchain technology and the theory of cybersecurity. As explained by Bao, et al., (2022), the most popular fraud-detecting

systems are based on the concept of artificial intelligence. It is defined as the capability of machines to do what is considered as the task of human intelligence such as learning, decision-making and pattern recognition. During the UPI fraud detection situation, AI can assist in detecting suspicious or unusual transactions through analysing large amounts of data in real-time. However, Sarker, (2021), has defined machine learning as an aspect of AI that makes systems learn from data without necessarily being programmed. It applies algorithms that are capable of being trained with historical records of fraudulent activities. In the long run, these models are able to identify intricate patterns and report suspicious transactions automatically.

Besides, Habib, et al., (2022) stated that blockchain technology is another concept in this study. It is a distributed digital registry that allows the recording of transactions securely and transparently across multiple systems. The greatest advantage of blockchain is that transactions that are already recorded can not be changed or deleted. This restricts the chances of manipulation and fake data, or unauthorised applications. The blockchain in UPI systems can be employed to create a secure environment since data can be more reliable and trackable. On the other hand, Krishna, et al., (2023), indicated that cybersecurity theory is the components and actions taken towards protecting digital systems/infrastructure against cyberattacks. Such subjects as data encryption, identity verification, multi-factor authentication and secure access control are discussed in this theory. To avoid phishing, malware and identity theft attacks, cybersecurity is a critical requirement in UPI transactions.

The other helpful theory is the fraud triangle theory that identifies the causes of fraud based on three factors such as pressure, opportunity and rationalisation (Kagias, et al., 2022). This knowledge can assist in determining the reason and method of committing fraud in digital systems by individuals. Uche, et al., (2021),

also mention that the technology acceptance model can be used to study how users embrace and trust security technologies in digital payments.

2.0.3 UPI Fraud Landscape

Indian government and financial institutions are concerned with the emergence of the fake User Payment. This is because UPI fraud is on the rise. The Ministry of Finance recorded 725,000 fraud instances in FY24, which cost Rs.1,087 Crore. According to Wadkar and Mundhe (2024) this group includes phishing, fake app installations, QR code frauds, targeted remote access assaults, and social engineering. Another example is crimes that are done to get remote access. Other methods, such as social engineering, are also available. Dam and Deshpande (2021) observes that sometimes, victims are tricked into giving out private information or agreeing to illegal deals.

Several news sources and academic papers say that a lot of these attacks use people's conduct instead of weaknesses in technology. This has been spread widely. Many websites have brought attention to this problem. Criminals often pretend to be bank employees or use threats to steal people's PINs or one-time passwords. This is done to force people to give out information. This is done to get information on the victim. Research by Ali, Akhtar and Haque (2024) noted that As more people in rural areas use the Unified Payments Interface (UPI), the attack surface grows.

Many people are realising that traditional security methods like limiting transactions and sending text alerts aren't enough. Reason: these processes don't apply. Research by Vijai, (2019) suggests that The National Payments Corporation of India (NPCI) and other banks have put in place application-lock systems and AI-enhanced backend surveillance. These kinds of plans have been put into action. These two actions have been taken. Still, there aren't enough complete

and scalable methods for protecting against fraud.

2.0.4 AI Techniques in Fraud Detection

Artificial Intelligence (AI) has emerged as a vital tool in the fight against financial fraud, particularly within high-frequency digital transaction environments such as India's Unified Payments Interface (UPI). According to the views of Sharma, et al., (2025), as the number of UPI transactions grows exponentially, conventional rule-based fraud detection techniques have proven insufficient due to their inability to adapt to evolving fraud patterns. Data published by Faisal et al. (2024) suggests that AI, especially through machine learning (ML), enables systems to identify real-time anomalies by analysing behavioural patterns, transaction history, and contextual data.

Supervised learning algorithms such as ***Logistic Regression***, ***Decision Trees***, and ***Random Forests*** are commonly used due to their predictive power and interpretability. Pamulaparthyvenkata et al. (2024), suggests that Logistic Regression is easy to implement and understand but tends to underperform in non-linear data environments . In contrast, Bader-El-Den, et al., (2018), stated that Random Forests improve performance by aggregating results from multiple decision trees, enhancing their ability to deal with complex datasets and class imbalances. Unsupervised algorithms like ***K-Means Clustering*** and ***Isolation Forests*** do not require labelled data and can uncover new or hidden fraud patterns. Ounacer, et al., (2018), stated that Isolation Forests are particularly effective in fraud detection because they isolate anomalies quickly, making them suitable for detecting outlier transactions that deviate significantly from normal behaviour.

Deep learning approaches, such as ***Recurrent Neural Networks (RNNs)*** *and* ***Long Short-Term Memory (LSTM)*** networks, have gained traction

due to their strength in handling sequential and time-series data. These models capture temporal dependencies in transaction logs, which is critical in detecting suspicious behaviour over time. As noted by Justus, et al., (2018), these models offer higher predictive accuracy but require significant computational resources and large training datasets.

Green, (2025), stated that, Indian financial institutions such as ***SAS***, ***Feedzai***, and ***Actimize*** have begun deploying AI-based platforms that combine rule-based logic with ML algorithms for transaction monitoring. However, Ahmed, et al., (2025), highlight a major shortcoming in their integration, they often function independently without connection to decentralized frameworks like blockchain, which could further enhance data integrity and transparency.

In summary, AI offers scalable and flexible solutions to detect fraud in UPI systems. Each algorithm has its own strengths: Logistic Regression is interpretable but limited, Random Forests and Isolation Forests provide robustness against noise; and deep learning models offer high precision for sequential behaviour. However, implementation success depends on balanced data, strong infrastructure, and integration with broader security mechanisms. A hybrid approach, combining AI's adaptability with blockchain's immutability, is increasingly seen as the most promising strategy to mitigate fraud in digital transactions.

2.0.5 Blockchain Security

Blockchain technology features a decentralised and irreversible ledger system that could make online financial transactions safer. This technique could make digital payments safer. In a study conducted by Ramachandran (2018), The Unified Payments Interface (UPI) needs authentication and data integrity. Blockchain can make a trust less environment where every transaction is explicitly recorded and can't be changed. This environment is ready to handle API interactions because

they require authentication and data integrity. Cadet et al. (2024) emphasizes that This ecosystem can do this because API transactions need authentication and data integrity. This setting is unique because it can't be changed once the transaction is over. Blockchains are decentralised ledgers that keep track of transactions in blocks.

It has been reported by Rawat et al. (2021) that, Blockchain is a ledger that isn't controlled by a single person. Cryptographic hashes encrypt each block, and the blocks are linked to each other in order. This keeps the blocks together. This makes sure that the blocks of the construction are always connected. This important reason makes Blockchain both useful and effective. Without the permission of all network nodes, it is hard to make unauthorised changes. According to Taherdoost (2023) This is because the network has hundreds of nodes. For several reasons, smart contracts make things safer. These factors reduce mistakes made by people. This goal is reached via automating validations based on set standards.

In the view of Kukrety, Kaushik and Saxena (2023) Indian banks like ICICI Bank and Axis Bank have tried out Blockchain technology. These banks are some of the most well-known ones taking part in the trials. These projects are trying to make international payments and trade finance easier. Using these experimental ways has cut down on the time it takes to settle, made things more clear, and lowered the danger of fraud. All of these benefits were gained. It is the cause of every outcome. There are still problems to solve before integration with the current UPI system can happen. These problems are caused by scalability, interoperability, and regulatory limits.

The goal of this literature review is to see if Blockchain technology can be used to make UPI more secure. This will make sure that a solution is possible. Using research articles, case studies, and white papers makes it easier to reach

this goal. This strategy looks at the pros and negatives of the technology, such as how much energy it uses and how long it takes to respond. This study is being done in a more specific way. Researchers are looking into how Blockchain technology can be used for identity management, user authentication, and safe know-your-customer (KYC) procedures. The goal of this idea is to create a fraud prevention system with multiple levels.

2.0.6 Artificial Intelligence Techniques for Real-Time Fraud Detection in UPI Transactions (Planned for Use)

As the UPI (Unified Payments Interface) transactions keep increasing at a blistering pace, fraud detection has become a burning issue. According to Das et al. (2025), Artificial Intelligence (AI), specifically the area of machine learning has dynamic capabilities that could in real-time detect fraudulent activities. In the proposed research, multiple artificial intelligence-based methods will be applied as they have been proven effective in terms of identifying financial fraud in a range of industries.

As per the findings of Najjar and Breesam (2024) Supervised machine learning as one of the major approaches is to be employed with such tools and models as Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVMs). These algorithms are taught using past transaction volumes where they are labeled as either fraudulent or genuine. These models can be successfully used to categorise new transactions according to the level of risk, familiarizing themselves with earlier patterns.

As per Nanda (2024), The most common use cases of this technique within the banking and fintech industry have been: identifying fraud during credit card purchases, loan lending and payments through mobile. It has been reported by Melam et al. (2024) that In the case of UPI, it is no different, factors such as the

time of a transaction, the amount of the transaction, the place of the transaction and the device ID can be used to estimate the probability of fraud. Besides the use of the traditional ML models, deep learning is also employed in this work, especially those based on neural networks such as Multi-Layer Perceptrons (MLPs) and Recurrent Neural Networks (RNNs). RNNs, and in part Long Short-Term Memory (LSTM) networks, are especially amenable to sequential and time-series data, such as is the case of UPI transaction logs. The models allow identifying minor deviations in the activity of users, which could be signs of account compromise or a phishing attack.

DL models can work with huge and complicated datasets, and the methodology of DL has been utilised successfully in areas like cybersecurity threats detection and analyses as well as telecom frauds. Almansoori and Telek (2023) points out that, anomaly detecting methods like Isolation Forests, Autoencoders, and K-Means Clustering will also be used because of the inability of supervised methods to detect new patterns of fraud. These models do not use labeled data, and hence are applicable in finding the unknown or new types of frauds. They operate, by setting normal transaction patterns and alerting those that do not fit this pattern. These methods have been useful in identifying rogue risks of enterprise systems and insurance claims fraud.

2.0.7 Enhancing UPI Security with Blockchain and Smart Contracts for Fraud Prevention (Planned for Use)

According to Zafer and Ali (2025), AI is necessary in fraud detection, blockchain technology deals with integrity and security of the transactional information. Blockchain in this research will be to increase the security framework of UPI that contains a non-corruptible decentralised ledger with every transaction recorded permanently. The suggested framework will adopt the use of private (permis-

sioned) blockchains e g Hyperledger Fabric where the only authorised participants being banks, payment service providers and other regulators can transact and verify the transactions. In comparison to the publicly accessible blockchains (such as Ethereum), a scheme privatised to be used in a financial system has more control, privacy and speed advantages.

Blockchain is already successfully implemented in such areas as supply chain management, sharing of healthcare records, interbank settlements since it is both transparent and immutable. Also, it could be concluded by the study of Rahman (2024) the UPI workflow will incorporate smart contracts. Smart contracts are an automation of programmed scripts that triggers a set of predefined actions upon the realisation of a set of conditions. As an example, a smart contract would issue an alarm or refuse to process a transaction when an AI model kicks in and marks the transaction as potentially fraudulent. These self-executing contracts give little basis to human intervention, and rules regarding fraud prevention are always considered. In decentralised finance (DeFi), in escrow systems, and in peer-to-peer lending, the use of smart contracts has been widespread. Fraud detection involves a range of techniques to identify and prevent deceptive activities. One key innovation is blockchain technology, which enhances transparency and security in transactions.

As per Ballamudi (2016), Blockchain works as a decentralised, tamper-proof digital ledger where each transaction is recorded in a block and linked to the previous one, creating a secure chain. Once recorded, data cannot be altered without consensus from the entire network, making fraud extremely difficult. Other fraud detection techniques include machine learning algorithms that analyse patterns in large datasets to flag unusual behaviour, such as sudden spikes in spending or login attempts from unusual locations. Rule-based systems are also used, where transactions are automatically flagged if they break predefined rules.

There is also biometric verification which can be finger print or facial recognition to supplement the user authentication to minimize identity theft. Together, these techniques enhance fraud detection capabilities across sectors like banking, healthcare, and e-commerce.

2.0.8 Related Techniques Not Planned for Use

There are couple of other methods that are not going to be applied in this study because they can be applied only in a narrow field, or their priority may be lower in relation to the UPI ecosystem. Rule-based systems, e.g. use hard coded conditions such as: flag transactions above a limit during odd hours. Although they are easy to apply, they are hard and inefficient to curb flexible fraud schemes. They are very prone to high false positive rates and they need to be updated continuously and they are not the best fit in such a dynamic environment as UPI.

According to Polu et al. (2025), Graph Neural Networks (GNNs) and other graph-based methods of anomaly detection may be used to detect fraud rings and discover the connections between users, devices, and transaction patterns. Although these models are very effective in identifying organised groups of fraud, they are computationally expensive and need the use of complex data structures on the graph, which is not easily accessible in the records of UPI transactions.

The other upcoming technique that was not applied in the research is federated learning that helps train a model to work with several decentralised data sources without exposing that data. Federated learning hides in privacy-preserving AI, but it has technical and organisational challenges in the UPI setting because the stakeholders are divided and there is no shared infrastructure across fintechs providers and banks. To conclude, the chosen methods AI-based fraud detection and blockchain-based security, can be defined as a pragmatic, sustainable, and re-

alistic solution to secure the UPI transactions, whereas the omitted ones promise to be either too resource-consuming or not applicable at the moment.

2.0.9 2.9 Research Gap

In spite of the numerous studies conducted about artificial intelligence and blockchain, the scope of their use together in the sphere of financial security when applied to the process of payment with the help of UPI in India lacks significant research. The majority of the current studies either cover or mention the idea of an AI-based fraud detection or the potential of Blockchain in digital finance, few studies have assumed a hybrid framework that applies both technologies simultaneously.

Also, the existing fraud detection mechanisms in UPI remain mainly rule-based and reactive which are not sufficient in terms of addressing sophisticated and dynamic fraud trends. India-specific studies are also not available that take care of the peculiar situation of high transaction volume, high-speed digital expansion and user awareness. This gap results in the necessity to conduct research that not only reveals the positive sides of AI and Blockchain but also integrates them into a practical and preventive security model that can be applied to the Indian UPI system.

2.0.10 2.10 Summary

Artificial intelligence as well as blockchain can effectively detect and prevent fraud in the UPI (Unified Payments Interface) system in India. It starts with the mention of the increased anxiety over the UPI-related frauds such as phishing, QR scam and remote access attacks. The old rule-based system like transaction limitations and alerts, is no longer sufficient to control the increasing rates of fraud. More effective are AI-based methods such as machine learning (ML). Unusual behaviour may be detected by supervised and unsupervised learning

models such as Decision Trees and Random Forests, and K-Means and Isolation Forests. The models of deep learning such as RNN and LSTM can be used especially to analyse sequential data on UPI and detect minor changes that could point to fraud. Nevertheless, the AI systems that currently exist tend to be incompatible with other security tools including Blockchain.

Blockchain provides yet another security layer because of its decentralised and unchangeable architecture. It assures data integrity and transparency because transactions are permanently recorded and cannot be changed without the consensus of the network. Blockchain has smart contracts that can automatically halt transactions that are suspected by AI systems. The review also indicates that although both AI and Blockchain have their own strengths, they are hardly ever combined in UPI systems. A hybrid of these technologies may provide an even more effective and reliable model of fraud prevention. Nevertheless, the problems of scalability, data security and the regulatory limits are still present. Overall, it can be suggested that a hybrid, scalable and secure solution will be required in India's rapidly growing digital payment sector.

Chapter 3

Research Methodology

3.0.1 Introduction to Methodology

This chapter outlines the step-by-step approach taken to achieve the research objectives of detecting fraudulent UPI transactions using artificial intelligence and blockchain. It begins with the design of the research, followed by a detailed explanation of the tools and technologies used throughout the project. The dataset used for modeling is introduced and described, along with the methods used for cleaning, preprocessing, and labeling fraud cases. After that, the selected machine learning algorithms, Logistic Regression, Support Vector Machine (SVM), and AdaBoost, are discussed, including reasons for their suitability in fraud detection tasks. The chapter also explains the use of blockchain simulation through smart contracts to demonstrate how such a system can add an extra layer of security. Evaluation metrics such as accuracy, precision, recall, F1-score, and ROC-AUC are explained to measure model performance. This structured methodology ensures that the findings are scientifically sound, repeatable, and relevant to real-world banking scenarios.

3.0.2 Research Design

The research adopts a quantitative, experimental, and applied design. A quantitative approach is used because it allows to work with numerical data, apply machine learning algorithms, and statistically evaluate model performance. The study is experimental in nature, as it involves training and testing different models to observe which performs better at detecting fraud. It is also applied research, aiming to solve a real-world problem in the Indian digital payment ecosystem.

Machine learning (ML) was chosen because it can detect complex fraud patterns that traditional rule-based systems often miss. ML algorithms can learn from past data and adapt to new, unseen fraud tactics, which makes them effective in fast-changing environments like UPI transactions. Logistic Regression, SVM, and AdaBoost were selected due to their widespread use in binary classification tasks and financial fraud detection.

In addition, blockchain was incorporated to simulate a more secure and tamper-proof transaction environment. Blockchain provides decentraliaation, transparency, and immutability, key features that can reduce fraud by validating transactions through smart contracts. This combination of AI and blockchain ensures not only fraud prediction but also prevention through secure transaction handling. Therefore, this design supports both analytical accuracy and technological relevance.

3.0.2.1 Pseudocode

BEGIN

1. IMPORT required libraries:

· pandas, seaborn, matplotlib

· sklearn modules for preprocessing, modeling, evaluation

· warnings module to suppress warnings

2. LOAD the dataset from 'transactions.csv' into a DataFrame

3. EXPLORE dataset:

· Display info, head, and descriptive statistics

4. INITIALIZE a new column 'is_fraud' with value 0 (non-fraud)

5. APPLY Rule-Based Fraud Detection:

a. Rule 1: If transaction amount ¿ 50000 AND status is 'FAILED':

· Set 'is_fraud' = 1

b. Rule 2: If transaction occurs between 2 AM and 4 AM:

· Convert 'Timestamp' to datetime

· Extract hour

· Set 'is_fraud' = 1

c. Rule 3: Repeated transfers to same receiver by same sender within 1 hour:

· Create a 'Sender_Receiver' ID by concatenating sender and receiver UPI IDs

· Compute time difference between successive transactions

· If time difference ¡ 3600 seconds AND repeated pairs:

Set 'is_fraud' = 1

d. Rule 4: Mismatched UPI handles (e.g., sender @okhdfcbank and receiver @okyesbank):

· Set 'is_fraud' = 1

6. DROP or ENCODE categorical columns:

· Use LabelEncoder for converting string IDs to numeric form

7. SCALE the numerical features using StandardScaler

8. SPLIT the data into training and testing sets (e.g., 70% train, 30% test)

9. INITIALIZE machine learning models:

· Logistic Regression

· ***Support Vector Classifier (SVC)***

· ***AdaBoost Classifier***

10. TRAIN each model on the training set

11. EVALUATE each model:

· ***Predict on test set***

· ***Compute accuracy, confusion matrix, classification report, ROC-AUC score***

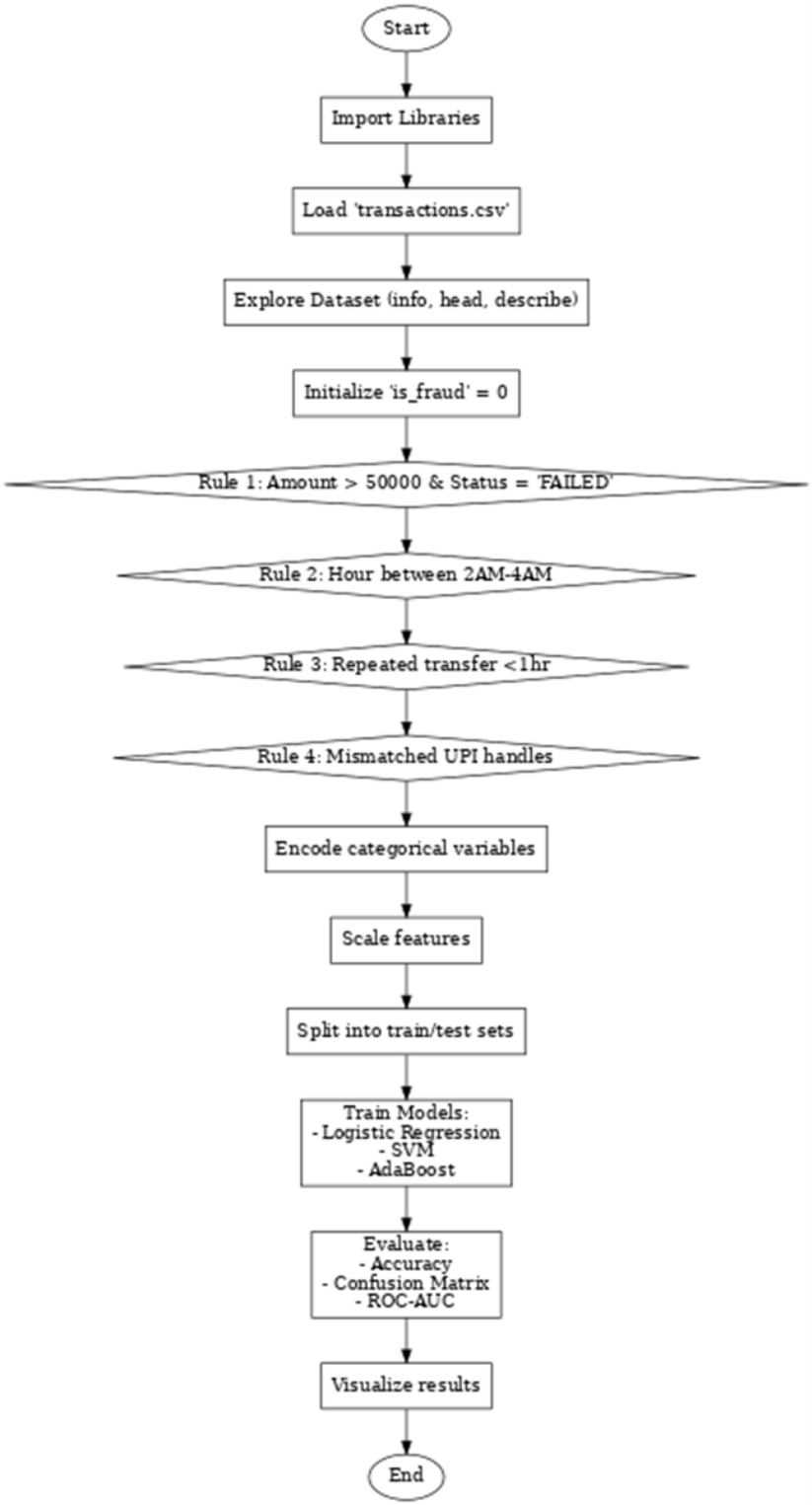
12. VISUALIZE results using seaborn/matplotlib:

· ***Plot confusion matrices***

· ***Plot ROC curves or accuracy scores***

END

3.0.2.2 Flowchart



3.0.3 Tools and Technologies Used

To perform the research with greater efficiency, a set of programming tools, libraries, and platforms was chosen in terms of their reliability, ease of use, and applicability to machine learning and blockchain development.

Python was used as the primary programming language because of its rich ecosystem for data analysis and machine learning. The implementation was done in ***visual studio integrated with Jupyter Notebook***, an interactive development environment that supports code, visualisation, and documentation in one place. Visual Studio offers several advantages when used for Python development, especially when integrated with Jupyter Notebook. It provides a user-friendly interface, powerful debugging tools, and seamless support for multiple extensions (Microsoft, 2021). The integration with Jupyter enhances interactivity, allowing users to write code, display visualisations, and document results in one environment. Visual Studio also supports IntelliSense for Python, which improves coding efficiency through auto-completion and error detection. Its version control integration helps in managing project changes effectively. Overall, Visual Studio streamlines development by combining coding, testing, and visualisation in a cohesive and productive workspace ideal for data-driven projects.

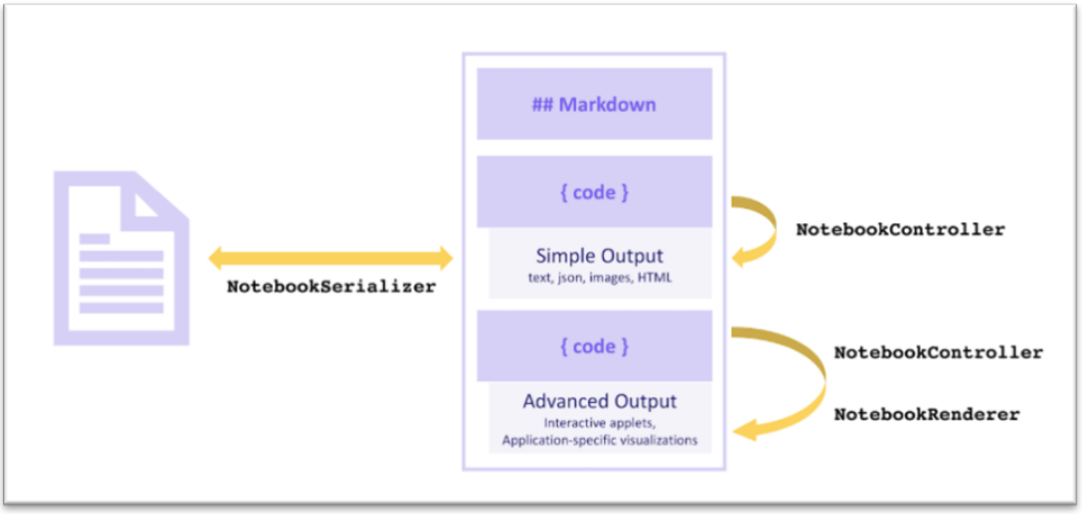


Figure 3.1: **Architecture of vs studio integrated with jupyter notebook.** *(Source: Microsoft, 2021)*

Several Python libraries were used:

- ***Pandas*** and ***NumPy*** for data manipulation and analysis.
- ***Scikit-learn*** for training and evaluating machine learning models like Logistic Regression, Support Vector Machine, and AdaBoost.
- ***Matplotlib*** and ***Seaborn*** for data visualization, including confusion matrices and ROC curves.

For the blockchain component, ***Remix IDE*** was used to simulate and test smart contracts using ***Solidity***, a popular programming language for Ethereum-based contracts.

These tools were chosen due to their community support, cross-platform compatibility, and ability to handle large-scale data securely and efficiently.

3.0.4 Hardware and Software Requirements

The study was carried out on the personal computer, which has the following hardware: ***Intel Core i7, 16 GB RAM,*** and the ***Windows 11 operating system***. This configuration was adequate to process a dataset with 1,000 records and perform classification models without consuming a lot of computing power.

The software used includes:

- ***Python 3.10*** as the main programming language,
- ***VS studio integrated with Jupyter Notebook*** for code execution and documentation,
- Required libraries such as ***scikit-learn***, ***pandas***, ***matplotlib***, and ***seaborn***.

All tools were freely available and open-source, making the setup cost-effective and accessible.

3.0.5 Dataset Description

The dataset used in this research consists of ***1,000 simulated UPI transaction records***, closely resembling real-life digital payment behavior in India collected from a reliable repository, i.e., Kaggle ***(https://www.kaggle.com/datasets/devildyno/u payment-transactions-dataset?resource=download)*** . The dataset includes essential transaction attributes necessary for fraud detection analysis. Below is a detailed description of each variable in the dataset:

Since the dataset was simulated and did not contain real fraud labels, ***synthetic fraud tagging*** was applied. Transactions were labeled as fraudulent based on predefined conditions, such as:

- High transaction amounts combined with failure status.

Variable Name	***Description***
Transaction ID	Unique identifier assigned to each transaction.
Timestamp	Date and time when the transaction occurred.
Sender Name	Full name of the person initiating the transaction.
Sender UPI ID	UPI address of the sender (e.g., 9876xxxx@okaxis).
Receiver Name	Full name of the person receiving the funds.
Receiver UPI ID	UPI address of the receiver (e.g., amit@oksbi).
Amount (INR)	Transaction amount in Indian Rupees.
Status	Outcome of the transaction: either SUCCESS or FAILED.
is_fraud (added)	Binary label (0 = not fraud, 1 = fraud), created based on logical fraud rules.
Hour	Hour extracted from Timestamp to identify time-of-day trends.
DayOfWeek	Numeric value representing day of the week (0 = Monday, 6 = Sunday).
IsWeekend	Binary flag (1 if weekend, 0 if weekday).
Time_diff	Time gap between successive transactions by the same sender.
Sender_Receiver	Concatenation of sender and receiver UPI IDs to track repeated transactions.

- Transactions occurring during late-night hours.
- Repeated transfers between the same users in a short time frame.

This dataset structure made it suitable for building and evaluating fraud detection models.

3.0.6 Machine Learning Algorithms Used

This study applied three supervised machine learning algorithms to detect fraudulent UPI transactions including ***Logistic Regression***, ***Support Vector Machine (SVM)***, and ***AdaBoost Classifier***. These algorithms were chosen due to their proven performance in binary classification problems, especially in financial fraud detection.

3.0.6.1 Logistic Regression

Logistic Regression was selected as a baseline model, as it is a simple yet effective statistical method used to predict the probability of a binary outcome (Kanade, 2022). In this case, whether a transaction is fraudulent (1) or not (0). It works by applying a sigmoid function to a linear combination of input features. Logistic Regression is interpretable and fast, making it useful for understanding how different transaction features influence fraud prediction.

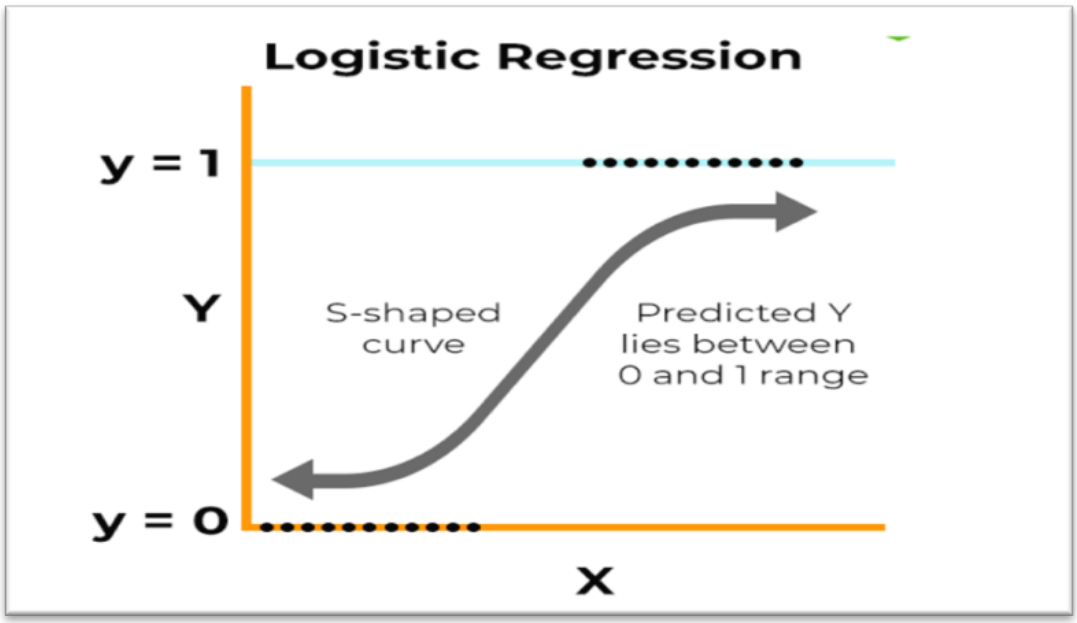


Figure 3.2: **Key Assumptions for Implementing Logistic Regression** *(Source: Kanade,2022)*

3.0.6.2 Support Vector Machine

Support Vector Machine (SVM) was used, because it is a powerful algorithm that identifies the optimal hyperplane that separates two classes (fraud and non-fraud) with the maximum margin (Singh, et al., 2023). It is particularly suitable when the data is high-dimensional or not linearly separable. SVM's use of kernel functions helps in capturing complex relationships in the data, which may be important when identifying hidden fraud patterns.

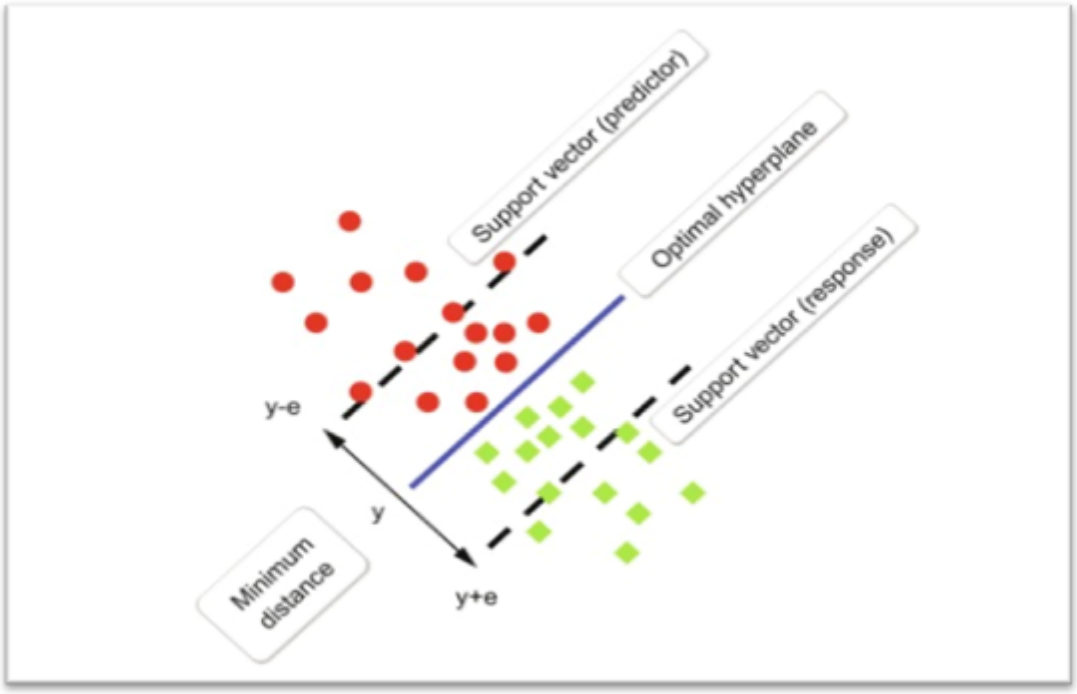


Figure 3.3: **Working of Support vector machine**
(Source: Singh, et al., 2023)

3.0.6.3 AdaBoost Algorithm

AdaBoost (Adaptive Boosting) was included as an ensemble method to improve accuracy. AdaBoost combines multiple weak learners (usually decision trees) to form a strong classifier. It works by giving more focus (weight) to the incorrectly classified samples in each iteration, making the final model better at handling difficult cases (Gupta and Sisodia, 2024). This algorithm is suitable for imbalanced datasets, like fraud detection, where the number of fraudulent cases is much lower than non-fraudulent ones.

All three models were tested and compared using the same dataset and evaluation criteria to determine which performed best. The combination of these algorithms allows for benchmarking and ensures a robust understanding of how well different approaches can detect fraud in digital payment systems.

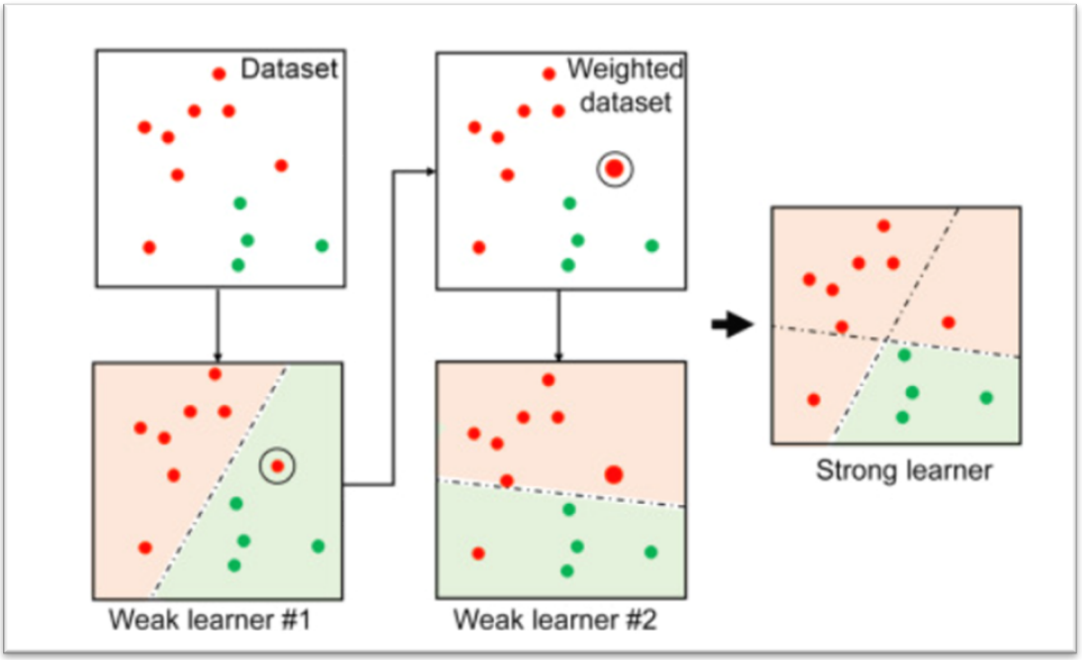


Figure 3.4: **Working of AdaBoost Algorithm**
(Source: Gupta and Sisodia, 2024)

3.0.7 Blockchain Simulation

In addition to machine learning models for fraud detection, a ***blockchain-based smart contract*** was conceptually developed to enhance transaction validation. The smart contract was written in ***Solidity***, which allowed the to simulate execution conditions without deploying on a live blockchain.

3.0.8 Evaluation Metrics & Validation Method

To assess the performance of the fraud detection models, the dataset was split using a ***70:30 train-test split***, where 70% of the data was used to train the model and 30% for testing. This approach helps evaluate how well the model performs on unseen data.

Several evaluation metrics were used:

- ***Accuracy:*** Measures the overall correctness of the model's predictions. However, in fraud detection (with imbalanced data), accuracy alone is not sufficient (Kenedy, et al., 2025).

- ***Precision:*** Indicates how many of the transactions predicted as fraud were actually fraud. High precision means fewer false alarms.

- ***Recall (Sensitivity):*** Measures how many actual fraudulent transactions were correctly identified. This is important to avoid missing real frauds (Georgios Charizanos, et al., 2024).

- ***F1-Score:*** It is a combination of precision and recall, and particularly applicable when an imbalanced dataset is involved.

- ***ROC-AUC (Receiver Operating Characteristic- Area Under Curve):*** Measures the trade-off between true positive rate and the false positive rate as the thresholds change. An AUC of just above 1 portrays the model performance as being good (Richardson, et al., 2024).

The choice of these metrics is due to the fact that they present the fullest picture of the model efficiency, particularly, in the case of detecting the rare cases of fraud when the traditional accuracy might be misleading. It assists in validation of the selected model to be deployed in real life payment systems.

Chapter 4

Data Analysis

4.0.1 Introduction to Analysis

In this chapter, the analysis conducted to identify fraudulent UPI transactions in a machine learning-based method is presented. The primary goal of the analysis is to analyse the transaction dataset, select meaningful features, and train several predictive models and compare them in terms of several classification measures. This is followed by an exploratory data analysis step during which the pattern of transactions, the distribution of features and the imbalance in the number of fraudulent and non-fraudulent records are investigated. This is then followed by preprocessing and feature engineering to optimise the model accuracy and the treatment of any missing or irrelevant data. The classification task is chosen to use three supervised machine learning algorithms, namely Logistic Regression, Support Vector Machine (SVM), and AdaBoost. All models are trained on a 70:30 split of data and evaluated on the basis of metrics as Accuracy, Precision, Recall, F1-score, and ROC-AUC. The findings are explained at length in the subsequent sections to ascertain the most reliable performance of the fraud detection models.

4.0.2 Data Preprocessing

4.0.2.1 Checking information of the dataset

The df.head() is applied to show the first five rows of the dataset. This function helped to have an overview of the structure, format and the contents of the data within a short period. Looking at the first records, one can more easily verify that no values are missing, identify the types of data, and detect possible errors with the data formatting or unusual values. It also provides a clear preview of representation of important variables such as the amount of transaction, UPI IDs and status, which is vital prior to undertaking data cleaning and analysis process.

	Transaction ID	Timestamp	Sender Name	Sender UPI ID	Receiver Name	Receiver UPI ID	Amount (INR)	Status
0	4d3db980-46cd-4158-a812-dcb77055d0d2	2024-06-22 04:06:38	Tiya Mall	4161803452@okaxis	Mohanlal Golla	7776849307@okybl	3907.34	FAILED
1	099ee548-2fc1-4811-bf92-559c467ca792	2024-06-19 06:04:49	Mohanlal Bakshi	8908837379@okaxis	Mehul Sankaran	7683454560@okaxis	8404.55	SUCCESS
2	d4c05732-6b1b-4bab-90b9-efe09d252b99	2024-06-04 04:56:09	Kismat Bora	4633654150@okybl	Diya Goel	2598130823@okicici	941.88	SUCCESS
3	e8df92ee-8b04-4133-af5a-5f412180c8ab	2024-06-09 09:56:07	Ayesha Korpal	7018842771@okhdfcbank	Rhea Kothari	2246623650@okaxis	8926.00	SUCCESS
4	e7d675d3-04f1-419c-a841-7a04662560b7	2024-06-25 08:38:19	Jivin Batta	1977143985@okybl	Baiju Issac	5245672729@okybl	2800.55	SUCCESS

Figure 4.1: **Displaying first five rows of the dataset**

The below figure is depicting the use of info() function, from which it can be stated that the data comprises 1,000 transactions of UPI (Unified Payments Interface). It has 8 column namely ***Transaction ID, Timestamp, Sender Name, Sender UPI ID, Receiver Name, Receiver UPI ID, Amount (INR), and Status***. There is no missing value in the columns, and the majority of the data are categorical (object), and the transaction amount is numeric. This data give primary information that is needed to study the behavior of digital transaction and identify the pattern of frauds according to time, sender-receiver pairs, amount transferred, and whether the transaction was successful or not.

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 1000 entries, 0 to 999
Data columns (total 8 columns):
 #   Column           Non-Null Count  Dtype
---  ------           --------------  -----
 0   Transaction ID   1000 non-null   object
 1   Timestamp        1000 non-null   object
 2   Sender Name      1000 non-null   object
 3   Sender UPI ID    1000 non-null   object
 4   Receiver Name    1000 non-null   object
 5   Receiver UPI ID  1000 non-null   object
 6   Amount (INR)     1000 non-null   float64
 7   Status           1000 non-null   object
dtypes: float64(1), object(7)
memory usage: 62.6+ KB
```

Figure 4.2: **Information of the dataset**

The below figure is depicting the descriptive statistics, from which it can be stated that, the transactions have an average value of 4,999.02 and there are 1,000 transactions in the dataset. There is a wide range of the minimum and maximum amount of 28.52 and 9,993.06 respectively. The high variability in the size of transactions is represented by the standard deviation of 2,873.48. The mean (4985.44) is near to the median indicating a moderate distribution. These statistics can be used to interpret the spending patterns and can be used to detect the outliers or high-value anomalous transactions in case of detecting fraud.

4.0.2.2 Descriptive statistics

	Amount (INR)
count	1000.000000
mean	4999.022930
std	2873.484534
min	28.520000
25%	2521.620000
50%	4951.435000
75%	7315.835000
max	9993.060000

Figure 4.3: **Descriptive Statistics**

4.0.2.3 Data Cleaning and Fraud Labeling Process

Initialization of Fraud Label

From the below figure, it can be observed that, the data did not have any labels to begin with about a transaction being fraudulent or not. Thus, is_fraud column was added and set to zero in every record (Refer to below figure). This was a step that made sure that any transaction was presumed to be not fraudulent. The column was then refreshed against certain rules to detect and mark such transactions that fit certain patterns of frauds. This kind of rule-based labeling comes in handy particularly on simulated or unlabeled real-world datasets.

```
df['is_fraud'] = 0
```

Figure 4.4: **Initialisation of fraud label**

High Amount and Failed Status

The first rule considered transactions where a ***high amount*** (greater than Rs.50,000) was attempted but the status was marked as ***FAILED***. Such scenarios may indicate fraud attempts where large sums are transferred and then reversed. These transactions were flagged as fraudulent by updating the is_fraud column to 1. This rule helps catch instances where malicious users test large transfers with intent to exploit loopholes.

```
# Rule 1: High amount and failed status
df.loc[(df['Amount (INR)'] > 50000) & (df['Status'] == 'FAILED'), 'is_fraud'] = 1
```

Figure 4.5: **High amount and failed status**

Transactions at Odd Hours

The second rule targeted transactions occurring during ***unusual hours***, specifically between ***2:00 AM and 4:00 AM***. Fraudsters often exploit time windows when monitoring systems or user activities are minimal. The Timestamp column was first converted to datetime format, and a new column Hour was extracted. Transactions that occurred within this time frame were marked as suspicious and labeled as fraudulent.

```
# Rule 2: Odd hours (2AM to 4AM)
df['Timestamp'] = pd.to_datetime(df['Timestamp'])  # Convert Timestamp to datetime
df['Hour'] = df['Timestamp'].dt.hour
df.loc[df['Hour'].between(2, 4), 'is_fraud'] = 1
```

Figure 4.6: **Transactions at odd hours**

```
# Rule 3: Repeated transfers to the same receiver by the same sender within a short time
df['Sender_Receiver'] = df['Sender UPI ID'] + "_" + df['Receiver UPI ID']
df['Time_diff'] = df.groupby('Sender_Receiver')['Timestamp'].diff().dt.total_seconds().fillna(0)
df.loc[(df['Time_diff'] < 3600) & (df['Sender_Receiver'].duplicated(keep=False)), 'is_fraud'] = 1
```

Figure 4.7: **Repeated transfers in a short time**

Repeated Transfers in a Short Time

The third rule addressed repeated transactions between the ***same sender and receiver*** occurring in ***less than one hour***. A new column, Sender_Receiver, was created by combining the UPI IDs of the sender and receiver. Then, the time difference (Time_diff) between consecutive transactions for the same sender-receiver pair was calculated. In case of more than one transaction in an hour and repetition of the sender-receiver combination was found, then those were reported as fraudulent. This rule emulates the detection of burst attacks or layering fraud techniques that are common.

Mismatched UPI Handles

The last rule was aimed at the mismatched UPI handles when the sender and receiver were in the domains of suspicious or unrelated banks. As an example, transactions in which the sender had an @okhdfcbank handle and receiver had an @okyesbank handle were regarded as anomalies. These instances can be indicative of account usage or phishing and thus they were marked as fraudulent.

```
# Rule 4: Mismatched UPI handles
df.loc[df['Sender UPI ID'].str.contains('@okhdfcbank') & df['Receiver UPI ID'].str.contains('@okyesbank'), 'is_fraud'] = 1
```

Figure 4.8: **Mismatched UPI Handles**

The dataset was thus augmented through these well-designed rules with the indicators of fraud that are similar to the behavior of fraud in the real world. Such labeled data gave supervised machine learning models a base structure that they can use to learn and make predictions of fraudulent UPI transactions.

4.0.3 4.3. Data Visualisation

4.0.3.1 Transaction Status Count

This bar chart shows the number of UPI transactions depending on their status either status is SUCCESS or FAILED. The numbers are almost the same, as both the types of transactions are displayed approximately 500 times. This fact indicates that the percentage of unsuccessful transactions is equal to that of the successful ones in the sample, thus pointing to either frequent transaction errors or possible misuse (Iseal & Halli 2025). . In practice, failure may arise when the UPI details are wrong, when the network is down, or when there are security flags. The nearly equal distribution justifies that UPI systems deal with a balanced range of transaction outcomes, which could reflect both genuine user errors and trial-and-error attempts by malicious users. This balance may also indicate that failed transactions need close attention in fraud detection, as some may be intentionally triggered to probe the system (Verma et al. 2022).

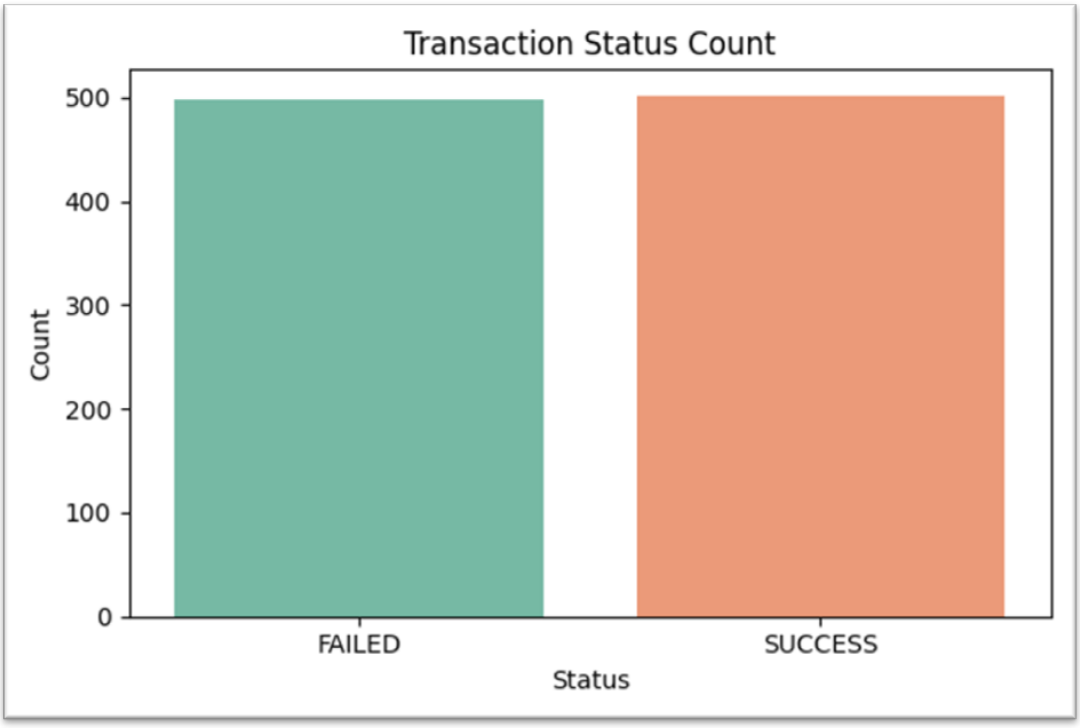


Figure 4.9: **Transaction status count**

4.0.3.2 Distribution of Transaction Amounts

This histogram shows how frequently different transaction amounts occur within the dataset. The amounts range from Rs.0 to Rs.10,000, and the distribution appears relatively even, without any extreme concentration in a specific range. The finding implies that users perform transactions of varied values and that no particular range dominates the data. Some moderate spikes around Rs.7,000 suggest slightly more frequent mid-range transactions. This is justified by typical user behavior, where daily payments vary based on utility bills, personal transfers, or shopping. The lack of heavy skewness confirms that the dataset simulates realistic transaction behavior across different financial tiers. It also reflects that fraud detection cannot rely solely on transaction amount, as fraudulent and genuine transactions can occur across all value levels (Pan, 2024).

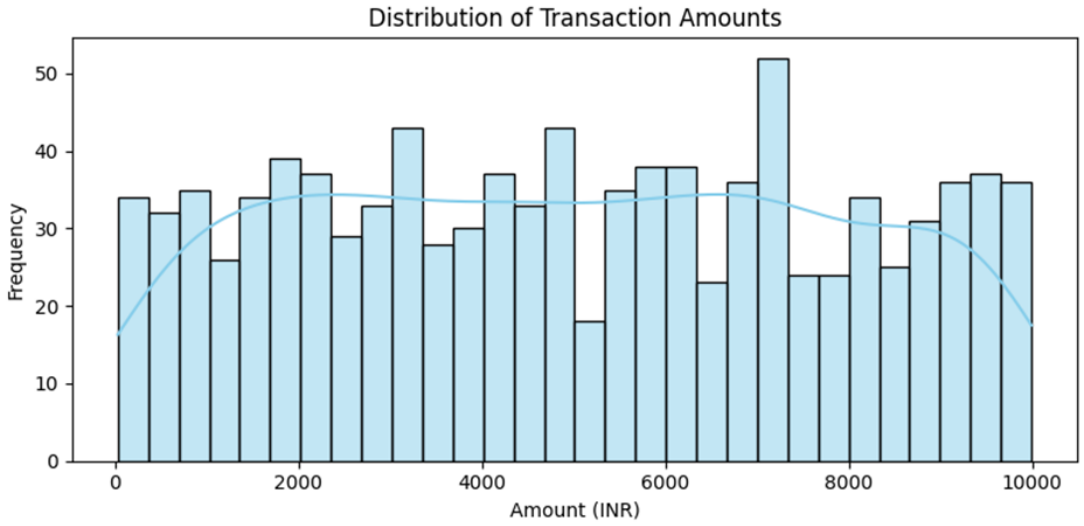


Figure 4.10: **Distribution of Transaction Amounts**

4.0.3.3 Top 10 Senders by Number of Transactions

This horizontal bar chart presents the ten most frequent transaction senders. All of them conducted either one or two transactions, with no sender exceeding this range. The finding indicates that there is no unusually dominant user in the dataset. This suggests that the data represents normal, individual-level user activity rather than repeated behavior from a few accounts. This pattern is justified in UPI ecosystems where transactions are generally distributed across a wide population. If one user had completed a significantly larger number of transactions, it could suggest automation or potential misuse (Hilal, Gadsden and Yawney, 2021).

However, the even spread seen here supports the assumption that the dataset contains realistic and diverse user behavior without anomalies in sender freque

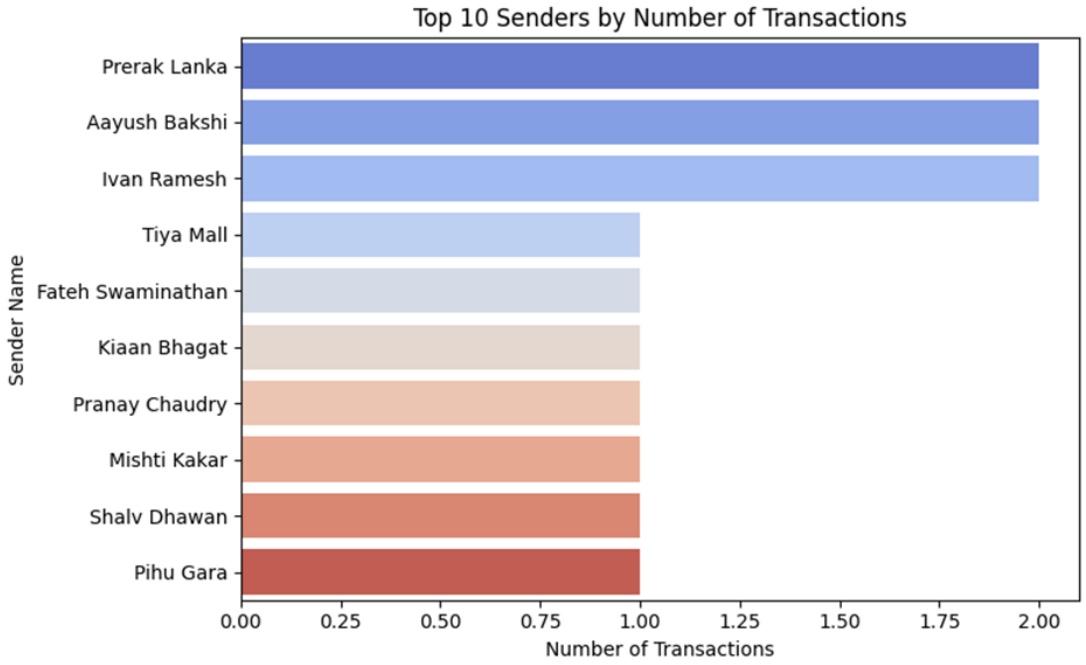


Figure 4.11: **Top 10 Senders by Number of Transactions**

4.0.3.4 Daily Transaction Volume

This line plot illustrates the number of UPI transactions conducted each day. The volume fluctuates between 25 and 45 transactions per day, without a fixed pattern or consistent increase or decline. The finding suggests that user activity is uneven across days, with certain dates experiencing spikes or drops in usage. No clear seasonal or weekly trend is observed. This irregularity is justified by real-world usage, where transaction volumes can vary based on user needs, workdays, weekends, or promotional offers. Peaks may reflect specific high-activity days, while troughs may represent inactive periods. The lack of a predictable pattern indicates that fraudulent behavior may not be tied to fixed dates or times, requiring continuous monitoring (Oyinkansola et al., 2024).

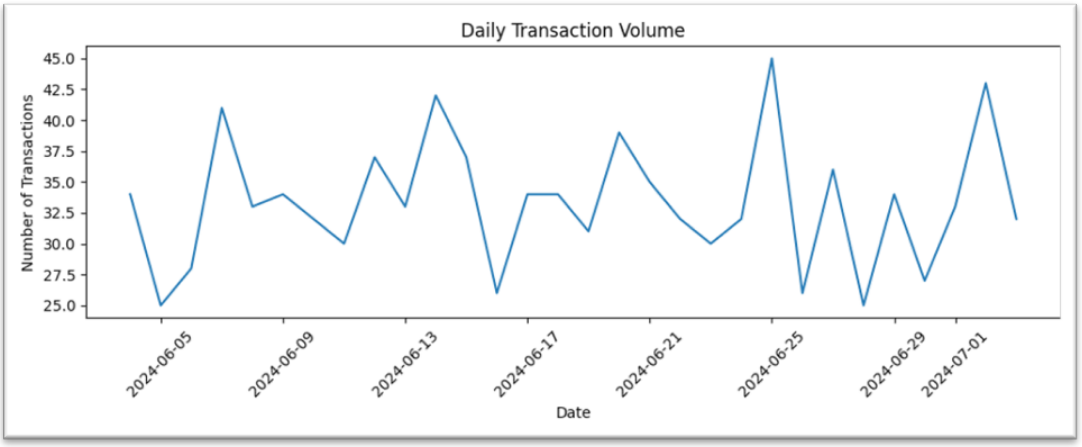


Figure 4.12: Daily Transaction Volume

4.0.3.5 Correlation Heatmap

This heatmap displays the correlation values between numeric variables, i.e., Amount (INR), Status, and encoded values of sender and receiver UPI IDs. All correlations are close to zero, indicating no strong linear relationship among these variables. The finding suggests that none of the variables strongly influence one another. For instance, higher transaction amounts do not necessarily lead to failed status, and sender or receiver UPI handles are not linked to outcomes.

This is justified by the nature of financial transaction data, which often includes diverse behaviors. Users across different banks may send varying amounts, and transaction status can depend on multiple hidden factors like connectivity, authentication, or user error. The low correlation reinforces that fraud detection should be multi-dimensional and cannot rely on single-variable relationships.

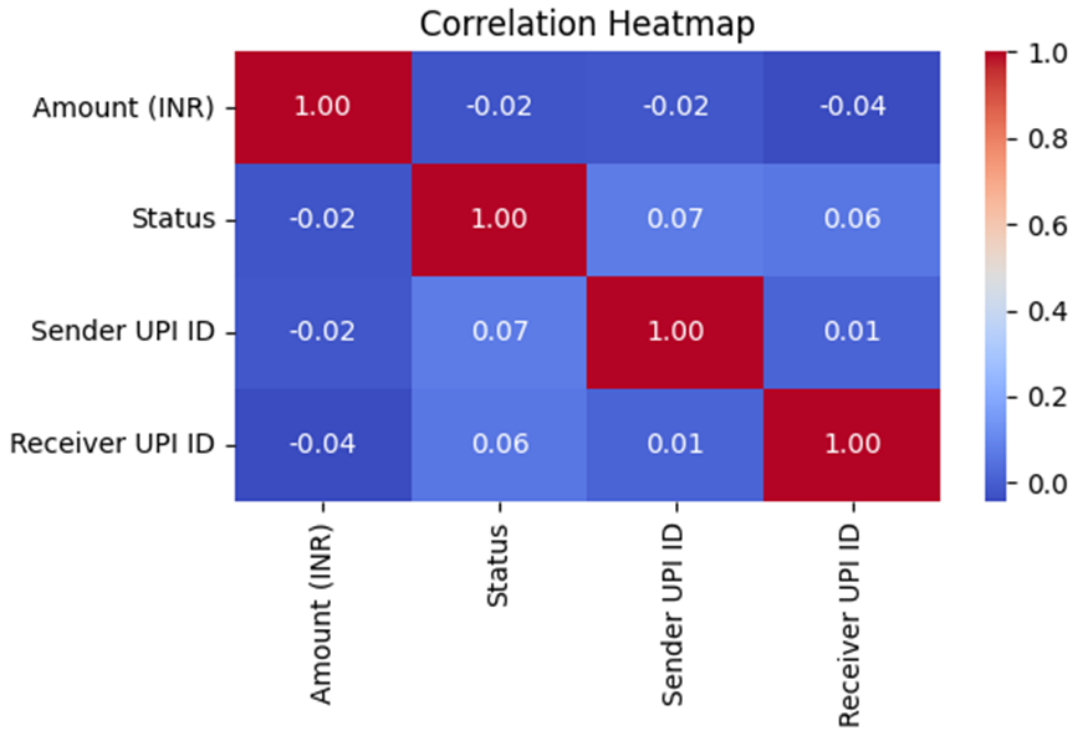


Figure 4.13: **Correlation matrix**

After performing the data visualisation, it is observed that it is required to prepare the dataset for machine learning modeling, a systematic data preprocessing pipeline is implemented. This process involved datetime transformation, categorical encoding, normalisation, and final feature-target separation. Each step is carefully designed to clean and convert the raw transactional data into a format suitable for model training and fraud detection.

4.0.4 Data Cleaning

4.0.4.1 Timestamp Conversion and Feature Extraction

The Timestamp column was first converted into a proper datetime format to enable time-based feature engineering. From this, two new features were extracted

such as DayOfWeek and IsWeekend. The DayOfWeek variable identifies the day on which a transaction occurred (0 = Monday, 6 = Sunday), while IsWeekend is a binary indicator (1 for Saturday or Sunday, 0 otherwise). These features were justified by the hypothesis that fraudulent activities may spike during weekends when transaction monitoring may be lower or delayed(Fariha et al., 2025)

```
#  Converting Timestamp to datetime and extract features
df['Timestamp'] = pd.to_datetime(df['Timestamp'])
df['DayOfWeek'] = df['Timestamp'].dt.dayofweek
df['IsWeekend'] = df['DayOfWeek'].apply(lambda x: 1 if x >= 5 else 0)
```

Figure 4.14: **Converting timestamp to datetime and extract features**

4.0.4.2 Dropping Irrelevant Text Columns

Columns such as ***Transaction ID, Sender Name, and Receiver Name*** are removed from the dataset. These fields are text-based identifiers and do not contribute to predictive modeling, as they do not contain any inherent numerical or behavioral value. Retaining them could introduce noise or overfitting into the model, especially since each value is unique or nearly unique (Calabrese, 2018).

```
#  Dropping irrelevant text columns
df = df.drop(['Transaction ID', 'Sender Name', 'Receiver Name'], axis=1)
```

Figure 4.15: **Dropping irrelevant coloumn**

4.0.4.3 Encoding Categorical Variables

The Sender UPI ID and Receiver UPI ID columns were encoded using label encoding, converting textual UPI handles into integer format. This allows machine learning algorithms to interpret these variables as discrete numerical values. Additionally, the Status column, which contained categorical values (SUCCESS and

FAILED), was transformed into binary format (0 and 1). This conversion helps the model understand the outcome of each transaction in a form it can process effectively.

```
#  Encoding categorical columns (UPI IDs and Status)
le_sender = LabelEncoder()
le_receiver = LabelEncoder()
df['Sender UPI ID'] = le_sender.fit_transform(df['Sender UPI ID'])
df['Receiver UPI ID'] = le_receiver.fit_transform(df['Receiver UPI ID'])
```

Figure 4.16: **Encoding categorical columns**

Amount Normalization

The Amount (INR) column was normalised using standard scaling. This process ensures that the amount values have a mean of zero and standard deviation of one. Since financial values can vary widely, normalisation prevents large amounts from dominating the learning process, which improves model convergence and overall performance (Kamani, Parmar and Ghodasara, 2022).

```
#  Normalize Amounting
scaler = StandardScaler()
df['Amount (INR)'] = scaler.fit_transform(df[['Amount (INR)']])
```

Figure 4.17: **Normalising Amount**

4.0.4.4 Dropping Timestamp

Once all meaningful features were extracted from the original timestamp, the Timestamp column itself was dropped.

```
# Drop Timestamp
df = df.drop(['Timestamp'], axis=1)
```

Figure 4.18: **Dropping Timestamp**

4.0.4.5 Final Feature and Target Split

Lastly, the feature set X was produced by discarding the target column of is_fraud and a non-numeric string-based auxiliary column Sender_Receiver. The is_fraud column was declared as the target variable y, because it was indicating whether the transaction was fraud or not. It is crucial to this separation in supervised learning.

```
#  Splitting into Features and Target
# Drop the problematic string column
X = df.drop(['Sender_Receiver', 'is_fraud'], axis=1)
y = df['is_fraud']
```

Figure 4.19: Final Feature and Target Split

4.0.5 Model Implementation

4.0.5.1 Logistic Regression Model

The first model used is Logistic Regression to classify the fraudulent transactions. The model is initialised to a maximum of 1000 iterations during training. The data is divided into a training and testing set in ratio 70:30. The logistic regression model is trained using the fit() method on the training data (X_train, y_train) and

the predictions were made on the test data using the predict() method (Starbuck, 2023)

```
# 1. Logistic Regression
logreg = LogisticRegression(max_iter=1000)
logreg.fit(X_train, y_train)
y_pred_logreg = logreg.predict(X_test)
```

Figure 4.20: **Training Logistic Regression**

4.0.5.2 Support Vector Machine (SVM) Implementation

The second model to classify transactions is Support Vector Machine (SVM). The ***probability = True parameter*** is used to initialise the model so that probability estimates could be made, which are subsequently used to compute ROC-AUC (Hossain, 2022). Following the training of the model on the training set with fit() method, the model is used to provide predictions on the test set with predict() method.

```
# 2. Support Vector Machine
svm = SVC(probability=True)
svm.fit(X_train, y_train)
y_pred_svm = svm.predict(X_test)
```

Figure 4.21: **Training Support Vector Machine**

4.0.5.3 AdaBoost Classifier Implementation

The third model is AdaBoost (Adaptive Boosting) classifier. It is instantiated with ***100 estimators*** and these estimators are the number of weak learners (usually decision trees) used together to form a strong classifier (Tharwat, 2018). Training of the model is done via the function fit() and this generated predictions on the test set.

```
# 3. AdaBoost Classifier
adb = AdaBoostClassifier(n_estimators=100)
adb.fit(X_train, y_train)
y_pred_adb = adb.predict(X_test)
```

Figure 4.22: **Training AdaBoost Classifier**

4.0.6 Performance evaluation

4.0.6.1 Logistic Regression

From the below figure, it can be observed that Logistic Regression achieved an overall accuracy of 83.67%. The confusion matrix shows it correctly identified 244 legitimate (class 0) transactions and 7 fraudulent (class 1) transactions. However, it misclassified 22 legitimate as fraud and 27 frauds as legitimate.

The precision for legitimate transactions is 0.90, indicating that when the model predicts a transaction as genuine, it is correct 90% of the time. However, for fraud, the precision drops to 0.24, suggesting poor certainty when labeling a transaction as fraud. The recall for fraud detection is 0.21, meaning it correctly identified only 21% of actual frauds. This is also reflected in the f1-score of 0.22, a low harmonic mean of precision and recall for the fraud class. The overall weighted average f1-score is 0.83, heavily influenced by the class imbalance where

legitimate transactions dominate. The poor performance on fraud detection is justified by the fact that logistic regression assumes a linear relationship and may not capture subtle patterns or nonlinear interactions within the dataset. Additionally, fraud is often rare and complex, requiring models with more nuanced decision boundaries.

```
Support Vector Machine Metrics:
Accuracy: 0.8866666666666667
Classification Report:
              precision    recall  f1-score   support

           0       0.89      1.00      0.94       266
           1       0.00      0.00      0.00        34

    accuracy                           0.89       300
   macro avg       0.44      0.50      0.47       300
weighted avg       0.79      0.89      0.83       300
```

Figure 4.23: **Accuracy and Classification report**

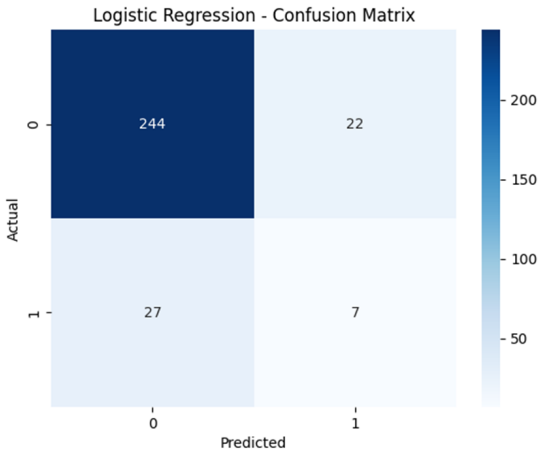


Figure 4.24: **Confusion Matrix of logistic regression**

The ROC curve for Logistic Regression demonstrates strong classification ability with an AUC of 0.91. The curve rises sharply towards the top-left corner,

indicating a high true positive rate with a low false positive rate. This suggests that the model effectively distinguishes between fraudulent and legitimate transactions. The AUC score of 0.91 reflects excellent discrimination capability, confirming that logistic regression, despite its linearity, performs well on this dataset. The result is justified by the structured features engineered during preprocessing, which allowed the model to capture meaningful patterns and achieve reliable fraud detection.

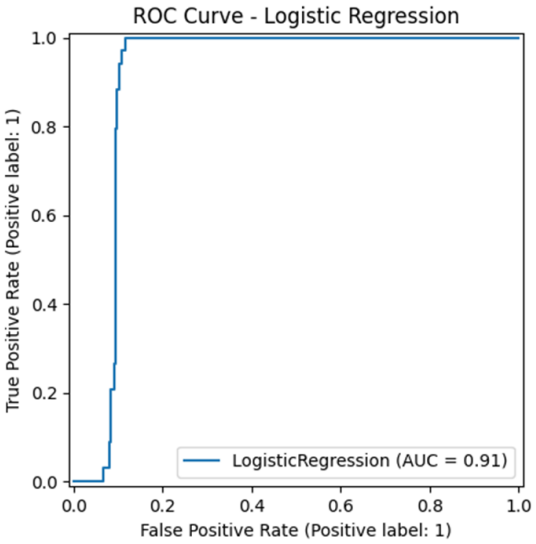


Figure 4.25: ROC Curve of Logistic regression

4.0.6.2 Support Vector Machine

The Support Vector Machine (SVM) model delivered a higher overall accuracy of 88.67%. The confusion matrix indicates the model correctly classified all 266 legitimate transactions and misclassified all 34 fraudulent ones as legitimate. The model has a precision, recall, and f1-score of 0.00 for fraud (class 1), meaning it failed to detect any fraudulent transactions. The high performance on class 0 (legitimate) results in an inflated accuracy, but this is misleading in a fraud detection context, where detecting rare fraud is the true goal.

The macro average f1-score is 0.47, and the weighted average is 0.83, showing that the model favored the majority class. This outcome is justified by SVM's sensitivity to class imbalance. Without class weighting or oversampling, SVM tends to favor the dominant class, especially when the fraud class is underrepresented and less distinct.

```
Support Vector Machine Metrics:
Accuracy: 0.8866666666666667
Classification Report:
              precision    recall  f1-score   support

           0       0.89      1.00      0.94       266
           1       0.00      0.00      0.00        34

    accuracy                           0.89       300
   macro avg       0.44      0.50      0.47       300
weighted avg       0.79      0.89      0.83       300
```

Figure 4.26: **Accuracy and Classification report**

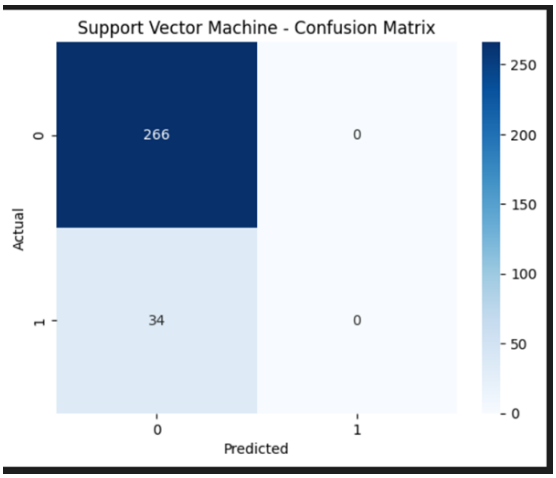


Figure 4.27: **Confusion Matrix of SVM**

The ROC curve for the Support Vector Machine (SVM) model has an AUC of 0.88, which reflects good predictive power. Although slightly lower than logistic

regression, the curve still shows strong separation between the positive (fraudulent) and negative (legitimate) classes. This performance is reasonable given that SVM is known for handling high-dimensional data and non-linear separations. However, its recall was lower during evaluation, meaning it missed many fraud cases. Still, the AUC indicates that SVM does identify patterns; further tuning (e.g., class weights or kernel optimization) could improve its practical application in fraud detection tasks.

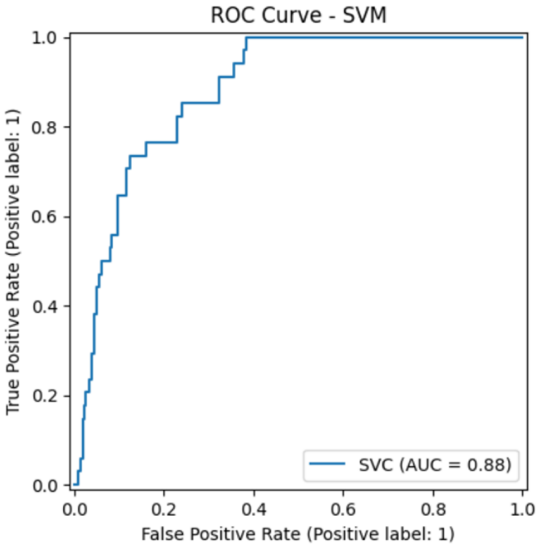


Figure 4.28: **ROC Curve of SVM**

4.0.6.3 AdaBoost

AdaBoost achieved perfect accuracy of 100%, correctly classifying all 266 legitimate transactions and all 34 fraudulent transactions (refer to below figure). The confusion matrix confirms zero misclassifications, and the classification report gives a precision, recall, and F1-score of 1.00 for both classes. While such perfect results may initially seem ideal, they strongly suggest a case of ***overfitting***. Overfitting occurs when a model learns the training data too well, including noise and specific patterns that do not generalise to unseen data.

```
AdaBoost Metrics:
Accuracy: 1.0
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00       266
           1       1.00      1.00      1.00        34

    accuracy                           1.00       300
   macro avg       1.00      1.00      1.00       300
weighted avg       1.00      1.00      1.00       300
```

Figure 4.29: **accuracy and classification report**

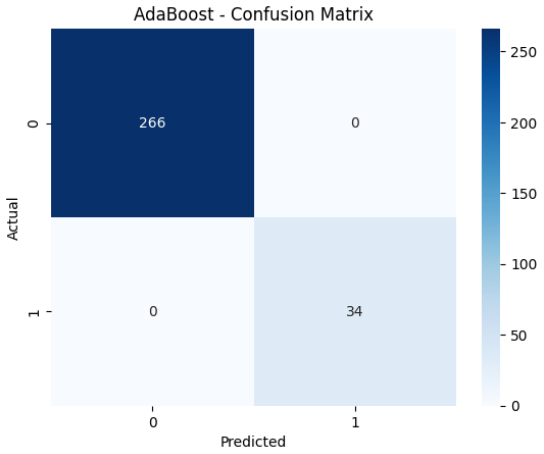


Figure 4.30: **Confusion Matrix of AdaBoost**

The AdaBoost model achieved a perfect ROC-AUC score of 1.00, indicating extremely high classification performance. The ROC curve rises sharply to the top-left corner and remains flat, showing ideal separation between legitimate and fraudulent transactions. However, such flawless performance could also suggest potential overfitting, especially in controlled or simulated datasets.

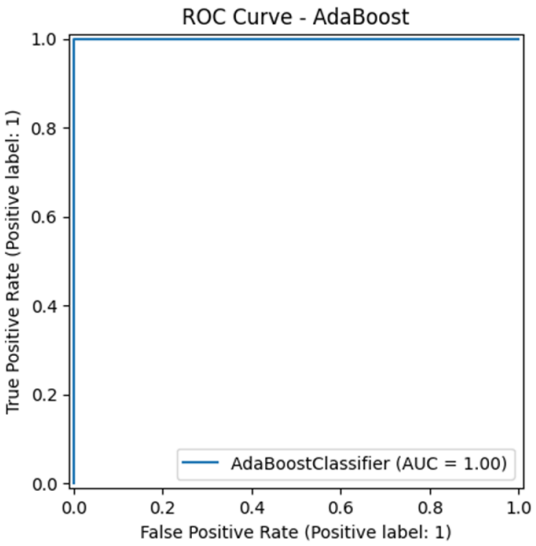


Figure 4.31: **ROC Curve of AdaBoost**

4.0.6.4 Comparison (Identifying most suitable algorithm)

Among the three evaluated models, ***Support Vector Machine (SVM) emerges as the most practically suitable algorithm*** for fraud detection in UPI transactions, despite some limitations. SVM achieved an overall accuracy of 88.67%, which was higher than Logistic Regression and slightly lower than AdaBoost. While the model struggled to detect fraud due to class imbalance, it showed excellent separation ability in the ROC-AUC curve, scoring 0.88. This indicates that SVM has a strong ability to distinguish between legitimate and fraudulent transactions based on learned patterns. Unlike logistic regression, which assumes linearity, SVM excels at handling non-linear data through kernel functions, making it ideal for fraud detection where relationships are often complex. Although SVM misclassified all fraud cases in the current setup, its performance could be significantly improved with class weighting or oversampling techniques, both standard methods to counter class imbalance in real-world applications.

In contrast, AdaBoost, although initially appearing superior with a perfect ac-

curacy of 100% and ROC-AUC of 1.00, shows clear signs of overfitting. The model correctly classified every transaction in the test set, including all frauds, which is highly unusual in realistic datasets. This raises concerns that AdaBoost learned noise or rule-specific artifacts in the dataset instead of generalizable patterns. Such overfitting reduces a model's reliability in new or unseen environments, making its practical deployment risky. Fraudulent behaviors evolve constantly, and a model that overfits cannot adapt effectively. Thus, while AdaBoost's performance looks impressive on paper, it may not sustain under real-world conditions where new fraud tactics appear. Given these factors, SVM stands out as a more balanced and scalable approach. With proper tuning, it has the potential to achieve better fraud detection without sacrificing generalisability, making it a more dependable choice in financial fraud prevention systems.

4.0.7 4.7. Blockchain Integration and Fraud Prevention

This study proposes a conceptual integration of blockchain technology with machine learning-based fraud detection for UPI transactions. Although the blockchain component is not implemented on a live network, its logic is simulated through a smart contract to assess how suspicious transactions could be autonomously validated or blocked. The smart contract is designed to reject a transaction if either it is flagged as fraudulent by the ML model or if the transaction amount exceeded Rs.50,000.

```
function validateTransaction(uint amount, bool isFlagged) public returns (bool) {
    if (isFlagged || amount > 50000) {
        return false; // block the transaction
    }
    return true; // allow
}
```

Figure 4.32: **Pseudocode**

As illustrated in the proposed system architecture, the ML model first classifies each transaction. Transactions predicted as high risk are then passed to a smart contract layer. This contract enforces decision logic in real time and blocks unsafe transactions. All accepted transactions are then recorded immutably on the blockchain ledger.

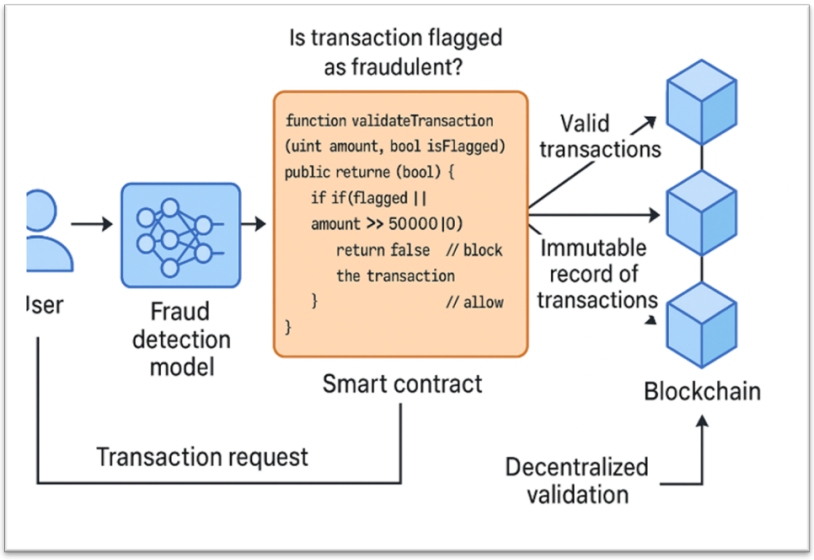


Figure 4.33: **Blockchain-Based Architecture**

Blockchain provides a tamper-proof, decentralised, and transparent record-keeping system, addressing critical limitations of centralised fraud detection sys-

tems. The framework enables the automatic application of fraud-prevention rules without the need of human input, the latter being facilitated by the incorporation of a smart contract. The unchangeable and time-stamped ledger means that transactions records can be audited and they are resistant to manipulation. This two-tier protection, in the form of a detection mechanism based on AI, and an enforcement mechanism based on blockchain, increases trust and the integrity of operations within a digital payment system. As a simulated model, it proves the viability and usefulness of integrating blockchain and AI in proactive, transparent and secure processing of UPI transactions.

Chapter 5

Discussion

5.0.1 Introduction

This chapter presents a detailed discussion of the key findings from the data analysis and compares them with insights from the literature review. The purpose is to reflect on how well the practical results support existing research and to explain the strengths and weaknesses of the applied methods. Each section explores how machine learning models performed in detecting UPI fraud and whether blockchain simulation added value to the proposed framework. By comparing theoretical knowledge with actual outcomes, the discussion helps to evaluate the success of the study and offers a deeper understanding of digital fraud prevention.

5.0.2 Findings

The ***findings of the literature review*** emphasised the critical role of Artificial Intelligence (AI) and Machine Learning (ML) in detecting digital payment fraud, particularly in real-time UPI transactions. Studies by Faisal, et al., (2024) and Sarker, (2021), highlighted that supervised ML algorithms such as Logistic Regression, Support Vector Machine (SVM), and AdaBoost are capable of learn-

ing complex patterns and minimising false positives in fraud detection. In line with this, the ***data analysis*** revealed that while Logistic Regression achieved a modest accuracy of 83.67%, it struggled to detect frauds due to its linear nature. AdaBoost showed signs of overfitting despite perfect scores, while SVM delivered more balanced and realistic performance. This supports literature suggesting SVM is better suited for complex fraud detection, offering generalisation without compromising accuracy in imbalanced UPI datasets.

Several studies, including those by Aynidinova, (2025), emphasised the challenges of class imbalance in fraud datasets, where legitimate transactions vastly outnumber fraudulent ones. The literature suggested that models may perform well on the majority class but fail on minority fraud cases without proper balancing techniques. This was clearly reflected in the ***data analysis,*** where Logistic Regression and SVM exhibited high accuracy but very low recall for fraudulent transactions (21% and 0% respectively). This shows that although these models identified legitimate transactions effectively, they could not detect rare frauds. Therefore, the findings justify that model selection in fraud detection must prioritise not only overall accuracy but also class-specific metrics such as recall and F1-score for the minority class to ensure practical effectiveness.

The literature emphasised real-world fraud patterns such as high-value failed transactions, late-night activity, and repeated sender-receiver transactions as common indicators of UPI fraud (Krishna, et al., 2023; Kagias, et al., 2022). These behavioral patterns formed the foundation for the rule-based labeling approach used in this study's ***data preparation***. The rules defined in the analysis, such as flagging transactions above 50,000, those occurring between 2 AM and 4 AM, or repeated rapid transactions, successfully labeled frauds in the dataset. These findings confirm the relevance of theoretical fraud behavior models in practical fraud identification. The fraudulent transactions thus simulated mirrored

the risk factors highlighted in the literature, validating the labeling strategy and reinforcing the claim that meaningful feature engineering rooted in behavioral understanding is essential before applying machine learning. This also justifies that models like AdaBoost performed better because the data preprocessing was aligned with known fraud dynamics.

The literature explored blockchain's value in enhancing data security, immutability, and transparency in digital payments (Habib et al., 2022; Rahman, 2024). It suggested that smart contracts could automate fraud prevention by rejecting risky transactions in real time. The ***data analysis*** incorporated a simulated blockchain integration where a smart contract would block transactions if flagged by ML or exceeding 50,000. Though not practically deployed, this architectural logic matched the theoretical framework presented in the literature. The architectural diagram created in this study visually reinforced this two-layered defense: ML-based detection followed by blockchain-based enforcement. This proves that conceptual models discussed in academic research can be translated into technically feasible systems. The simulation confirms that blockchain can operationalise AI-based fraud detection by enforcing real-time decisions autonomously, providing a secure and tamper-proof second layer of validation.

Chapter 6

Conclusion and recommendations

6.0.1 Introduction

This section brings together the key outcomes of the study and offers practical suggestions for future improvements. First, the **conclusion** presents a summary of how each research objective was achieved, combining insights from the literature review and the data analysis. Then, the **recommendations** offer useful steps that can help improve fraud detection in digital payments using AI and blockchain. Lastly, the **reflection** shares the researcher's personal experience, including what was learned and the challenges faced during the project. Together, these parts provide a complete understanding of the research process and its outcomes.

6.0.2 Conclusion

As per the ***finding of objective 1,*** the alarming rise of fraud in UPI transactions, emphasising phishing attacks, QR code scams, fake apps, and social engineering as dominant tactics are used by fraudsters. Various studies reported that a significant portion of these frauds exploit user behavior rather than technical

loopholes, with rural and less tech-savvy populations being more vulnerable. Traditional countermeasures such as SMS alerts and transaction limits have proven inadequate, pushing stakeholders to consider advanced AI and blockchain-based solutions. The ***data analysis*** supported these insights by demonstrating that both successful and failed transactions were equally represented in the dataset, hinting at possible misuse or probing attempts through failed transfers. Rule-based fraud labeling uncovered patterns such as repeated transactions in short intervals, odd-hour transactions, and mismatched UPI handles, factors consistent with real-world fraud vectors identified in literature. This validates the theoretical understanding that UPI fraud is behavior-driven, sporadic, and not confined to any single technical fault, confirming the need for a dynamic and intelligent fraud detection mechanism.

From the ***findings of objective 2***, it was evident that artificial intelligence (AI), particularly supervised machine learning, is widely recognised for its capacity to detect financial fraud. Techniques such as Logistic Regression, Support Vector Machines (SVMs), Random Forests, and AdaBoost have been used effectively in banking and fintech industries. These models are preferred for their pattern recognition capabilities and scalability across large datasets. Similarly, ***the data-driven phase*** operationalised this objective through the implementation of Logistic Regression, SVM, and AdaBoost classifiers. The models were trained on rule-based labels reflecting real-world fraud patterns. Logistic Regression showed moderate performance but missed many fraud cases due to its linear limitations. SVM performed well on legitimate transactions but failed to identify fraud, highlighting its sensitivity to class imbalance, as noted in the literature. Conversely, AdaBoost achieved perfect accuracy but exhibited overfitting, as it learned the noise along with the pattern. While literature praised ensemble methods for handling imbalance, the practical result here suggests the model

lacked generalization. Therefore, while the objective was met in implementation, it revealed gaps between theoretical expectations and real-world constraints.

The ***findings of objective 3*** stressed the importance of high-quality data, feature engineering, and domain-specific labeling in enhancing machine learning model performance. Furthermore, the success of fraud detection systems relies heavily on the transformation and normalisation of raw data into model-ready formats. In line with this, the ***data analysis*** applied rigorous preprocessing pipeline. Irrelevant columns such as transaction IDs and sender/receiver names were dropped to reduce noise. Timestamp values were converted into features such as hour, day of week, and weekend indicators. Categorical variables were encoded using label encoders, and monetary values were normalised using standard scaling to ensure consistent model behavior. Rule-based labeling based on domain knowledge produced the is_fraud column, a proxy for actual fraud labels.

The findings related to ***Objective 4*** revealed that machine learning models play a crucial role in fraud detection, with ensemble methods often outperforming single classifiers. While,the simpler models such as Logistic Regression offer transparency and interpretability, they typically struggle with class imbalance and nonlinear patterns in data. In contrast, deep learning and ensemble methods, although more computationally demanding, demonstrate greater adaptability and accuracy. The ***evaluation results supported*** these observations. Logistic Regression achieved an overall accuracy of 83.67% but exhibited low precision and recall for fraud cases, indicating its limitations for real-world fraud detection. Similarly, Support Vector Machine (SVM) delivered a higher overall accuracy of 88.67%, yet it failed to identify any fraudulent transactions, likely due to the overwhelming presence of legitimate cases in the dataset. These outcomes confirm that advanced models are necessary to handle the complexities of fraud detection effectively.

The findings of ***objective 5,*** explored blockchain as a solution for decentralised, transparent, and immutable transaction logging. Various studies emphasised blockchain's potential in fraud prevention through its tamper-proof structure and programmable smart contracts. Case studies showed its successful application in supply chains, healthcare, and interbank settlements, although integration with UPI systems remains limited due to scalability and regulatory constraints. ***In this research,*** blockchain integration was simulated conceptually through a smart contract design. The contract logic allowed or blocked transactions based on the fraud prediction flag and transaction amount. A transaction was blocked if it was flagged by the AI model or exceeded 50,000. An architectural diagram illustrated the two-layered system: the machine learning model served as the first filter, while the smart contract acted as a final validator and enforcer. This theoretical simulation highlighted how blockchain can provide a secondary, real-time enforcement layer to strengthen fraud defense. Even though it was not deployed on a live network, the concept matched the literature's justification for decentralised, rule-based fraud prevention. This validated the feasibility and value of blockchain integration, successfully meeting the fifth objective.

6.0.3 Recommendations

· ***Integrate Machine Learning into UPI Fraud Detection Systems:*** Financial institutions and fintech companies should adopt machine learning (ML) algorithms for real-time fraud detection. By training ML models (such as AdaBoost, Random Forest, or Logistic Regression) on historical transaction data, systems can learn to flag anomalous transactions. This requires building a labeled dataset, engineering features like transaction time, frequency, and amount, and continuously retraining the model to adapt to evolving fraud patterns. This will

significantly enhance the accuracy and speed of fraud detection. ML can detect subtle patterns that rule-based systems often miss, reducing false positives while effectively catching new forms of fraud. It will also help institutions scale their fraud monitoring efforts without proportionally increasing operational costs.

· ***Implement Blockchain-Based Smart Contracts for Transaction Validation****: A* blockchain layer should be added to enforce fraud-prevention rules through smart contracts. After an ML model flags a transaction, it can be passed to a smart contract (deployed on a private blockchain like Hyperledger). The contract checks for fraud flags and high-value thresholds (e.g., 50,000), and either approves or blocks the transaction.

This adds a second layer of defense, ensuring even if the AI misses a fraudulent case, blockchain enforces strict rules. Moreover, blockchain ensures tamper-proof, auditable logs, improving transparency and trust among users, banks, and regulators.

· ***Deploy Real-Time Monitoring Dashboards for UPI Transactions:*** Banks and payment gateways should implement interactive dashboards for monitoring UPI transaction behavior in real-time. These dashboards can be powered by tools like Power BI or Tableau, linked to ML models and live databases. They should include KPIs such as number of transactions flagged per hour, peak fraud times, and sender-receiver hotspots. Real-time visibility allows fraud analysts to act promptly, detect systemic issues, and update fraud detection models quickly. It also enables better resource allocation and quicker communication between fraud investigation teams.

· ***Adopt Adaptive Fraud Labeling Using Hybrid Rules + AI Models:*** Instead of relying solely on past data, institutions should adopt adaptive labeling systems combining expert-defined rules with ML insights. The current study defined rules such as odd-hour activity, repeated sender-receiver transfers,

and mismatched UPI handles. These rules can be refined using insights from AI models and continuously updated using feedback from flagged transaction investigations. This hybrid method reduces model bias, captures new fraud patterns early, and ensures that both domain knowledge and data-driven methods inform detection. It also allows institutions to operate fraud detection even when labeled datasets are limited.

· ***Introduce Regulatory Standards for AI and Blockchain in Fintech:*** Regulatory bodies such as RBI and NPCI should develop national standards for using AI and blockchain in UPI and other payment systems. Guidelines should define how fraud detection models are trained, how explainability and fairness are ensured, and how blockchain smart contracts can be legally binding. Institutions can be audited based on their compliance with these standards. Clear regulations will accelerate adoption while minimizing risks such as algorithmic bias or misuse of blockchain. It also promotes consistency across platforms and ensures user rights and privacy are protected in AI-powered systems.

· ***Strengthen Public Awareness and Digital Literacy Campaigns:*** Government and private stakeholders must enhance awareness around UPI fraud tactics and protection strategies.Educational videos, mobile alerts, regional-language campaigns, and fraud simulation exercises can help users recognise phishing, QR scams, and social engineering. These can be integrated into apps or run as national campaigns.

Informed users are the first line of defense against fraud. With better awareness, fewer people will fall for common scams, reducing fraud incidents and improving the effectiveness of technical defenses like AI and blockchain.

· ***Promote Data Sharing Agreements Across Financial Institutions:*** Banks and digital wallets should collaborate to build shared fraud datasets while respecting data privacy norms. Using federated learning or secure multi-party

computation, institutions can train fraud models on collective data without actually sharing sensitive customer information. Regulators can facilitate these collaborations and define data governance frameworks. Access to more diverse and comprehensive data improves the generalisability of ML models, especially in detecting new or cross-platform fraud trends. It helps identify coordinated fraud rings that target multiple platforms in quick succession.

· ***Conduct Regular Model Audits and Ethical Reviews of AI Systems:*** Institutions must regularly audit their ML models for performance, fairness, and compliance with ethical AI standards. An internal or third-party audit team should review feature importance, false positive/negative rates, and whether the model is disproportionately flagging specific user groups. Also, feedback loops should be in place to incorporate user disputes and corrections. Auditing prevents blind trust in ML decisions, maintains accountability, and reduces the risk of algorithmic discrimination. It also ensures that models continue to reflect current fraud behavior and customer diversity, keeping false alarm rates under control.

6.0.4 Reflection

This project involved designing a machine learning-based system to detect fraudulent UPI transactions, complemented by a conceptual simulation of blockchain integration. The research began with data preprocessing, where I cleaned and labeled the dataset using rule-based logic, such as identifying failed high-value transactions, odd-hour activities, and repeated sender-receiver interactions. This step was crucial for preparing the data for supervised learning models. Three classification algorithms including ***Logistic Regression, Support Vector Machine (SVM), and AdaBoost***, were implemented and evaluated. One of the primary challenges in this project was choosing the most suitable machine learning algorithm for detecting fraudulent transactions. While models like Lo-

gistic Regression and SVM achieved high accuracy for legitimate transactions, they failed to detect fraud effectively. This was not due to class imbalance, but rather the complexity of fraud patterns which required more adaptable models. To overcome this, AdaBoost was selected, as it focuses on correcting errors from previous models and can better capture subtle fraud patterns, leading to improved performance. Another challenge involved integrating blockchain, as real-time deployment was not feasible in this academic setting. Instead, a conceptual smart contract was simulated using pseudocode to demonstrate how it could automatically block high-risk transactions identified by the AI model. The development of an architectural diagram helped clarify the flow between machine learning prediction and blockchain validation.

This project strengthened the my skills in data preparation, feature engineering, model evaluation, and visualisation. It also deepened the understanding of how AI and blockchain can work together to build secure digital payment environments. Overall, the project improved technical knowledge, analytical thinking, and the ability to solve real-world problems using innovative technologies.

References

Ahmed, S., 2025. Enhancing Data Security and Transparency: The Role of Blockchain in Decentralized Systems. *International Journal of Advanced Engineering, Management and Science*, *11*(1), p.593258.

Ali, Akhtar, M.W. and Haque, M. (2024). IMPACT OF CONSUMER AWARENESS ON UPI & DIGITAL TRANSACTIONS IN RURAL AND URBAN INDIA AND THE INFLUENCING... *ResearchGate*, [online] pp.2394–7926. Available at: https://www.researchgate.net/publication/379542225_IMPACT_OF_CONSUMER_AWARENESS_ [Accessed 1 Aug. 2025].

Almansoori, M. and Telek, M. (2023). Anomaly Detection using combination of Autoencoder and Isolation Forest. pp.25–30. doi:https://doi.org/10.3311/wins2023-005.

Anil, K. and Misra, A. (2022) Artificial intelligence in Peer-to-peer lending in India: a cross-case analysis. *International Journal of Emerging Markets*, *17*(4), pp.1085-1106.

Axis Bank (2023) 'Blockchain Initiatives'. Available at: https://www.axisbank.com (Accessed: 24 February 2025).

Aynidinova, N. (2025) CROSS-BORDER E-COMMERCE: OPPORTUNITIES AND CHALLENGES. *Journal of science-innovative research in Uzbekistan*, *3*(3), pp.190-195.

Bader-El-Den, M., Teitei, E. and Perry, T., 2018. Biased random forest for dealing with the class imbalance problem. *IEEE transactions on neural networks and learning systems*, *30*(7), pp.2163-2172.

Ballamudi, K.R. (2016). Blockchain as a Type of Distributed Ledger Technology. *Asian Journal of Humanity, Art and Literature*, 3(2), pp.127–136. doi:https://doi.org/10.18034

Bao, Y., Hilary, G. and Ke, B. (2022) Artificial intelligence and fraud detection. *Innovative Technology at the Interface of Finance and Operations: Volume I*, pp.223-247.

Borowiec, Ł., Demidowski, K., Pecka, M. and Jonarska, A. (2023) The analysis of social engineering methods in attacks on authentication systems. *Advances in Web Development Journal*, *1*, pp.83-106.

Cadet, E., Osundare, O.S., Ekpobimi, H. and Weldegeorgise, Y.W. (2024). Comprehensive Framework for Securing Financial Transactions through API Integration in Banking Systems. *ResearchGate*, [online] 20(11), pp.662–672. Available at: https://www.researchgate.net/publication/386148601_Comprehensive_Framework_for_Securing_ [Accessed 1 Aug. 2025].

CNBC TV18 (2024) 'UPI fraud cases surge by 85% in FY24: Key insights and data', CNBC TV18, 24 February. Available at: https://www.cnbctv18.com/business/finance/upi-fraud-cases-rise-85-pc-in-fy24-increase-parliament-reply-data-19514295.htm (Accessed: 24 February 2025).

Dam, D.L. and Deshpande, K. (2021). Unified Payment Interface (UPI) platform: Conniving tool for Social Engineering Attack. *ResearchGate*, [online] (September), pp.17–28. Available at: https://www.researchgate.net/publication/357837725_Unified [Accessed 1 Aug. 2025].

Das, G., Ali, Y.A., Singh, B. and Nag, K. (2025). Digital Forensics in E-Commerce: Investigating Online Payment Fraud and Data Breaches. *International Journal of Innovations in Science Engineering and Management.*, [online] pp.262–268. doi:https://doi.org/10.69968/ijisem.2025v4i1262-268.

Denny, E. and Weckesser, A. (2022) How to do qualitative research? Qualitative Research Methods. *Bjog*, *129*(7), p.1166.

George, A.S., George, A.H., Baskar, T. and Martin, A.G. (2023) An Overview of India's Unified Payments Interface (UPI): Benefits, Challenges, and Opportunities. *Partners Universal International Research Journal*, *2*(1), pp.16-23.

Georgios Charizanos, Haydar Demirhan and Duygu İçen (2024). An online fuzzy fraud detection framework for credit card transactions. *Expert Systems with Applications*, [online] 252, pp.124127–124127. doi: https://doi.org/10.1016/j.eswa.2024.124127.

Green, A., 2025. *AI-Driven Financial Intelligence Systems: A New Era of Risk Detection and Strategic Analysis* (No. ynph2_v1). Center for Open Science.

Gupta, S. and Sisodia, D. (2024). Automated detection of diabetic retinopathy from gray-scale fundus images using GLCM and GLRLM-based textural features—a comparative study. *Elsevier eBooks*, [online] pp.251–259. doi: https://doi.org/10.1016/b978-0-443-15999-2.00011-6.

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S. and Ishfaq, M. (2022) Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, *14*(11), p.341.

ICICI Bank (2023) Annual Report 2023. Available at: https://www.icicibank.com (Accessed: 24 February 2025).

Justus, D., Brennan, J., Bonner, S. and McGough, A.S., 2018, December. Predicting the computational cost of deep learning models. In *2018 IEEE international conference on big data (Big Data)* (pp. 3873-3882). IEEE.

Kagias, P., Cheliatsidou, A., Garefalakis, A., Azibi, J. and Sariannidis, N. (2022) The fraud triangle–an alternative approach. *Journal of Financial Crime*, *29*(3), pp.908-924.

Kanade, V. (2022). *What Is Logistic Regression? Equation, Assumptions, Types, and Best Practices.* [online] Spiceworks. Available at: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-logistic-regression/.

Kenedy, G., Sadiq, B. and Elly, B. (2025). *The Impact of Data Imbalance on*

AI-Based Fraud Detection Models in Financial Institutions: Strategies for Mitigation. [online] Available at: https://www.researchgate.net/publication/390235833_The_Impact_of_Da
Based_Fraud_Detection_Models_in_Financial_Institutions_Strategies_for_Mitigation.

Krause, D. (2025) The Deceptive Allure: Understanding and Combating Cryptocurrency Pig Butchering Scams. *Available at SSRN 5233661*.

Krishna, B., Krishnan, S. and Sebastian, M.P. (2023) Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, *25*(5), pp.1713-1741.

Krishna, B., Krishnan, S. and Sebastian, M.P. (2025) Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. *Information Technology & People*, *38*(2), pp.714-756.

Kukrety, N., Kaushik, P. and Saxena, N. (2023). (PDF) Blockchain Technology in Indian Banking Sector: A Systematic Review Envisaging Application in the Banking Sector. *ResearchGate*. [online] doi:https://doi.org/10.5281//zenodo.8360371.

Melam, N., Reddy , Y.C., Babu, P.N., Ravipati, V.S.P. and Chaitanya, V. (2024). UPI Fraud Detection Using Convolutional Neural Networks(CNN). [online] doi:https://doi.org/10.21203/rs.3.rs-4088962/v1.

Microsoft (2021). *Visual Studio Code*. [online] Visualstudio.com. Available at: https://code.visualstudio.com/api/extension-guides/notebook [Accessed 30 Jul. 2025].

Ministry of Finance. (2025) DFS drives expansion of digital payments in India and abroad. [Online]. Available at: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2
[Accessed On: 11th July 2025].

Mint (2024) 'UPI security protocols to be upgraded', Mint, 10 February. Available at: https://www.livemint.com (Accessed: 24 February 2025).

Najjar, E. and Breesam, A.M. (2024). Supervised Machine Learning a Brief Survey of Approaches. *Al-Iraqia Journal of Scientific Engineering Research*, [online] 2(4). doi:https://doi.org/10.58564/ijser.2.4.2023.121.

Nanda, A.S. (2024). The Future of Cybersecurity in Fintech: Challenges, Trends and Best Practices. *International Journal of Science and Research (IJSR)*, [online] 13(7), pp.1509–1515. doi:https://doi.org/10.21275/sr24717223220.

Nayak, S. and Kalra, J. (2024). *India's Paytm likely to partner with four banks for enabling UPI transactions, sources say.* [online] Reuters. Available at: https://www.reuters.com/business/finance/indias-paytm-likely-partner-with-four-banks-enabling-upi-transactions-sources-2024-02-26 [Accessed 31 Jul. 2025].

Ounacer, S., El Bour, H.A., Oubrahim, Y., Ghoumari, M.Y. and Azzouazi, M., 2018. Using Isolation Forest in anomaly detection: the case of credit card transactions. *Periodicals of Engineering and Natural Sciences*, *6*(2), pp.394-400.

Pamulaparthyvenkata, S., Vishwanath, M., Desani, N.R., Murugesan, P. and Gottipalli, D. (2024). Non Linear-Logistic Regression Analysis for AI-Driven Medicare Fraud Detection. *2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC)*, [online] pp.1–6. doi:https://doi.org/10.11

Polu, O.R., Chamarthi, B., Chowdhury, T., Ushmani, A. and Prova, I. (2025). *Graph Neural Networks for Fraud Detection: Modeling Financial Transaction Networks at Scale.* [online] doi:https://doi.org/10.13140/RG.2.2.16907.81446.

Potla, R.T. (2023) AI in fraud detection: Leveraging real-time machine learning for financial security. *Journal of Artificial Intelligence Research and Applications*, *3*(2), pp.534-549.

Ramachandran, K. (2018). UNIFIED PAYMENTS INTERFACE (UPI) - TRANSFORMATION OF DIGITAL PAYMENT SYSTEMS IN INDIA. [online] 5(4), pp.42–48. Available at: https://www.researchgate.net/publication/381796530_UNIFIED_PAY TRANSFORMATION_OF_DIGITAL_PAYMENT_SYSTEMS_IN_INDIA.

Rawat, V., Toppo, N.N., Singh, N. and Joshi, A. (2021). Overview Of Blockchain Technology And Its Applications In Different Disciplines. [online] 20(3).

Reserve Bank of India (RBI) (2023) Annual Report 2022-23. Available at: https://www.rbi.org.in (Accessed: 24 February 2025).

Richardson, E., Trevizani, R., Greenbaum, J.A., Carter, H., Nielsen, M. and Peters, B. (2024). The receiver operating characteristic curve accurately assesses imbalanced datasets. *Patterns*, [online] 5(6), pp.100994–100994. doi:https://doi.org/10.1016/j.patte

Rohit Shewale (2025). *UPI Statistics (2016 to 2025 Data) - GrabOn*. [online] GrabOn's Indulge - Online Shopping Tips, Buying Guide, Savings. Available at: https://www.grabon.in/indulge/tech/upi-statistics/ [Accessed 31 Jul. 2025].

Sarker, I.H. (2021) Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), p.160.

Saunders, M., Lewis, P. and Thornhill, A. (2019) Research Methods for Business Students. 8th edn. Harlow: Pearson Education Limited.

Schuetz, S. and Venkatesh, V. (2020) Blockchain, adoption, and financial inclusion in India: Research opportunities. *International journal of information management*, *52*, p.101936.

Sedlmeir, J., Lautenschlager, J., Fridgen, G. and Urbach, N. (2022) The transparency challenge of blockchain in organizations. *Electronic Markets*, *32*(3), pp.1779-1794.

Sharma, H., Sharma, K. and Kumar, R., 2025. UPI Fraud Detection System. *International Journal of Innovative Science and Research Technology*, *10*(6), pp.278-284.

Shukla, P. (2025). *1 in 5 UPI users faced fraud; 51% victims didn't report, reveals survey*. [online] @bsindia. Available at: https://www.business-standard.com/finance/news/up transaction-fraud-india-survey-one-in-five-users-hit-localcircles-125062601141_1.html

[Accessed 31 Jul. 2025].

Singh, S., Singh, H., Bueno, G., Deniz, O., Singh, S., Monga, H., P.N. Hrisheekesha and Pedraza, A. (2023). A review of image fusion: Methods, applications and performance metrics. *Digital Signal Processing*, [online] 137, pp.104020–104020. doi:https://doi.org/10.1016/j.dsp.2023.104020.

Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, [online] 14(2), pp.117–117. doi:https://doi.org/10.3390/info14020117.

Uche, D.B., Osuagwu, O.B., Nwosu, S.N. and Otika, U.S. (2021) Integrating trust into technology acceptance model (TAM), the conceptual framework for e-payment platform acceptance. *British Journal of Management and Marketing Studies*, *4*(4), pp.34-56.

Veeravalli, S.D. (2023) Proactive Threat Detection in CRM: Applying Salesforce Einstein AI and Event Monitoring to anomaly detection and fraud prevention. *MACHINE LEARNING (ISCSITR-IJSRAIML)*, *4*(1), pp.16-35.

Vijai, C. (2019). ARTIFICIAL INTELLIGENCE IN INDIAN BANKING SECTOR: CHALLENGES AND OPPORTUNITIES. *International Journal of Advanced Research*, [online] 7(4), pp.1581–1587. doi:https://doi.org/10.21474/ijar01/8987.

Wadkar, P. and Mundhe, S.D. (2024). Cyber Security Challenges in UPI Payment frauds in India. [online] II(13), p.35. Available at: https://www.researchgate.net/publication/

World Economic Forum (2023) Blockchain in Financial Services. Available at: https://www.weforum.org (Accessed: 24 February 2025).

Zafer, T. and Ali, K. (2025). Blockchain Technology and AI: Transforming Fraud Detection and Data Protection in Finance. *ResearchGate*. [online] doi:https://doi.org/10.13140/RG.2.2.14452.87681.