FRAUD TRANSACTION ALERT AND FUNDS MANAGEMENT

Ketaki Ghawali[1], Aryan Mane[2], Tanuj Merchant[3]

Assistant Professor[1], Student[2], Student[2]

Department of Information Technology and Data Science,

Vidyalankar School of Information Technology,Mumbai, India.

Abstract:

In the dynamic realm of digital payments, the persistent threat of transaction fraud and financial mismanagement necessitates innovative solutions. This research paper explores the efficacy of the Fraud Transaction Alert and Funds Management Application, a sophisticated tool designed to counter the evolving tactics of fraudsters. Utilizing advanced algorithms, the application scrutinizes end-users' transaction histories to assess the probability of fraudulent or unintentional transactions, aiming to mitigate significant financial losses.

Against the backdrop of prevalent digital payment methods like UPIs and card payments, the paper addresses the need for effective daily expense monitoring to curb unnecessary spending. The application takes a proactive stance, providing users with comprehensive records of daily expenditures and personalized spending limits set within specific timeframes. This approach facilitates the alignment of spending habits with savings goals, fostering enhanced financial control and informed decision-making.

The research delves into the real-time insights offered by the application into transaction data and financial behavior. Beyond safeguarding againstpotential fraud, the application actively promotes responsible spending, contributing to bolstering financial security in our increasingly digital and interconnected world. Positioned as a beacon of technological innovation, the Fraud Transaction Alert and Funds Management Application guide users towards a future marked by financial stability and peace of mind in their digital financial endeavors.

I. INTRODUCTION

As digital payment systems rapidly advance, ushering in unprecedented convenience, they concurrently present challenges such as transaction fraud and financial mismanagement. This research paper thoroughly examines the Fraud Transaction Alert and Funds Management Application a sophisticated response to the dynamic tactics of fraudsters in the evolving digital payment environment.

II. BACKGROUND

The surge in digital transactions, particularly through UPIs and card payments, has posed challenges in monitoring daily expenses, leading to unplanned spending. The Fraud Transaction Alert and Funds Management Application employs advanced algorithms to analyze users' transaction history, aiming to prevent financial losses by assessing the likelihood of fraudulent or unintentional transactions. Additionally, the application promotes financial discipline through personalized spending limits and comprehensive daily expenditure records.

III. OBJECTIVES

This paper explores the distinct objectives of the Fraud Transaction Alert and Funds Management Application in the crowded landscape of financial management applications. From real-time alert systems and behavioural analysis to personalized spending limits and in-app scam reporting, the application's objectives encompass a broad spectrum. Committed to GDPR compliance, user data privacy and security are integral to its functionality.

In terms of scope, the Fraud Transaction Alert and Funds Management Application comprehensively addresses transaction fraud and financial mismanagement in the digital payment landscape. Utilizing advanced algorithms and machine learning, it aims to set new standards in real-time tracking and analysis compared to existing financial management apps. Key features such as alert systems, behavioural analysis, personalized spending limits, and scam reporting contribute to a safer and more secure financial environment. Monthly financial reports provide a holistic approach, empowering users in the digital age.

IV. HOW SCAMMERS OPERATE:

Scammers adeptly exploit various tactics to deceive individuals within the UPI framework. One prevalent method involves adopting a false preteen of authority, wherein scammers assume roles as government officials, police officers, or tech support representatives. By alleging the victim's involvement in financial wrongdoing or legal offenses, they coerce individuals into making payments through gift cards, citing the need to evade imminent arrest or legal repercussions.

Another deceptive tactic involves scammers masquerading as charitable organizations, appealing to the generosity of potential donors. In soliciting modest gift card donations, they aim to obtain the victim's UPI PIN and bank account details. Subsequently, this sensitive information is leveraged to transfer funds from the victim's account to the scammer's own, under the guise of charitable contributions.

Online marketplace scams present yet another avenue for scammers to exploit unsuspecting individuals. Operating within online marketplaces or classified ads, scammers entice victims with heavily discounted products, requesting payment in gift cards while promising additional cashback rewards. However, once the payment is made, the scammer vanishes, leaving victims without the promised item or any cashback.

V. IMPACT ON FINANCIAL DISCIPLINE

Individuals face a widespread challenge concerning the management of their finances. While the convenience of online transactions has undeniably streamlined spending, it has also introduced complexities. Many individuals, though not falling victim to fraudulent activities, encounter difficulties in establishing precise spending boundaries. This tendency towards overspending on non-essential items gradually depletes savings, emphasizing the urgent need for enhanced financial discipline.

The accessibility of online payment methods often acts as a catalyst for impulsive purchases, necessitating the development of practical tools and strategies to foster more prudent financial management. As individuals navigate the digital landscape, the impact of UPI scams [1] on financial discipline becomes a crucial focal point for research and the development of countermeasures to empower users in safeguarding their financial well-being.

VI. METHODOLOGICAL INNOVATION

In the context of existing literature and prevalent discussions surrounding UPI scams, this research contributes novel insights and strategies in understanding and addressing the challenges posed by deceptive practices within the Unified Payment Interface. The elucidation of scammers' tactics [2], encompassing false pretences of authority, deceptive charity schemes, and online marketplace scams, serves as a foundational framework for comprehending the intricacies of fraudulent activities within the digital payment landscape.

Building upon the existing discourse, our research endeavours to expand the conceptualization of UPI scams by presenting a comprehensive analysis of scammers' methodologies. By delineating the multifaceted techniques employed, including the coercive tactics of assuming authoritative roles, masquerading as charitable entities, and exploiting online marketplaces, this study seeks to offer a nuanced understanding of the evolving landscape of financial deceit in the digital realm.

Furthermore, our research extends beyond the mere elucidation of scammer tactics [3] to explore the consequential impact on financial discipline. In recognizing the broader implications for individuals in the contemporary digital landscape, this study distinguishes itself by delving into the intricate dynamics of financial management. The identified challenges, particularly in the context of overspending on non-essential items and the gradual depletion of savings, underscore the critical need for enhanced financial discipline—a fact that, to our knowledge, has received limited attention in the current literature.

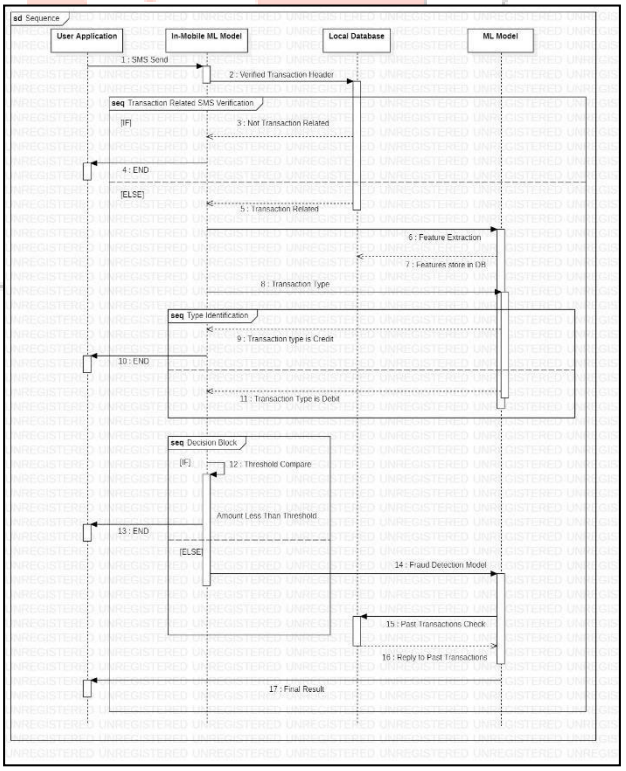

Figure 1: Sequence Chart

Additionally, our research deviates from the prevailing discussions by proposing the development of practical tools and strategies to foster more prudent

financial management. In acknowledging the catalysing effect of online payment methods on impulsive purchases, we propose avenues for the creation of innovative solutions that align with the evolving nature of financial transactions. This departure from conventional approaches emphasizes our commitment to not only diagnosing existing challenges but also proactively contributing to the development of tangible and effective countermeasures.

VII. SYSTEM DESIGN

The system comprises several interconnected modules, each serving a distinct function to enhance functionality and security. The "Profile Module" manages user profiles and authentication, the "User Login Module" adds post-login security layers, and the "SMS Module" categorizes messages. The "Feature Extraction Module" streamlines data extraction, while the "Vikhed Module" optimizes system performance based on SMS details. The "Reports Module" facilitates user reporting, and the "Detection Model Module" automates fraud detection. Lastly, the "NLP Module" processes SMS content for meaningful analysis [4] . Together, these modules form a robust framework addressing diverse challenges in user interaction and data management. The detailed description of every module is as follows:

- **Profile Module**

The "Profile" module serves as a pivotal component within the software system, overseeing the management of user profiles. This module encompasses essential attributes including "profile_id," phone number, password, first name, and last name. Its functionalities, such as "update_info" and "create_account," empower users to both modify their profile details and establish new profiles *Table 1*. This module plays a vital role in facilitating user authentication, personalization, and efficient data management. In the context of a research paper, the "Profile" module emerges as a critical element that contributes to the overall functionality and security of the software system, warranting in-depth investigation and analysis.

Table 1: Profile Schema

Name	Constraints	Data Type
profile_id	Primary Key, Unique	Integer
phone_number	Foreign Key	integer
ac_number	Unique	integer
email	Unique	varchar(255)
first_name	None	varchar(255)
last_name	None	varchar(255)
address	None	Varchar(255)

- **User Login Module**

Within the scope of our research paper, the "user_login" module takes center stage as a fundamental element responsible for user authentication within the software system. It leverages key attributes such as profile ID, phone number, and password to uniquely identify and authenticate users during the login process. Operations like "validate_user" play a pivotal role in guaranteeing secure access, while the inclusion of features such as "Unlock_App" *Table 2:* User Schema with a security pin adds an additional layer of post-login security. This module assumes a critical role in safeguarding user data and interactions, thereby ensuring controlled and secure access within the application. As we delve into our research, a comprehensive examination of the "user_login" module becomes imperative, shedding light on its mechanisms and contributions to the overall security framework of the software system.

Table 2: User Schema

Name	Constraints	Data Type
phone_number	Primary Key, Unique	integer
password	Unique	varchar(8,16)
email	Foreign Key	varchar(255)
first_name	None	varchar(255)
last_name	None	varchar(255)
security_pin	None	integer

- **SMS Module**

The "sms" module emerges as a crucial component responsible for handling text messages within the software system. This module captures essential information, including sender details, timestamp, and message headers *[Table 3]*. The "validate_header" operation within this module plays a significant role in discerning between regular communication and potentially important transactions. This distinction enhances the overall management of messages and contributes to an improved user experience. The "sms" module is integral to the systematic processing and categorization of text messages, playing a pivotal role in fostering effective communication within the broader system. In our research, a detailed exploration of the

functionalities and impact of the "sms" module becomes essential, shedding light on its contributions to the overall efficiency and user satisfaction within the software ecosystem.

Table 3: SMS Schema

Name	Constraints	Data Type
sender_id	Primary Key, Unique	integer
sms_header	None	varchar(255)
sms_body	None	String
sms_time	None	Datetime

- **feature_extraction Module**

The "feature_extraction" module acts as a vital interface within the NLP framework, specifically designed for the segmentation of SMS message headers and bodies. *[Table 4]* This segmentation is of paramount importance in effectively processing and extracting pertinent information from text messages. The encapsulation of these operations within the module serves to optimize data preprocessing tasks in the NLP system, ultimately augmenting its efficiency in handling SMS data.

Table 4: Feature Schema

Name	Constraints	Data Type
transaction_msg	None	Object

- **Vikhed Module**

The "Vikhed" module functions as a pivotal decision-making component within the system, evaluating various SMS details, including account numbers, dates, amounts, and types *[Table 5]*. Its primary role involves determining the activation of a detection model based on this information, with the overarching goal of optimizing system performance and minimizing false alarms. Through its operations, this module significantly improves the system's capacity to process SMS data with efficacy, ensuring efficient resource allocation.

Table 5: Vikhed Schema

Name	Constraints	Data Type
ac_number	Foreign Key	integer
sms_date	None	datetime
transaction_amt	None	Integer
transactio_type	None	String

- **Reports Module**

The "Reports" module serves as a user-friendly interface for reporting fraudulent transactions, enabling users to submit details of potential scams. This module initiates requests to the server to promptly notify authorities, thereby streamlining the reporting process and expediting the handling of potential fraud incidents. *[*Table *6]* By providing a seamless mechanism for users to contribute to the reporting and resolution of fraudulent activities, this component plays a crucial role in promoting user security and fostering collaboration with relevant authorities.

Table 6: Report Schema

Name	Constraints	Data Type
report_id	Primary Key,	Integer
profile_id	Foreign Key	Integer
sender_id	Foreign Key	integer
title	None	Varchar(255)
description	None	Varchar(255)
report_image	None	Blob
report_count	None	Integer
report_time	None	Datetime

- **Detection Model**

The "Detection Model" module serves as a critical component within the system, leveraging information from the "Vikhed" and "NLP" modules. By employing advanced machine learning techniques [5], it systematically evaluates the likelihood of fraudulent transactions. This module plays a pivotal role in automating the fraud detection process, generating probabilistic assessments of potential scams based on the information *[Table 7]* at hand. Through its capabilities, the module significantly contributes to enhancing the overall security and efficiency of the system in identifying and addressing potential instances of fraud.

Table 7: Detection Module Schema

Name	Constraints	Data Type
nlp_obj	None	object
sms_amount	None	integer
nlp_date	None	Integer
records	None	list

- **NLP Module**

The "NLP" (Natural Language Processing) module assumes a pivotal role within the system, concentrating on the processing of the body of SMS messages. Employing a diverse range of sophisticated NLP techniques, its primary purpose is to meticulously extract relevant information *[Table 8]* and details embedded within the unstructured text content of the messages. By undertaking this intricate task, the module serves as a transformative agent, converting raw and unorganized textual data into a structured and meaningful format.

This conversion process is instrumental in facilitating subsequent stages of analysis and decision-making within the system. The "NLP" module acts as a linguistic interpreter, decoding the intricacies of human language present in SMS messages and distilling them into a comprehensible and analyzable form. Its capabilities empower the system to derive valuable insights, enabling more informed and contextually aware decisions.

In essence, the "NLP" module acts as a bridge between the inherent complexity of human language in SMS messages and the need for structured information within the system. Through its advanced processing techniques, it not only enhances the system's ability to interpret and understand textual data but also plays a crucial role in enabling downstream components to effectively utilize the extracted information for improved system performance and decision-making.

Table 8: NLP Schema

Name	Constraints	Data Type
transaction_sms	none	object
transaction_amt	None	integer
transaction_type	none	String
sms_date	None	datetime
ac_number	None	Integer
reference_no	None	Varchar

VIII. PROTOTYPING

In the prototype phase, focus was on the development and validation of a transaction verification model, comprising key components such as the user application, in-mobile machine learning (ML) model, local database, and a cloud-hosted ML model. The process initiates with SMS verification, where the user application sends an SMS for transaction confirmation, and the user responds with a confirmation code. The in-mobile ML model then assesses whether the received SMS is transaction-related, aborting non-relevant transactions and allowing the continuation of relevant ones.

Following this, the in-mobile ML model engages in feature extraction, parsing essential transaction details like sender, receiver, amount, date, and time. These features are stored locally for further processing. Subsequently, the model identifies the type of transaction (credit or debit) to determine the appropriate threshold for fraud detection. The in-mobile ML model then compares the transaction amount with the predefined threshold, categorizing transactions as normal or suspicious based on the outcome.

Upon suspicion, the prototype invokes a fraud detection model hosted on a cloud server. This ML model employs the extracted features and the user's transaction history to ascertain the fraudulent nature of the transaction. The in-mobile ML model, acting as an intermediary, receives the final result from the cloud-hosted model and notifies the user, accordingly, completing the transaction verification process.

The prototype phase demonstrates the viability and efficiency of our proposed model in real-world scenarios, leveraging a combination of in-mobile and cloud-based ML capabilities *[Figure 2]*. Through this phase, we also gain insights into potential challenges and limitations, including network latency, data privacy concerns, and the overall accuracy of the model.

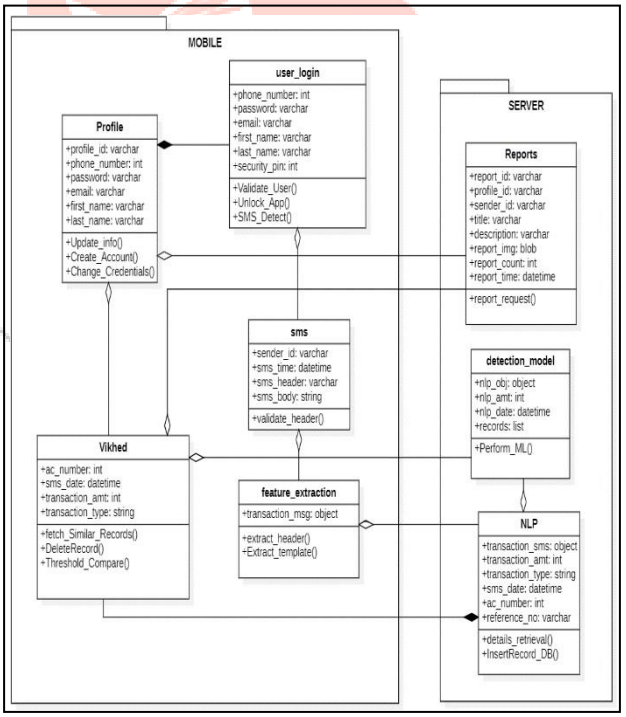

Figure 2: Class Diagram

Moving beyond the prototype, model's accuracy and performance become paramount considerations. Evaluating the fraud detection model solely based on accuracy is insufficient due to the imbalanced nature of fraud detection as a classification problem. Precision, recall, and F1-score emerge as critical metrics, measuring

the trade-off between false positives and false negatives. Acknowledging the significance of these metrics, proposed model, addresses challenges through natural language processing techniques for handling financial text information, a unique keywords loss function for enhanced performance, and a model distillation technique to optimize size and complexity.

IX. CONCLUSION

In light of the prevailing literature on UPI scams, this research advances the current discourse by introducing a novel conceptualization that addresses the limitations and challenges encountered by prior models. Unlike existing frameworks that predominantly focus on elucidating the tactics employed by scammers, our study delves into a more comprehensive analysis, distinguishing itself by examining the nuanced dynamics of financial deceit within the Unified Payment Interface. Notably, the identified challenges extend beyond the realm of scammer tactics to encompass the impact on individual financial discipline—a fact that has hitherto received limited scholarly attention. By meticulously outlining the deceptive methods employed, such as false pretences of authority, deceptive charity schemes, and online marketplace scams, our research not only contributes a nuanced understanding of the evolving landscape of financial fraud but also introduces an innovative perspective on the consequential implications for users.

Moreover, our departure from conventional approaches is evident in the proposed development of practical tools and strategies aimed at fostering more prudent financial management, thereby offering a proactive and forward-looking contribution to the field. This model, forged through meticulous research, signifies a substantive step towards addressing the complexities inherent in UPI scams and charting a course for more effective and resilient digital financial ecosystems.

X. REFERENCES

[1] G. J. Priya and S. Saradha, "Fraud Detection and Prevention Using Machine Learning Algorithms: A Review," 2021 7th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 2021, pp. 564-568, doi: 10.1109/ICEES51510.2021.9383631.

[2] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga and N. Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2019, pp. 488-493, doi: 10.1109/CONFLUENCE.2019.8776942.

[3] Seeja, K.R. and Masoumeh Zareapoor.,"Fraud Miner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining"., The Scientific World Journal, Hindawai Publishing Corporation, Volume 2014,Article ID 252797,pp. 1-10

[4] Y. R. M. R, K. A, R. D, R. Reshma, D. R. Santhosh and N. Mekala, "An Analytical Approach to Fraudulent Credit Card Transaction Detection using Various Machine Learning Algorithms," 2023 Second International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2023, pp. 1400-1404, doi: 10.1109/ICEARS56392.2023.10085157.

[5] Á. Gómez, L. Maimó, A. Celdrán, & F. Clemente, "An interpretable semi-supervised system for detecting cyberattacks using anomaly detection in industrial scenarios", IET Information Security, vol. 17, no. 4, p. 553-566, 2023.

[6] https://secureframe.com/hub/gdpr/what-is-gdpr-compliance

[7] https://www.weforum.org/agenda/2023/06/india-unified-payment-interface-impact/