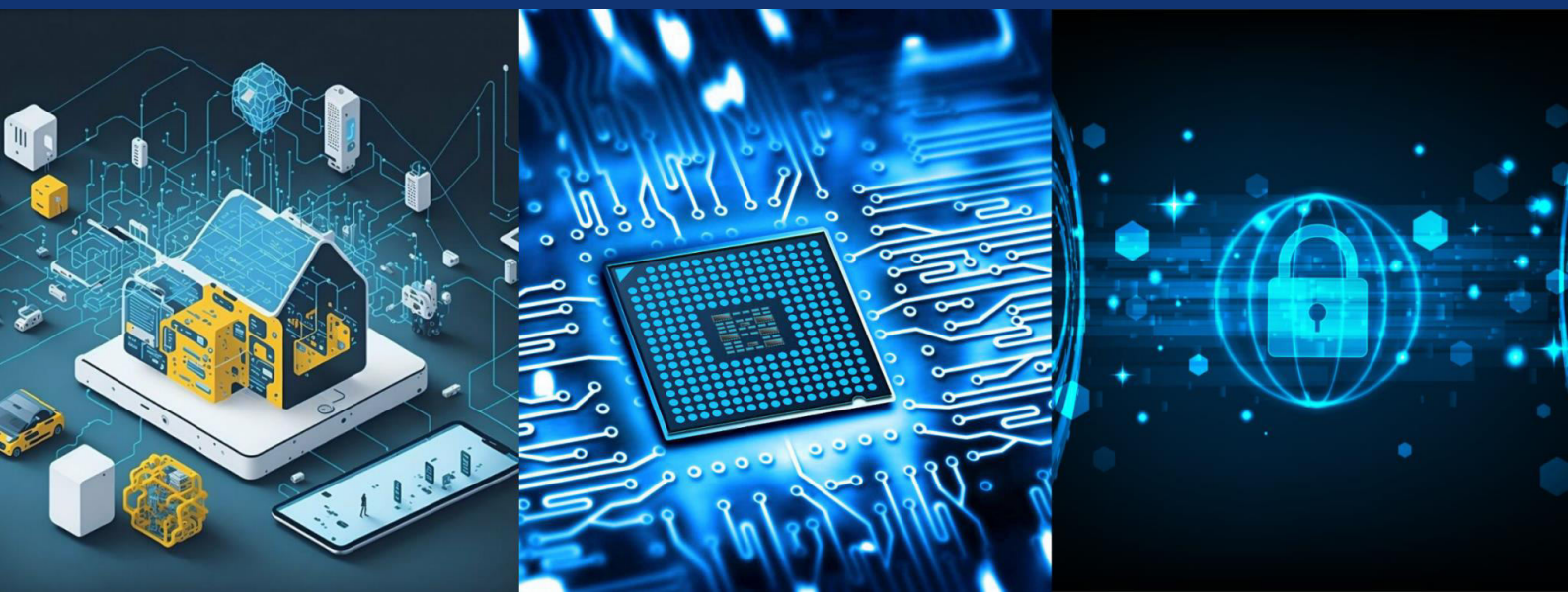
IJIRCCE

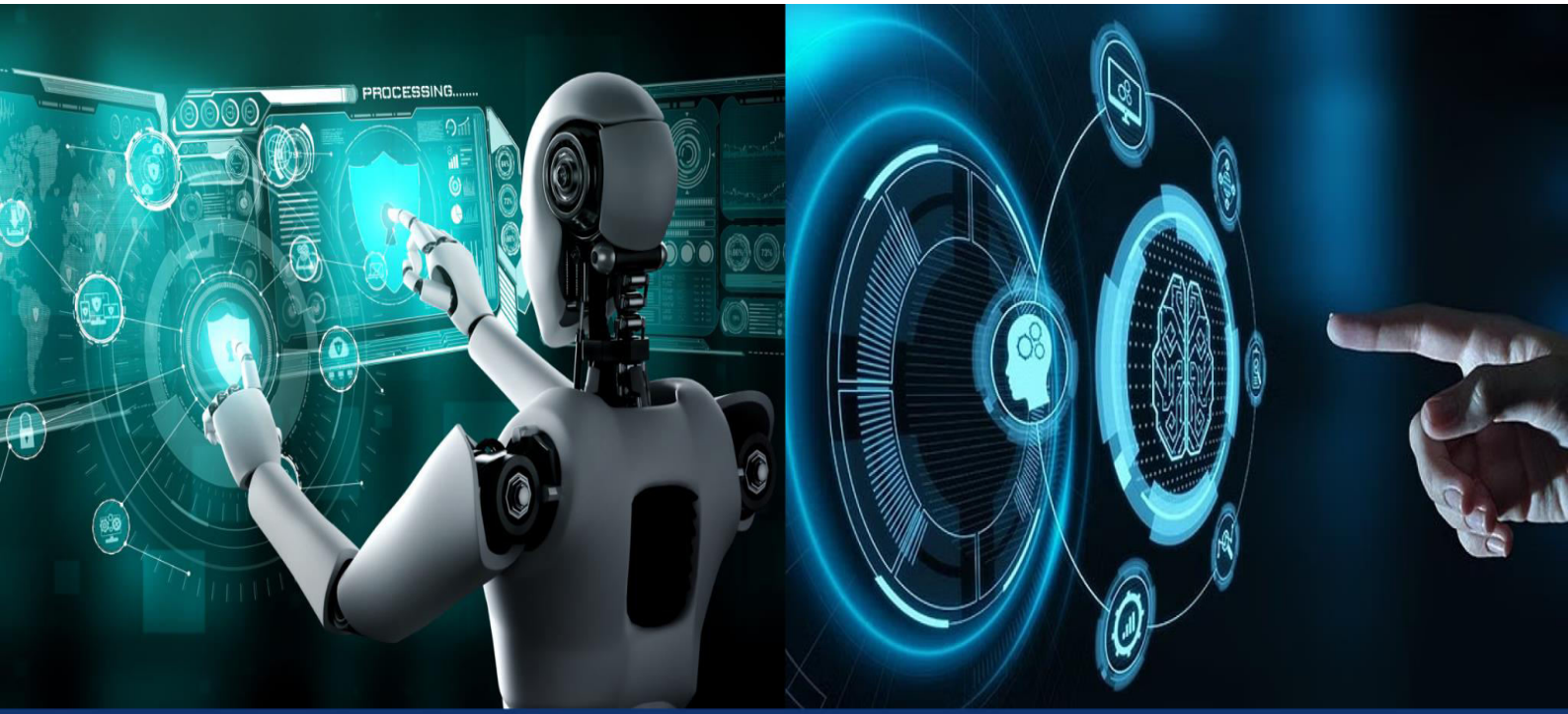
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405079

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Financial Fraud Detection Application

Purva Yogesh Pawar[1], Shruti Vaibhav Kharche[2], Rita Sanjay Mahajan[3], Prof. Vikas Narkhede[4]

UG Student, Dept. of Computer Engineering, KCE's College of Engineering and Management, Jalgaon, India[1-3]

Assistant Professor, Dept. of Computer Engineering, KCE's College of Engineering and Management, Jalgaon, India[4]

ABSTRACT: Financial fraud poses a persistent and escalating threat to global economic stability, resulting in substantial annual losses for individuals and financial institutions alike. Traditional, manual, and rules-based detection methods are often inefficient, time-consuming, and incapable of adapting to the increasing sophistication and volume of modern fraudulent activities. This study explores the application and effectiveness of advanced data analytics and machine learning (ML) techniques in automating and enhancing the accuracy of financial fraud detection systems across various domains, including credit card transactions, insurance claims, and banking operations. We analyze several supervised and unsupervised ML algorithms, such as Logistic Regression, Random Forests, Support Vector Machines (SVM), Artificial Neural Networks (ANN), and advanced deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks.

KEYWORDS: Financial Fraud , Fraud Detection, Machine Learning (ML) , Data Mining , Anomaly Detection , Financial Transactions , Predictive Modeling ,Artificial Intelligence (AI)

I. INTRODUCTION

Financial Fraud Detection is the process for not totally ending up the issue taking up the small step towards the security and protection . Day by Day we are doing transactions through many purposes and mediums and the user don't have an idea about the tracks set behind some frauds which can totally blank our bank accounts . Here this issue is happening even when we attain any calls , otp given to fraudulent person , Bank online system(even the banks are hacked), and so on . Before sharing any information related to our bank accounts is very important because even the people doing the frauds also contact you for asking your details of banks which will blank your bank totally

II. RESEARCH METHODOLOGY

The methodology includes the plan and procedure of recent study and realtime fraud detections It mainly gives the alert before paying to any number or upi . Design framework includes the database shareprefrences and the modules in the Financial Frayd Detection Applicatioin . The details are as follows:

2.1. Scope of the Study

This study mainly looks after on the design, development and implementation of a Financial Fraud detection Mobile Application. intended for use by the general public, emergency responders and disaster management authorities. However, it's helps the user in two ways but we need the helpers to I this application as the fraud taken place with the person should register their fraud in detail to help others and secondly it helps in preventing the fraud by checking it before paying to any doubtfull or any id to prevent the fraud .we are trying not to totally finish the fraud but the small step towards preventing the fraud.Its the user friendly application which will be easy to use for each user .The study on this application helped us to acchive the importance of preventing the fraud and removing the fear of financial frauds through online mediums .

However this was the greatest opportunity to seek in deep on this issue and discover the root cause of financial frauds happening throughout the world and it aims to solve the issue with the easy way and simple application processes .

2.2. Data Sources

The app pulls information from a variety of trustworthy sources to keep fraud alerts accurate and up-to-date. The registered data of the user with whom the fraud has taken place need to be stored properly without any loss if the information is lossed the application may lead to untrusted medium.The main aim is to gain the trust of the fraud checker before he is paying . The data was on the basic level so we have stored it through the sharedprefrences which

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405079

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

helps in storing the data permanently in the application.The proper output is expected after saving the data in the application . We refer to the proper and smooth working of the application by taking the input from the user in the registration of fraud .

2.3. Theoretical framework

The study is grounded in financial fraud principles, mobile technology and information dissemination theory. It follows the Financial cycle, which includes key phases: Fraud happened, registered, checked and decision making . This framework highlights the importance of timely information, effective communication and user behavior during Fraud handling . At its core, the framework includes concepts like real-time notification systems and user interaction models, all aimed at delivering crucial alerts and safety instructions to help reduce the impact of frauds taking place. Additionally, it incorporates human-centered design principles to ensure the app is easy to use, even in stressful situations. Communication theory underscores the need for clear, concise and timely alerts to minimize confusion among users. Risk communication models further enhance the effectiveness of the warning messages the app provides.

2.4. System Model Used

The system model is built around three key components: data sources, an application server and a mobile user interface. Authorized APIs provide crucial data that the server collects and processes. The server then analyzes this information to generate relevant alerts based on the user's registered fraud . These alerts are sent out via alert notifications in the mobile app who is checkig it . The user interface is designed to be user-friendly, allowing individuals to view alerts, access safety guidelines, and share their location with emergency contacts. To ensure quick communication, reliability and the ability to scale during emergencies, the system includes security features like user authentication and data encryption to protect sensitive information. It's also built to handle a large number of users.

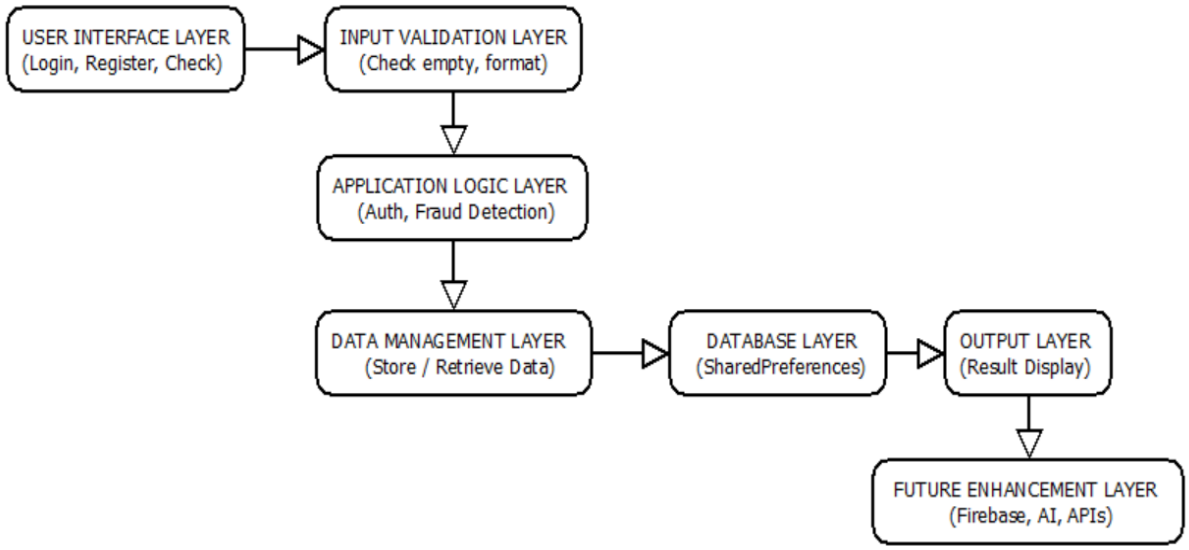


Figure 1: Architecture Diagram

III. RESULTS AND DISCUSSION

System Implementation Results

The main purpose of system design is to plan the overall working of the application. It includes designing the user interface, database structure, and flow of data between different parts of the system. In our project, it shows how a user will register fraud details, how that data will be stored, and how another user can search and check those details before making a payment. The system is designed to help users identify and prevent financial fraud. Nowadays, many frauds happen through UPI IDs, phone numbers, and online transactions.This phase also helps in organizing different components of the system such as frontend (user screens), backend (logic), and database (data storage). It ensures that all parts are properly connected and work smoothly together.System design makes the development process easier because everything is planned in advance. It reduces errors, improves performance, and helps in building a clear and user-friendly application. Validation is an important part of input design. It ensures that the data entered by the user is

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

correct and complete before processing. In this application, basic validation is applied such as checking whether the fields are empty or not. For example, if the user tries to register fraud without entering a phone number or UPI ID, the system shows a message asking the user to fill the required field.Similarly, during login and sign up, the system checks that all required fields are filled before proceeding. This helps in avoiding errors and ensures that only valid data is stored in the system. Validation is an important part of input design. It ensures that the data entered by the user is correct and complete before processing. In this application, basic validation is applied such as checking whether the fields are empty or not. For example, if the user tries to register fraud without entering a phone number or UPI ID, the system shows a message asking the user to fill the required field.Similarly, during login and sign up, the system checks that all required fields are filled before proceeding. This helps in avoiding errors and ensures that only valid data is stored in the system. output design focuses on how the system shows results to the user after processing the data. The main aim is to present the output in a clear and understandable way so that the user can easily take decisions. designed to give instant and meaningful feedback to the user. In future, the system can be improved to include detailed reports such as fraud history, list of reported frauds, and analytics.

The application provides outputs in the form of simple messages and screen responses. When a user performs an action like login, registering fraud, or checking fraud, the system immediately displays a result. For example, during login, the system shows messages like “Login Successful” or “Login Failed” based on the entered details. Similarly, when a user registers a fraud, aconfirmation message like “Fraud Registered Successfully” is displayed.The most impor tant output of the system is during fraud checking. When a user enters a phone number or UPI ID, the system compares it with stored data and shows the result: If the num ber is found in the database, it shows “Fraud Detected” and If not found, it shows “Safe Number” These outputs are displayed using simple notifications (Toast messages) so that the user can quickly understand the result without any confusion. In this project, detailed reports are not generated etc

IV. ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who contributed to the successful completion of this project titled **“Financial Fraud Detecytion System.”** I am deeply thankful to my project guide for their valuable guidance, continuous support and constructive suggestions throughout the development of this project. Their expertise and encouragement played a crucial role in shaping this work. I would also like to thank the Head of the Department and faculty members for providing the necessary resources and a supportive learning environment. I am grateful to my institution for offering the facilities and opportunities required to carry out this project effectively. I extend my sincere thanks to my friends and classmates for their cooperation, ideas and motivation during the project work. Lastly, I express my heartfelt gratitude to my parents and family members for their constant support and encouragement throughout my academic journey.

V. CONCLUSION AND FUTURE SCOPE

In The Financial Fraud Detection application was successfully developed to provide a simple and effective way to identify and prevent financial fraud. The system allows users to register fraud details such as phone numbers or UPI IDs and enables other users to check this information before making transactions. All the modules like login, sign up, fraud registration, and fraud checking work together smoothly to provide accurate and quick results. The application is user-friendly, easy to operate, and gives fast responses since it uses local data storage. It helps users make safer decisions and reduces the chances of falling into fraud. Overall, the project meets its main objectives and demonstrates a practical solution for fraud detection. In the future, it can be improved by adding a larger database, online connectivity, and advanced fraud detection techniques to make it more powerful and reliable

The future scope of the application can be further enhanced by integrating advanced technologies such as artificial intelligence and machine learning for improved fraud detecton and risk analysis. Multilingual support can be added to make the application accessible to a wider population. The system can be expanded to support wearable devices for continuous monitoring. Social media integration may help in faster information dissemination. Regular system upgrades and feature enhancements can further improve reliability and effectiveness. In the future, the application can evolve into a government support for getting this applicatioin worlwide and motivate everyone to help and get help for our security.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

[1] A. Srivastava, A. Kundu, S. Sural, A. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Com puting, Vol. 5, Issue 1, ISSN: 1545-5971, pp. 37-48, Jan 2008.
[2] I. Witten, E. Frank, M. Hall, "Data Mining Techniques" in Data Mining: Practical Machine Learning Tools and Techniques, 3rd Edition, Volume 1. Morgan Kaufmann, USA: Elsevier, 2011, pp. 45-60.
[3] V. Bhusari, S. Patil, "Study of Machine Learning Algorithms for Financial Fraud De tection", International Journal of Computer Applications, Vol. 182, Issue 45, ISSN: 0975-8887, pp. 20-25, Mar 2019. [4] A. Srivastava, A. Kundu, S. Sural, A. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transactions on Dependable and Secure Com puting, Vol. 5, Issue 1, ISSN: 1545-5971, pp. 37-48, Jan 2008.
[5] I. H. Witten, E. Frank, M. A. Hall, "Data Mining Techniques" in Data Mining: Practical Machine Learning Tools and Techniques, 3rd Edition, Volume 1. Morgan Kaufmann, USA: Elsevier, 2011, pp. 45-60.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details