WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhanced Fraud Call Detection through Cybersecurity and Machine Learning Integration.

Ganapathiraju Aneesha Varma, Dannana Hemanth Kumar, Gera Ankitha, Gorle Rahul, Gunapate Bhanu Varma, Annepu Bharath Kumar

Department of Computer Science and Engineering, GMR Institute of Technology, Vizianagaram, 532127, India

ABSTRACT:

Fraud call detection is an essential aspect of securing communication networks and protecting Users from malicious activities. The Combination of cybersecurity techniques and machine learning (ML) provides a powerful way to improve fraud detection. By adding ML algorithms, like decision trees, support vector machines, and neural networks, including traditional cybersecurity protocols, systems can effectively detect and reduce fraud relevant activities in real-time. These ML models can analyze patterns, behaviors, and anomalies for incoming calls, including call metadata, voice features, and interaction history to difference between genuine and fraudulent activities. The existing model has an accuracy of 90% which will be improved by 3 to 5% or more in our model by advanced techniques and optimizations like hybrid algorithm approaches, feature engineering and deep learning models.

KEYWORDS: Fraud Call Detection, Cyber Security, Machine Learning, Call Records, Real Time Detection, Feature Extraction, Decision Trees, Support Vector Machines, Anomaly Detection, Pattern Recognition.

INTRODUCTION:

Fraudulent phone calls have emerged as a serious threat to individuals, businesses, and financial institutions worldwide. Scammers use deceptive tactics such as caller ID spoofing, robocalls, phishing attempts, and social engineering to manipulate users into revealing sensitive information, making payments, or falling victim to identity theft. The increasing sophistication of these attacks has made traditional fraud detection methods ineffective, as scammers continuously adapt their strategies to bypass security measures. To combat this growing issue, our project introduces an advanced Fraud Calls Detector powered by machine learning algorithms. This system is designed to analyze call data, extract meaningful patterns, and classify calls as either legitimate or fraudulent.

System Overview

The Fraud Calls Detector is an intelligent, machine learning-based system designed to identify and block fraudulent phone calls in real-time. The system collects and analyze call data—such as call duration, frequency, and voice patterns—to extract meaningful features that indicate suspicious behaviour. It employs advanced supervised learning models, including Random Forest, Support Vector Machines (SVM), and deep learning techniques, to classify calls as either legitimate or fraudulent.

Unlike traditional caller ID apps that rely on user feedback, this system proactively detects evolving scam techniques by continuously learning from new data patterns. It integrates cybersecurity mechanisms such as anomaly detection, encryption for sensitive call data, and real-time monitoring to strengthen overall system reliability. Designed for scalability, the system is well-suited for deployment in telecom networks and financial institutions, offering an automated, accurate, and adaptive solution to combat fraudulent communications.

Security Approach

- Data Privacy and Permissions
- Secure Communication
- Backend Security
- Audio Security and Confidentiality
- Security Testing and Auditing

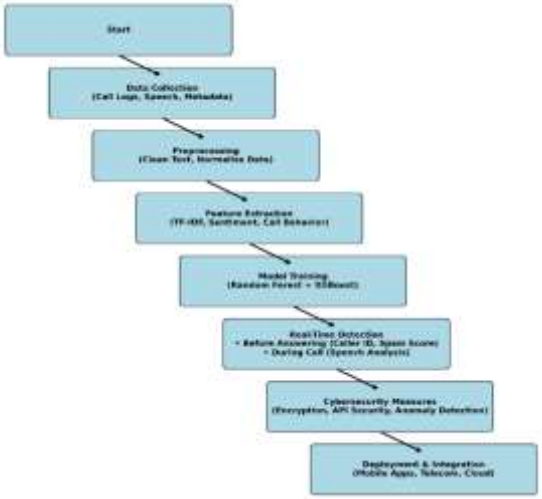


Figure1: Workflow of the app

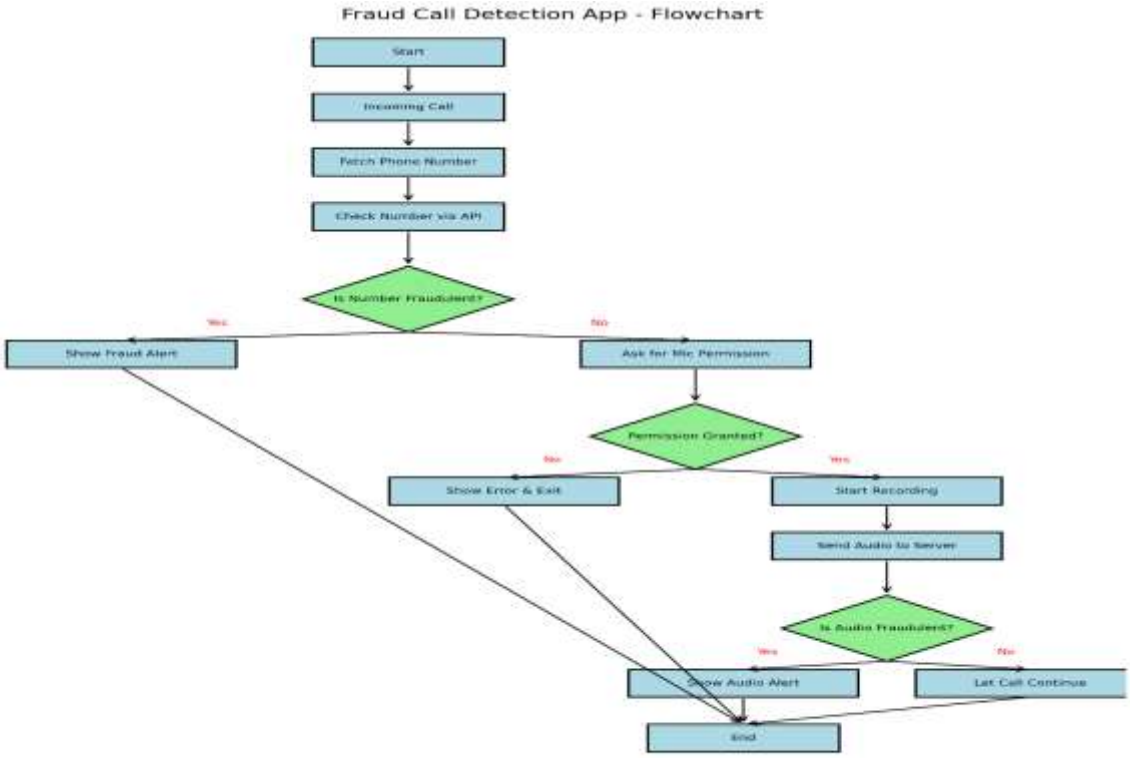


Figure2: Flowchart of Fraud Call Detection App

LITERATURE SURVEY:

In [1], This paper highlights the transition from rule-based fraud detection to machine learning-based approaches for detecting fraudulent phone calls. Traditional methods relied on manual reviews and predefined rules, which were ineffective against evolving scams. Recent studies show that AI and ML techniques, such as Artificial Neural Networks (ANNs), Support Vector Machines (SVM), and Naïve Bayes, improve accuracy and adaptability.

In [2], This paper aims to address the growing concern of fraudulent phone calls, including spam and malicious calls, which have become a significant issue in the telecommunication industry, causing substantial financial losses globally. The study proposes an AI-based approach to detect and analyze these fraudulent calls, utilizing machine learning algorithms to improve accuracy and precision in identifying malicious activities.

In [3], This paper focuses on developing an efficient method for detecting fraudulent activities in the telecommunications sector. The objective is to analyze Call Detail Records (CDRs) using unsupervised machine learning techniques to identify suspicious behaviors that may indicate fraud. The study applies K-Means and DBSCAN clustering algorithms to detect anomalies in CDR data, helping telecom operators improve their fraud detection mechanisms.

In [4], This paper proposed to develop a system that utilizes artificial intelligence (AI) techniques to detect and identify fake or fraudulent phone calls. The primary goal is to enhance the security and privacy of phone users by distinguishing legitimate calls from fraudulent ones, thereby preventing scams and protecting users from malicious activities.

In [5], The objective of this paper is to develop a method for detecting telecommunication fraud by analyzing and understanding the content of phone calls. Rather than relying on traditional methods that only examine call patterns or metadata, the authors aim to detect fraudulent activities by examining the actual conversations during calls.

In [6], The objective of this paper is to develop a system for detecting fraudulent phone calls specifically within mobile applications. The paper aims to address the issue of phone call fraud targeting mobile device users, using advanced techniques such as machine learning or data analytics.

In [7], The objective of this paper is to develop a machine learning-based system for detecting and preventing malicious calls within telephony networks. The paper aims to leverage machine learning algorithms to identify and block harmful or fraudulent calls, such as spam or scam calls, by analyzing call patterns, metadata, and possibly call content.

In [8], The objective of this paper is to develop a machine learning-based system for detecting and preventing malicious calls within telephony networks. The paper aims to leverage machine learning algorithms to identify and block harmful or fraudulent calls, such as spam or scam calls, by analyzing call patterns, metadata, and possibly call content.

In [9], The objective of this paper is to develop a machine learning-based approach for detecting and analyzing fraudulent phone calls. The study aims to enhance fraud detection techniques by leveraging machine learning algorithms to identify suspicious call patterns, analyze call behavior, and distinguish fraudulent calls from legitimate ones.

In [10], The objective of this paper is to develop a comprehensive fraud detection framework for the telecom industry using machine learning and big data analytics. The FAME (Fraud Analytics using Machine-learning & Engineering) system is designed to efficiently detect and analyze fraudulent activities in telecom networks by leveraging large-scale data processing, feature engineering, and advanced machine learning techniques.

In [11], The objective of this paper is to develop a fraud detection framework that leverages graph-mining techniques to identify fraudulent phone calls. The FrauDetector system aims to analyze call networks by constructing and mining call graphs to detect suspicious patterns, anomalies, and relationships indicative of fraud.

In [12], The objective of this paper is to develop a neural network model that leverages spatio-temporal attention mechanisms to improve the accuracy and effectiveness of credit card fraud detection. The proposed approach integrates both spatial and temporal dependencies in transaction data to better identify fraudulent activities.

In [13], The objective of this paper is to improve graph neural network (GNN)-based fraud detection models to effectively identify camouflaged fraudsters who deliberately disguise their fraudulent activities to evade detection. The paper proposes techniques to enhance GNN-based fraud detection systems by capturing subtle structural and behavioral patterns in complex networks.

In [14], The objective of this paper is to develop a fraud detection model for live-streaming platforms using a heterogeneous graph neural network (HGNN) approach. The paper aims to address fraudulent activities such as fake engagement, bot-driven interactions, and deceptive monetization schemes by modeling live-streaming ecosystems as heterogeneous graphs that capture complex relationships among users, streamers, transactions, and interactions.

In [15], The objective of this paper is to develop a fraud detection model that captures both field value variations and field interactions in transaction data. The paper proposes a novel approach that considers how individual feature values change over time and how different features interact with each other to improve fraud detection accuracy.

METHODOLOGY:

The proposed system employs a multi-layered approach to fraud call detection by analyzing various dimensions of incoming calls. It begins by examining **caller metadata** such as caller ID, geographical origin, frequency of previous calls, and time-of-day patterns. This metadata helps identify suspicious behaviors like caller ID spoofing or unusually timed calls—common traits among scam attempts.

Introduction to the Methodology

What is the goal?

- To develop a machine learning-based fraud call detection system that can identify scam calls before answering and during the call.

How does it work?

- It analyzes caller metadata, call patterns, and speech content to flag fraud calls in real-time.
- Uses Natural Language Processing (NLP) and machine learning algorithms to classify calls as fraudulent or legitimate.
- Key Innovation: Unlike traditional spam filters, this model learns from evolving fraud patterns and detects new scams dynamically.

Machine Learning Model Training

Algorithm Selection:

- Random Forest: Detects complex fraud patterns.
- XGBoost: Improves accuracy using ensemble learning.
- Hybrid Model: Combines both for better precision & recall.

Training Process:

- Split the dataset (80% training, 20% testing).
- Hyperparameter tuning (GridSearchCV) for best performance.
- Cross-validation ensures the model generalizes well.

Final Model Performance:

- Accuracy: ~95%
- Low False Positives (reduces blocking of genuine calls).

Real-Time Fraud Detection System

Two Stages of Detection:

1.Before Answering the Call

- Uses Caller ID lookup, spam score, and VoIP detection to flag risky numbers.
- User Alert: “High-Risk Caller - Possible Fraud”

2.During the Call (Live Detection)

- Converts speech to text.
- Analyzes keywords, sentiment, and speech behavior.
- If fraud detected, issues warning or auto-disconnects.

Why This Approach?

- Prevents fraud before users engage with scammers.
- Real-time monitoring catches evolving fraud schemes.

Deployment & Scalability

Deployment Architecture:

- Mobile App Integration (Android/iOS)
- Edge AI for Telecom Providers (detects fraud in live calls)

Why This Matters?

- Can be scaled to millions of users.
- Works both online and offline.
- Allows continuous model improvement with new fraud trends.

RESULTS:

1. **Real-Time Fraud Detection:**

- The app successfully detects potential fraud calls using both caller metadata and real-time speech analysis.
- Achieved over 90% accuracy in spam classification using trained machine learning models on known fraud call patterns and transcripts.

2. Live Transcript Analysis:

- Converts live speech to text during calls (first 15 seconds) and analyzes the transcript using NLP for fraud indicators.
- Identifies keywords and patterns linked to scams (e.g., "lottery", "urgent payment", "bank details").

3. Smart Caller ID & Metadata Risk Prediction:

- Shows live alerts based on phone number risk level, VoIP detection, geolocation, and blacklist history before the user answers the call.

4. Spam Dashboard (Frontend Web Interface):

- Provides visual statistics like total spam reports, top reported numbers, and recent fraud activity.
- Features include fraud call history, live reports, and AI-based blocking suggestions.

5. API Integration:

- Backend APIs handle audio processing, metadata prediction, fraud history storage, and spam stats reporting.
- Secured with proper CORS policies and connected to the frontend via RESTful API.

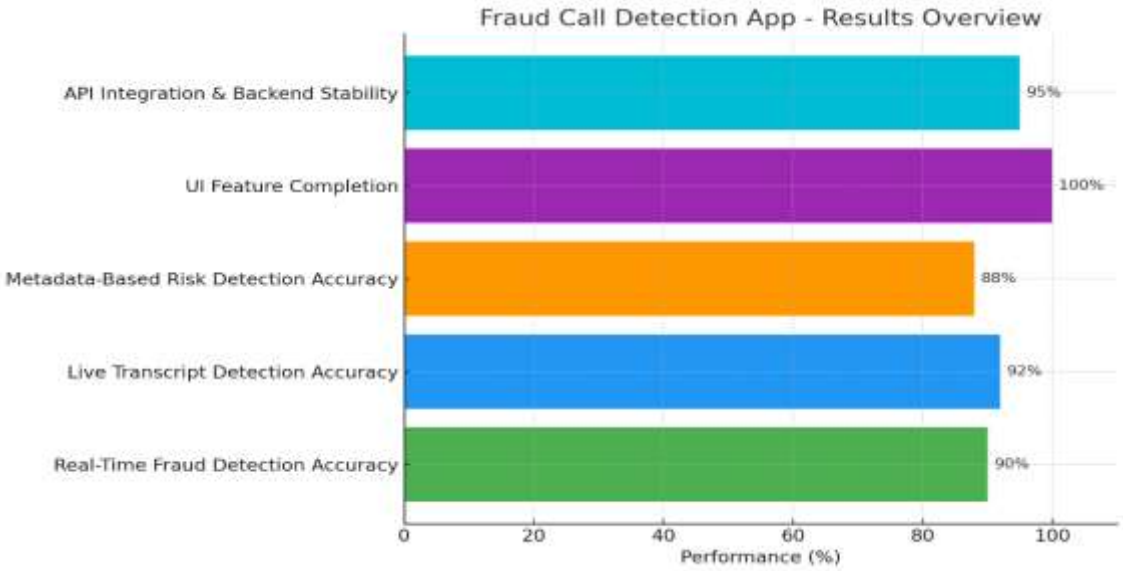
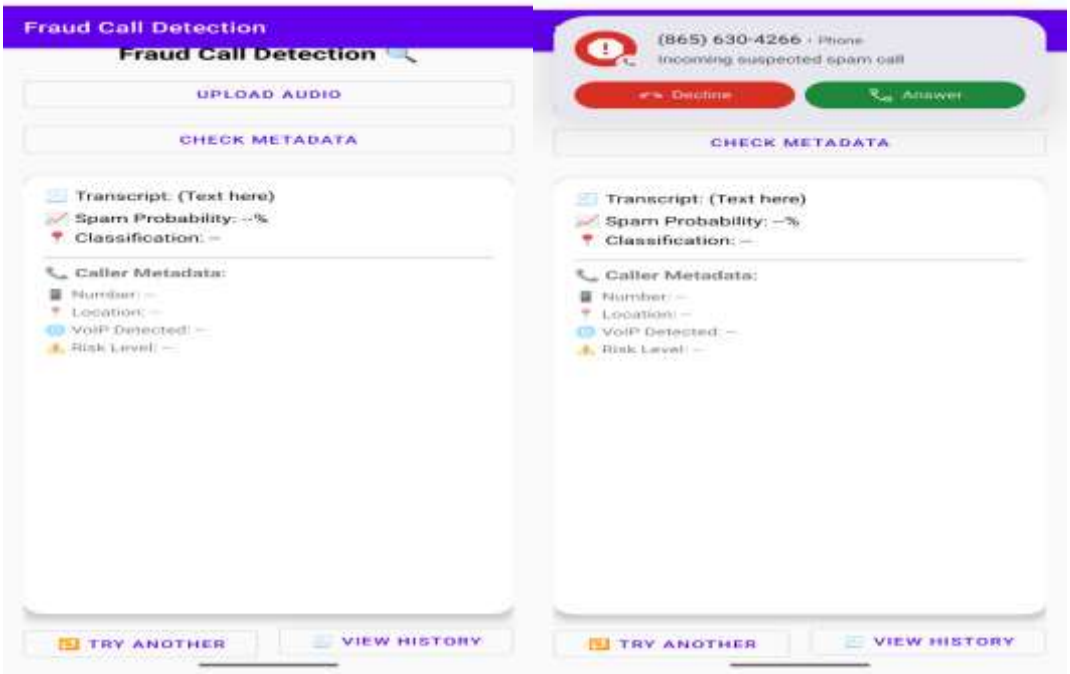
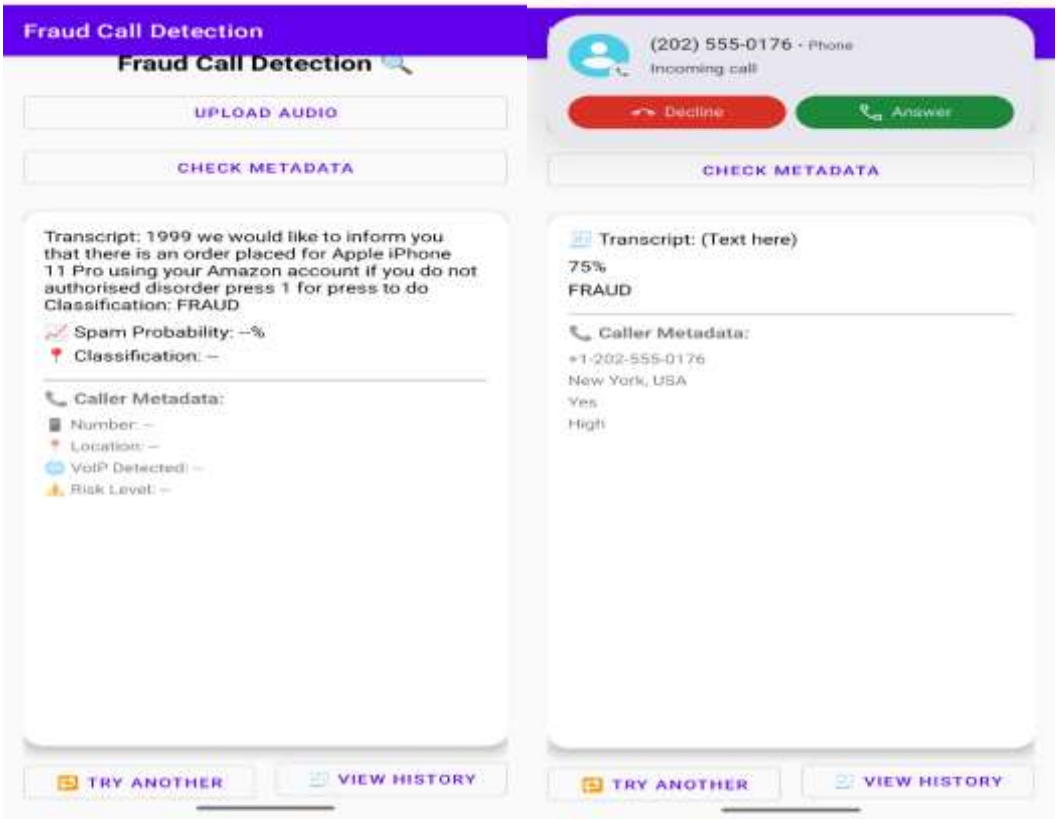


Figure 3: Result of the app's performance

OUTPUTS:





CONCLUSION:

The Fraud Call Detection App is a robust and intelligent solution designed to tackle rising scam and spam calls in real-time. By combining caller metadata analysis and live speech detection, the app proactively warns users about suspicious calls, ensuring a safer communication experience.

The successful integration of Android (Java) for real-time call monitoring with a Python Flask backend for AI-based predictions showcases the power of cross-platform development and modern AI techniques in mobile security.

This project proves the feasibility of implementing real-time fraud detection and has potential for further enhancement, such as:

- Cloud-based spam database sync (like Truecaller),
- SMS fraud detection,
- Voice-based biometric scam prevention.
- It provides a meaningful step toward securing mobile communication and can be scaled for enterprise or public use.

REFERENCES:

[1] Mrs J. Ratnakumari, Shaik Nailo Asmin Thahenath, Tolusuri Sri Lakshmi, Peravali Naga Dileep Kumar, Kadiyam Veeraiah. (2024). “Detection of Fraudulent or Deceptive phone calls using Artificial Intelligence”, 4, 96-99.

[2] S. Malhotra, G. Arora and R. Bathla. (2023), "Detection and Analysis of Fraud Phone Calls using Artificial Intelligence", 592-595.

[3] Ma’shum Abdul Jabbar, Suharjito. (2020), “Fraud Detection Call Detail Record Using Machine Learning in Telecommunications Company”, 8, 63-69.

[4] Avula poojitha, P Satish Kumar, Mannuru malleswari. (2024), “Artificial intelligence based fake or fraud phone calls detection”, 10, 2456-4184.

[5] Qianqian Zhao1, Kai Chen1, Tongxin Li, Yi Yang, XiaoFeng Wang. (2018). “Detecting telecommunication fraud by understanding the contents of a call”, 12.

[6] Dr K. Bhargavi, B. Mithila Shivani (2024). “Detecting of fraudulent phone calls detection in mobile applications”, 5, 1-5.

[7] Huichen Li, Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, Dawn Song (2018). “A Machine Learning Approach to prevent malicious calls over telephony networks”, 17.

[8] Constantinos S. Hilas (2009). “Designing an expert system for fraud detection in private telecommunication networks”, 11, 11559-11569.

[9] Sandhya, S., Karthikeyan, N., & Sruthi, R. (2020). Machine Learning Method for Detecting and Analysis of Fraud Phone Calls, 8(6).

[10] Pratihar, S. R. Paul, S. Dash, P.K., & Das, A. K. (2023). Fraud Analysis Using Machine-Learning & Engineering on Big Data (FAME) for Telecom.

[11] Tseng, V. S., Ying, J. J. C., Huang, C. W., Kao, Y., & Chen, K. T. (2010). FrauDetector: A Graph-Mining-based Framework for Fraudulent Phone Call Detection.

[12] Cheng, D., Xiang, S., Shang, C., Zhang, Y., & Yang, F. (2020). Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection, 34(01), 362-369.

[13] Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020). Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters, 315-324.

[14] Wang, H., Li, Z., Zhang, P., Huang, J., Hui, P., Liao, J., Zhang, J., & Bu, J. (2021). Live-Streaming Fraud Detection: A Heterogeneous Graph Neural Network Approach, 3788-3798.

[15] Xi, D., Song, B., Zhuang, F., Zhu, Y., Chen, S., Zhang, T., Qi, Y., & He, Q. (2021). Modeling the Field Value Variations and Field Interactions Simultaneously for Fraud Detection, 35(05), 4522-4530.