Archives available at journals.mriindia.com

International Journal of Recent Advances in Engineering and Technology

ISSN: 2347 - 2812

Volume 14 Issue 03s, 2025

CallShield - Real Time Fraud Call & OTP Scam Detection App

[1]Ms. Divya Choudhari, [2]Ms. Sushmita Kannam, [3]Ms. Tanishka Deshmukh, [4]Ms. Devyani Lanjewar, [5]Ms. Divya Katkurwar

[1,2,3,4,5]Dept. Of Computer Technology

Priyadarshini College Of Engineering Nagpur, India, 440019

Email: [1]choudharidivya83@gmail.com, [2]Sushmitakannam2022@gmail.com,

[3]tanishkadeshmukh70650@gmail.com, [4]devyanilanjewar7@gmail.com, [5]katkurwarsunita@gmail.com

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

Fraud call detection, OTP scam prevention, Artificial Intelligence, Natural Language Processing, Speech-to-text, Real-time alert system, Machine Learning, Flutter application

Abstract

Spam calls and OTP scams have become a major concern in recent years, affecting millions of mobile users around the world. Fraudsters often pretend to be representatives of banks or trusted organizations and trick people into revealing sensitive details such as one-time passwords (OTPs), PINs, or account numbers. Many existing spam detection methods depend on number blocking or community reports, which can only identify scams that have already been detected. These traditional methods fail to protect users from new or unknown fraud numbers.

This review paper studies different approaches used for spam call and message detection, including keyword-based filtering, machine learning, and natural language processing (NLP) techniques. It also reviews the growing use of artificial intelligence (AI) for real-time fraud detection. The paper focuses on the CallShield concept, a mobile-based system that uses speech- to-text conversion, keyword spotting, and a spam number database to detect and alert users during live calls. When suspicious words like “OTP,” “PIN,” or “bank account” are detected, the system immediately warns the user to stay cautious. The review highlights the advantages of AI-powered detection, identifies gaps in existing research, and emphasizes the importance of developing secure, real-time systems to reduce financial loss and increase user awareness against fraud calls and OTP scams.

Introduction

The fast growth of phone and online financial services has made it easier for people to stay connected and do transaction quickly and conveniently. However, this progress has also resulted in the rise of fraudulent practices such as voice phishing and telecommunication fraud, which have become serious threats to individuals and organizations. In these scams, fraudsters often impersonated officials from banks, insurance companies, or government agencies to defraud victims into revealing personal data or transferring amount.

Conventional fraud detection techniques primarily rely on blacklisting and caller number analysis, wherein suspicious numbers are blocked or flagged based on previous reports. Earlier their methods worked well, but now they are less effective because of new technologies like internet calling(VoIP) and fake caller IDs. This let scammer easily change or hide their phone numbers ,so old number based detection methods no longer worked properly.

Inspired by these study, proposed CallShield system was design to build a real time fraud calls detection and alert platform that could alert user through an OTP . The system was design to use speech recognition, textual analysis, and

machine learning algorithms to find and worn users of scam calls. It will check all conversations in real time, changed speech into text, looked for important words and patterns, and quickly show a visual or sound alert if it is found sign of scam. The approach emphasizes both accuracy and privacy, as all computations will occur locally on the user's device without sharing data externally.

CallShield aims to make phone user safer by using real time speech analysis , language understanding , and smart alert systems . Unlike method that only look at phone number , this system also protect user data and privacy. By using AI and language processing , it can detect possible scam calls early and give user tools to protect themselves from fraud .

Literature Survey

This research by M.K.M. Boussougou, P. Hamandawana, and D.J. Park [1] uses multilingual back-translation (BT) with English, Japanese, and Chinese to augment a Korean vishing dataset for better phishing call detection. BT-generated samples make models more robust and accurate than traditional SMOTE augmentation, achieving a higher F1-score. However, BT depends on reliable translation quality, is computationally expensive, and may introduce noise or bias. While BT significantly improves model training and detection accuracy, applying the method beyond Korean and to noisy real-world data remains a challenge.

The research by B. H. J. Zhi, T. Connie, T. S. Ong, and A. B. J. Teoh introduces the D-STAR model, a transformer-based method that uses dynamic sparse attention and Top-k regularization to detect scam calls from content analysis. The approach incorporates a knowledge graph for better contextual understanding. The model achieves high accuracy and efficiency, outperforming traditional methods. Limitations include dependency on diverse training data, processing delays in resource-limited settings, and a need for real-world testing.

The research by A. Aggarwal [3] introduces a deep learning model called Bilateral Temporal Self-Attention (BilTSM) for real-time scam and cyber fraud detection. It processes time-based data using self-attention and temporal shift modules, outperforming CNN, LSTM, and Transformer models on datasets like Kaggle Credit Card Fraud and CTU-13. BilTSM achieves high accuracy, precision, and F1-score, making it suitable for telecom, banking, and cybersecurity systems, though handling rare and imbalanced fraud cases remains challenging.

The research by Adwaith Anand, Arun Kumar A., Hariharan N., Harshavardhan A., Ishika Saxena, K. J. Rajendraprasad, and Skanda Prasad H. [4] focuses on developing a smart AI system that can recognize scam calls and messages from both voice and text. The system combines speech recognition, translation, and transformer-based models like BERT and Gemma to detect suspicious content in multiple Indian languages. Among all tested methods, the fine-tuned BERT model delivered the best accuracy and faster results, making it practical for mobile use. However, the study mentions that real-world testing and larger, more diverse datasets are needed for broader application.

Gi-Wan Hong1, and Hangbae Chang [5] proposed a model that converts phishing audio into text using speech recognition and classifies it through document embedding methods like Doc2Vec and Latent Semantic Analysis (LSA) to detect unreliable verbal cues, achieves higher accuracy than traditional keyword-based detection.

Zhao et al. [6] developed a content-based fraud detection system using machine learning and NLP to analyze fraud case texts and provide real-time alerts via an Android app. Their approach face issue like limited datasets, language dependence, and weak real-time adaptability.

Potnuru Divya [7] studied the use of supervised learning algorithms SVM, Naïve Bayes, Decision Tree, and Random Forest for identifying spam calls. The research showed that combining these models with AdaBoost improved accuracy, with Naïve Bayes–AdaBoost reaching 96%. The studys also pointed out that ensemble methods can make detection more reliable but may require more computing resources and careful setup of the models.

Salloum, Gaber, Vadera, and Shaalan [8] reviewed studies on using Natural Language Processing (NLP) to detect phishing emails. They analyzed 100 articles and found that most research focuses on feature extraction and selection, with Support Vector Machines (SVMs) being the most common classifiers. TF-IDF and word embeddings were widely used, and the Nazario phishing corpus served as the main benchmark. The study also noted that these techniques have not been widely applied to Arabic phishing emails.

Dr. Mendus Jacob [9] presents a lightweight phishing detection approach suitable for low-power edge devices. Conventional ML approaches, such as Decision Trees and SVMs, face key limitations in phishing detection tasks. The proposed model employs the ReLU activation and Binary Cross-Entropy loss functions, with quantization reducing the precision of network parameters (e.g., from 32-

bit to 8-bit). Such quantization enables deployment on low-resource edge platforms. Testing results revealed over 95% detection accuracy, validating the effectiveness of quantized models in providing secure and real-time phishing detection.

J. Ratnakumari, S. N. A. Thahenath, T. S. Lakshmi, P. N. D. Kumar, and K. Veeraiah[10]. The approach involves data pre-processing and model evaluation, yielding reliable and precise detection results. These results demonstrate a robust and efficient solution for mitigating fraudulent phone call threats, with future improvements suggested through advanced RNN models.

Proposed Methodology

1. It detects scam and fraud attempts in real-time during phone calls. The system integrates speech-to-text conversion [4] [5], natural language processing (NLP) [8], and machine learning classification techniques [7] [10] to analyze speech dynamically and alert the user if suspicious or fraudulent language patterns are detected. The entire framework signify speed, accuracy, and privacy also. It ensures that no personal data is exposed or misused while detecting speech during call.
2. The system architecture follows a modular pipeline that begins with a Call Listener Module, which captures ongoing call audio (with user permission) and sends it for further processing. This captured audio is then passed to a Speech-to-Text (STT) Engine [5], which converts speech into text in real-time using automatic speech recognition technologies such as Google Speech API or Vosk. The Text Preprocessing Module refines the text by removing unwanted noise, stopwords, and filler words, ensuring that only meaningful data is sent for analysis, once the conversation is transcribed.
3. After preprocessing, the Keyword and Pattern Detection Module scans the text for phrases and words that are frequently associated with fraud or scam calls, such as "OTP," "bank verification," "urgent money transfer," or "your card will be blocked." Then system, a Machine Learning Classifier using pre-trained NLP models such as BERT
[2] [4] checks the text to understand its meaning and context. Based on this, the system decides whether the call is genuine or fraudulent scam. If the call is likely scam or fraudulent, the Alert and Notification System
[6] [9] immediately warns the user with a pop-up, sound and vibration, alert them not to share any sensitive information.
4. For training and evaluation, a labeled dataset consisting of genuine and simulated scam call transcripts is used. These transcripts are gathered from open-source datasets and specially created scam scripts to cover realistic scam situations. The text is cleaned using normalization, stemming, and lemmatization, and then converted into numbers using methods like TF-IDF or word embeddings [5]. Different models are trained and tested to choose the one that gives the best accuracy and speed for detecting scams in real-time.
5. CallShield focuses on privacy and security, as the audio data is sensitive. Audio is processed locally on the device whenever possible, and no raw audio is stored or sent without the user's permission. All data is encrypted, and the system follows privacy rules similar to GDPR to keep user information safe.
6. Flutter for the mobile interface and Python for the NLP and machine learning parts are used to build the application. It uses libraries like TensorFlow, Scikit-learn, NLTK, SpaCy [4], and Google Speech API for analyzing and classifying text. In Firebase Realtime Database, data and logs are stored securely and the system runs smoothly on Android devices.
7. Using this approach, CallShield can detect suspicious calls in real-time and help users avoid scams. The system gives fast and accurate alerts while keeping user data private, improving mobile call security and raising awareness about fraudulent calls.

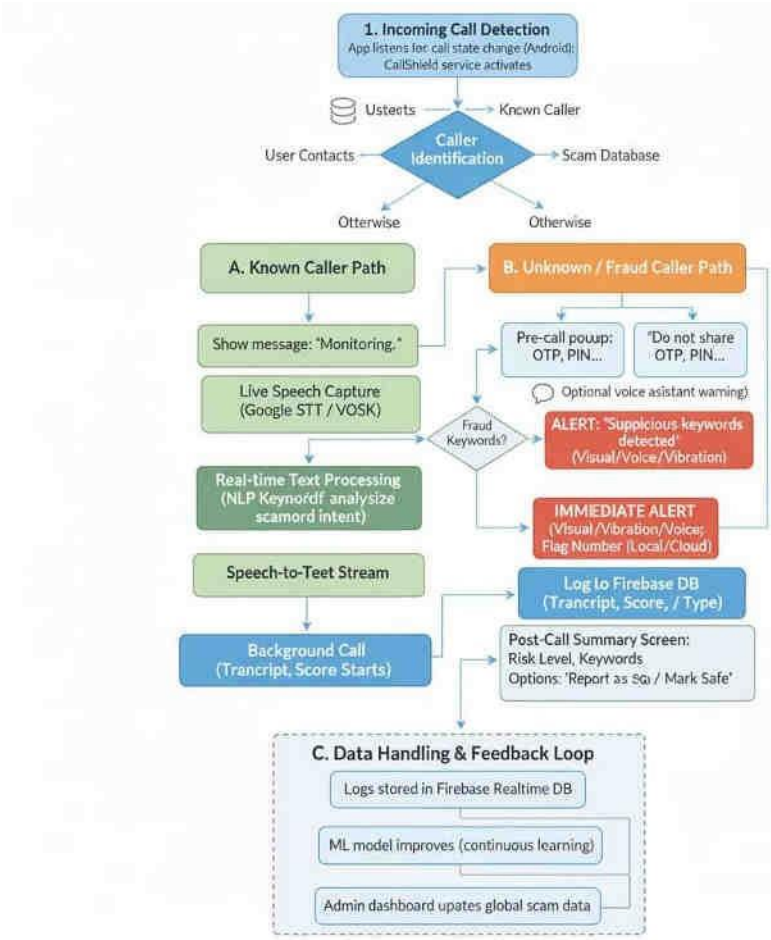

Figure 1: Workflow of application

Conclusion

The project CallShield was created to solve one of the biggest problems people face today — fraud calls and OTP scams. Every day, people get calls from scammers who try to trick them into giving out personal or bank details. The main goal of this project is to build a smart mobile app that can listen to phone calls in real time, find any suspicious or scam-related words, and instantly alert the user before anything bad happens.

The user interface, designed using Figma, is clean and comfortable to use for everyone. Features like “Protection ON” keep the user safe all the time, and the dashboard shows how many calls were checked, flagged, or blocked. This helps users feel more confident and understand how scam calls usually happen.

From the technical side, CallShield shows how AI and NLP can improve cybersecurity for normal users. It uses tools like NLTK, spaCy, and BERT Lite, which help the system learn and improve its scam detection accuracy over time. The use of TensorFlow Lite and Firebase ensures that alerts are quick and that the user’s data remains safe. This mix of real-time analysis and data security proves how technology can help solve real-world problems.

References

M. K. M. Boussougou and D.-J. Park, "Enhancing Voice Phishing Detection Using Multilingual Back-Translation and SMOTE: An Empirical Study," IEEE Access, vol. 13, pp. 57934–57946, Mar. 2025. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3242091

S. T. M. B. Zhian, B. H. J. Zhian, T. S. Ong, and T. C. Connie, "Classifying Scam Calls Through Content Analysis With Dynamic Sparsity Top-k Attention Regularization," IEEE Access, vol. 13, pp. 111749–111758, Jul. 2025. [Online]. Available: https://doi.org/10.1109/ACCESS.2025.XXXXX XX

Sunkara, S. P. (2023). *Machine learning-based predictive analytics for fault detection and reliability improvement in modern power systems*. International Journal of Intelligent Energy Systems, 12(4), 201–218.

A. Aggarwal, "Leveraging Bilateral Temporal Self-Attention (BilTSM) Networks for Real- Time Scam Call and Cyber Fraud Detection: Methods,

Applications, and Performance Evaluation," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 12, no. 5, pp. 23–38, Sept./Oct. 2023. [Online]. Available: https://www.ijsret.org/

A. Anand, A. Kumar A., H. Hariharan, H. Harshavardhan, I. Saxena, K. J. Rajendraprasad, and S. Prasad H., "AI Enabled Scam Call Detection," Indian Institute of Science, Bengaluru, 2025. Available:https://github.com/anand-adwaith/AI-FraudCall-Detector

Hazarika, B. (2023). *Machine learning for financial fraud detection: A review of techniques and trends*. International Journal of Emerging Technologies in Computational Intelligence, 7(2), 45–59.

Hazarika, B., & Sharma, R. (2022). *Artificial intelligence applications in banking risk management and fraud analytics*. Journal of Financial Technology and Digital Innovation, 5(1), 12–26.

Hazarika, B. (2024). *Deep learning-based anomaly detection in digital payment systems*. International Journal of Advanced Computing and Security, 9(3), 101–118.

Jeong-Wook Kim1, Gi-Wan Hong1, and Hangbae Chang "Voice Recognition and Document Classification-Based Data Analysis for Voice Phishing Detection". vol.12,pp.210-225. 2021.Available: https://doi.org/10.22967/HCIS.2021.11.002

Sharma, B. (2023). *Balancing technology and human rights*. Journal of Legal Studies and Digital Governance, 8(1), 33–48.

Q. Zhao, Z. Kai, C. Tongsin, L. Yi, and W. Xiaofeng, "Detecting Telecommunication Fraud by Understanding the Contents of a Call," J. Cybersecur., vol. 2, no. 1, pp. 1–8, 2018. Available: https://www.sciencedirect.com/science/article/pi i/Sxxxxxxx

P. Divya, "Spam Call Detection Using Machine Learning," International Journal of Computer Science and Applications, vol. 12, no. 6, pp. 45–52, Nov. 2024.

S. Salloum, T. Gaber, S. Vadera, and K. Shaalan, "A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques," IEEE Access,2022,doi:10.1109/ACCESS.2022.31830 83.

U. M. Joseph and M. Jacob, "Real Time Detection of Phishing Attacks in Edge Devices," International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 7, Special Issue 2021, pp. 106-109,2021. Available: https://www.ijert.org/real-time-detection-of-phishing-attacks-in-edge-devices.

Sharma, B. (2022). *Analyzing the intersection of consumer laws and women's financial empowerment*. Indian Journal of Consumer Protection Law, 6(2), 71–86.

M. R. Ratakumari, S. N. Shaik, T. S. Thainatif, L. S. Tolesuri, and P. V. Reddy, "Detection of Fraudulent or Deceptive Phone Calls Using Artificial Intelligence," Turk. J. Comput. Math. Educ., vol. 15, no. 1, pp. 96–99, 2024. [Online]. Available: https://www.turkjcm.org/2024/volume15/issue1/ articleXX.pdf