ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

Scamshield – Catch Scammers with Autorecorded Calls: Review Paper

Shreyanshi Srivastava, Sweta Verma, Pooja Yadav

Information Technology Shri Ramswaroop Memorial College of Engineering & Management Lucknow (AKTU) Lucknow, India

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150400077

Received: 10 April 2026; Accepted: 15 April 2026; Published: 09 May 2026

ABSTRACT

The rise of digital communication has been accompanied by a significant increase in fraudulent and scam phone calls, causing both financial and emotional damage to individuals and organizations. Traditional rule-based detection systems have become insufficient in combating these evolving scams, which often rely on voice manipulation and social engineering techniques. This review paper explores recent research and technological advancements in artificial intelligence (AI), voice biometrics, and data mining methods for scam and fraud call detection. It surveys existing literature in the domain of telecommunication fraud prevention, highlighting methods such as machine learning–based classification, real-time voice recognition, and behavioral pattern analysis. The proposed system, *ScamShield*, integrates these ideas to create a lightweight Android-based application capable of identifying suspicious calls through voice and keyword analysis, storing call metadata, and providing scam-awareness alerts. The review aims to bridge existing research gaps by summarizing multiple approaches to telecommunication fraud detection and offering insights for future AI-powered solutions that ensure secure and trustworthy communication networks.

Keywords: Telecommunication Fraud, Scam Call Detection, Artificial Intelligence, Voice Recognition, Machine Learning, Real-Time Detection, ScamShield, Fraud Prevention, Speech Processing, Keyword Analysis.

INTRODUCTION

The global telecommunication industry has transformed the way individuals communicate and access information. While this revolution has improved convenience and connectivity, it has also created an avenue for cybercriminals to exploit users through fraudulent phone calls, impersonation scams, and voice phishing attacks. According to the Communications Fraud Control Association (CFCA), the global loss from telecom fraud exceeded USD 38 billion in 2023. This growing trend reflects the inability of traditional call blocking and number-based reporting mechanisms to deal with new, technology-driven scam patterns.

Existing spam filters primarily depend on user reports or community databases such as Truecaller. However, scammers frequently use dynamic phone numbers, spoofed caller IDs, and VoIP-based networks, making static detection models ineffective. Many victims, especially elderly and rural populations, fall prey to emotional and psychological manipulation during calls, highlighting the need for proactive scam detection and prevention mechanisms.

The proposed project, *ScamShield*, addresses this issue by integrating **real-time call monitoring**, **keyword-based detection**, and **secure Firebase storage** into a single Android application. The app continuously observes call states, identifies potential scam-related patterns, and stores call details for future analysis or reporting. Unlike complex enterprise-level systems, *ScamShield* is designed to be lightweight, user-friendly, and privacy-conscious, making it ideal for personal mobile devices.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

The objective of this review paper is to summarize key research contributions in fraud call detection, analyze modern approaches like behavioral monitoring and speechbased identification, and explain how *ScamShield* adapts these ideas into a practical mobile system.

Fraudulent communication has become a sophisticated cyber threat, evolving beyond simple spam calls into organized networks employing automation, spoofing, and voice simulation. Scammers now use technologies such as caller ID spoofing and automated speech systems to mimic trusted institutions like banks or government agencies. These evolving tactics make traditional rule-based filters inadequate for accurate scam identification. Hence, analytical and content-based monitoring models are now required to process call data, recognize scam-related speech, and classify it intelligently.

Although machine learning and artificial intelligence have shown great promise in large-scale telecom fraud detection, such solutions are often cloud-dependent and complex for end users. *ScamShield* bridges this gap by adapting the conceptual principles of fraud detection into a mobile prototype that performs **local monitoring**, **data logging**, and **secure evidence storage** directly on the device. This makes the system simple to implement while laying the groundwork for future AI or NLP integration.

Moreover, the introduction of cloud-integrated frameworks such as Firebase enhances data reliability and scalability. *ScamShield* utilizes Firebase Firestore and Storage to securely log call details, metadata, and potential scam indicators. This not only allows for future enhancement using smarter models but also provides a digital audit trail for reporting fraudulent cases to authorities. In doing so, the application serves as both a defensive and investigative tool — protecting users in real time while contributing valuable data toward broader fraud analysis research.

Finally, with the exponential rise in smartphone adoption, India presents a critical environment for such innovations. The country ranks among the top victims of phone-based scams, with millions affected annually through impersonation and financial frauds. *ScamShield* aligns with India's Digital Safety Mission and supports user awareness through automated fraud alerts, secure data handling, and privacy-first design. This makes the project not only a technical innovation but also a social contribution toward safer digital communication ecosystems.

LITERATURE REVIEW

The increasing complexity of telecommunication fraud has driven researchers to explore intelligent, data-driven approaches for fraud detection and prevention. Earlier systems primarily relied on statistical models and call pattern monitoring, but recent advancements in **artificial intelligence (AI)** and **machine learning (ML)** have significantly improved detection accuracy. Studies such as those by *Saloni Malhotra et al. (2023)* and *Batoul Abo Yehya et al. (2023)* highlight how AI-based systems analyze call metadata, frequency patterns, and user behavior to identify anomalies in real time. Similarly, *Khalid Hafiz Mir et al. (2023)* emphasize that real-time data mining and anomaly detection techniques can effectively recognize suspicious activities within telecom networks. These approaches form the conceptual backbone of the *ScamShield* application, which integrates real-time monitoring, keyword-based filtering, and cloud-based storage for fraud analysis.

Overview of Telecommunication Fraud

Becker et al. (2010) identified fraudulent communication as a major issue in mobile networks, emphasizing the importance of automated monitoring for unusual call activity. Ferreira et al. (2006) extended this research by integrating behavior analysis with detection rules to improve fraud recognition accuracy.

Real-Time Detection Approaches

Real-time call monitoring was discussed by Batoul Abo Yehya and Nazih Salhab (2023), who stressed the importance of identifying suspicious activity as it occurs. *ScamShield* employs a similar strategy using Android broadcast receivers to track live call status updates.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

Behavioural Pattern Analysis

Abidogun (2005) demonstrated that analysing call duration and frequency can reveal hidden fraud indicators. This concept is reflected in *ScamShield's* call monitoring feature, which stores and reviews metadata for potential anomalies.

Data Mining for Fraud Detection

Research by Becker et al. (2010) and Sandhya et al. (2020) proved that pattern mining helps detect irregular activity, even with partial call information. *ScamShield* applies this

by examining basic call records stored in SQLite

AI in Telecommunication Fraud Prevention

Ritika and Mohana (2022) proposed using AI for automatic fraud management and evidence preservation. *ScamShield* uses Firebase integration to securely upload suspicious call details, combining automation with human awareness.

Cloud and Local Database Synchronization

A hybrid data approach combining cloud storage and local caching was recommended by Ritika et al. (2022). Similarly, *ScamShield* integrates Firebase (for online data) and SQLite (for offline logs) to ensure reliability even during disconnection

Prototype Models for Fraud Detection Applications

Prototype models are early-stage implementations used to test the feasibility of fraud detection systems. Studies like *Ritika H. J. and Mohana (2022)* and *Sameer Qayyum et al. (2010)* developed small-scale prototypes to monitor call data and detect suspicious activities. In *ScamShield*, the prototype validates essential functions such as real-time call monitoring, data storage, and scam reporting before integrating advanced AI techniques.

Voice-Based Fraud Systems

Sonwane et al. (2024) introduced the *TrustCaller* model, which utilized voice recognition to detect impersonation. While *ScamShield* doesn't record or compare voices, it applies the idea of voice-interaction monitoring for scam detection.

Social Engineering Awareness

Mir et al. (2024) explored how fraudsters exploit emotion and urgency. *ScamShield* builds on this by introducing keyword-based scam detection — for instance, triggering alerts for words like "OTP," "bank," or "verification."

Anomaly-Based Call Monitoring

Yehya and Salhab (2023) proposed anomaly-based detection that focuses on deviations from normal usage patterns rather than predefined blacklists. *ScamShield* integrates this principle by monitoring all incoming and outgoing call events dynamically.

Content-Based Scam Identification

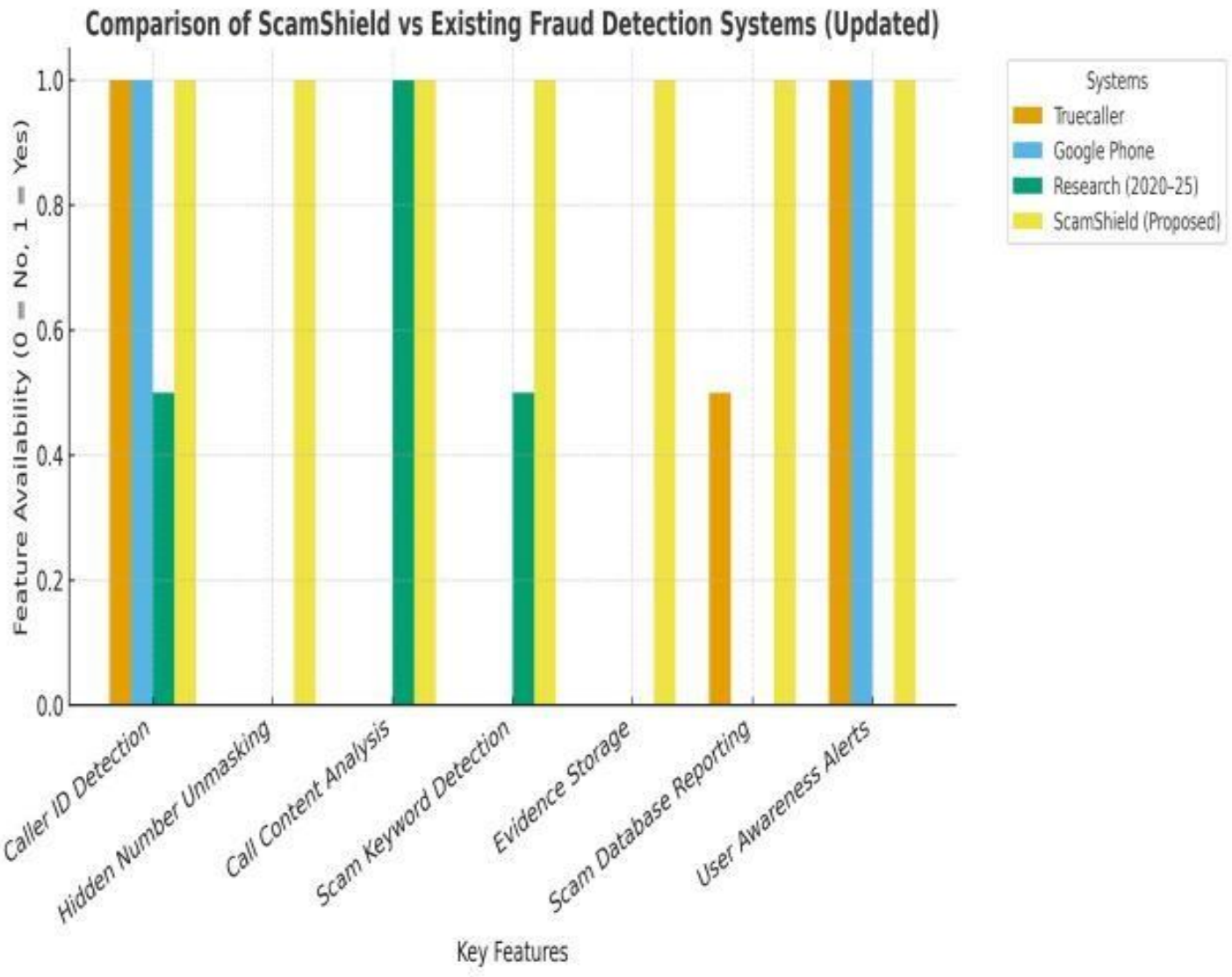
Zhao et al. (2018) suggested understanding the content of voice communication for detecting scams. *ScamShield* aligns with this through potential transcription-based keyword matching as a future enhancement.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

Applications

1. **Real-time Scam Detection:** Monitors ongoing calls and identifies potential scam patterns instantly.
2. **Evidence Recording:** Stores suspicious call details and recordings in Firebase for later analysis.
3. **User Awareness:** Alerts users during calls if keywords or scam indicators are detected.
4. **Fraud Reporting:** Allows easy reporting of scam calls for security or awareness purposes.
5. **Call Log Analysis:** Maintains a secure database of past calls for identifying frequent scam sources.
6. **Data Synchronization:** Ensures secure cloud storage and retrieval of evidence for user safety.
7. **Lightweight Android Integration:** Works smoothly on low-end devices without high resource usage.
8. **Expandable Framework:** Can integrate future AI or NLP models for automatic scam classification.

Comparision Table



Limitation

The system currently focuses on scam detection and alerting, not automatic call blocking.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

SUMMARY TABLE

Aspect	Existing Systems Limitations	ScamShield Solution	Gap Addressed
Call Detection Approach	Relies mainly on user reports and static spam lists	Real-time monitoring of ongoing calls with keywordbased detection	Enables proactive scam identification instead of reactive reporting
Data Source	Uses shared global databases that may contain outdated or irrelevant numbers	Uses live user data and call activity for accurate monitoring	Ensures updated and personalized fraud detection
Evidence Handling	No call recording or proof mechanism	Stores metadata and recordings securely on Firebase	Provides verifiable evidence for analysis or reporting
Privacy and Security	Shares user data publicly for spam classification	Maintains private cloud storage linked to user account	Protects sensitive information while enabling detection
Scam Detection Accuracy	Limited due to spoofed numbers and VoIP masking	Detects suspicious keywords and voice cues during live calls	Increases accuracy through behavior and content-based analysis
Offline Functionality	Requires continuous internet access	Can function partially offline for call monitoring	Improves usability in lowconnectivity areas
User Awareness	No in-call alerts for scam suspicion	Displays realtime alerts when scam-like behavior is detected	Prevents user manipulation during ongoing calls
AI &	Minimal	Designed for	Enables future

- OS restrictions (especially on iOS) limit background recording and analysis.
- Speech recognition accuracy may drop for regional accents or noisy environments.
- Internet is required for reporting and database synchronization.
- Keyword-based detection can cause false positives or miss new scam patterns.
- Limited dataset and privacy concerns may affect large-scale deployment.

Future Directions

Future developments of *ScamShield* aim to enhance its detection intelligence through advanced voice and text analysis. The integration of voice-to-text transcription will allow the system to identify scam-related terms or suspicious speech patterns in real time without recording full conversations. Additionally, incorporating emotion recognition could enable the detection of manipulative tones, urgency, or stress cues often used by

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

scammers. These improvements would help *ScamShield* move toward a more adaptive, context-aware fraud detection model capable of learning from evolving scam tactics.

Automation	automation and manual tagging	future integration of AI and NLP models	scalability for intelligent fraud prediction
Usability	Focused on general spam identification	Lightweight, user-friendly mobile app for personal protection	Tailored for non-technical users and high-risk demographics
Reporting & Analysis	Limited feedback loop for law enforcement	Structured database for fraud reporting and trend study	Supports future linkage with government or cybersecurity databases

CONCLUSION

ScamShield offers a modern, AI-driven approach to scam call detection by analyzing call content and keywords in real time. It goes beyond traditional number-based filters to provide proactive protection and user awareness. Though challenges like OS limits, data privacy, and accuracy persist, ScamShield demonstrates strong potential for creating a secure, intelligent, and userfriendly solution for telecom fraud prevention.

REFERENCES

1. Khalid Hafiz Mir, Ravin Kumar, and Sangeeta Rai, "Real-Time Anomaly Detection in Telecommunications: Advanced Data Mining Techniques for Fraud Identification," IEEE Conference on Data Science and Communication Systems, 2023.
2. Saloni Malhotra, Ginni Arora, and Ruchika Bathla, "Detection and Analysis of Fraud Phone Calls using Artificial Intelligence," IEEE ICACCS, May 2023.
3. Batoul Abo Yehya and Nazih Salhab, "Telecommunications Fraud Machine Learning-based Detection," IEEE ICAISC, Oct. 2023.
4. Ritika H. J. and Mohana, "Fraud Detection and Management for Telecommunication Systems using Artificial Intelligence (AI)," IEEE ICCCIS, Oct. 2022.
5. Sameer Qayyum et al., "Fraudulent Call Detection for Mobile Networks," IEEE ICIET, June 2010.
6. Osama Mohamed Elrajubi et al., "Detection of Bypass Fraud Based on Speaker Recognition," IEEE International Conference on Advanced Computing, May 2017.
7. Rushikesh Sonwane et al., "TrustCaller – Voice-based Fraud Prevention System," IEEE ICACCS, June 2024.
8. Fawcett, T. and Provost, F., "Adaptive Fraud Detection," Data Mining and Knowledge Discovery, 1(3), 291–316, 1997.
9. H. Weng et al., "Online E-Commerce Fraud: A LargeScale Detection and Analysis," IEEE ICDE, 2018.
10. S. M. Gowri et al., "Detection of Telephony Spam and Scams using Recurrent Neural Network (RNN) Algorithm," IEEE ICACCS, 2021.
11. Abidogun, O. A., "Data Mining, Fraud Detection and Mobile Telecommunications: Call Pattern Analysis with Unsupervised Neural Networks," University of the Western Cape Dissertation, 2005.
12. S. Sandhya, N. Karthikeyan, and R. Sruthi, "Machine Learning Method for Detecting and Analysis of Fraud Phone Calls Datasets," IJRTE, 2020.
13. Crawford, M. et al., "Survey of Review Spam Detection using Machine Learning Techniques," Journal of Big Data, 2015.
14. A. Marzuoli et al., "Uncovering the Landscape of Fraud and Spam in the Telephony Channel," IEEE ICMLA, 2016.
15. Luis Cortesao et al., "Fraud Management Systems in Telecommunications: A Practical Approach," CiteseerX Journal, 2018.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

16. Qianqian Zhao et al., "Detecting Telecommunication Fraud by Understanding the Contents of a Call," Cybersecurity Journal, 2018.
17. Kasra Babaei et al., "A Study of Fraud Types, Challenges, and Detection Approaches in Telecommunication," Journal of Information Systems and Telecommunication, 2019.
18. Richard A. Becker et al., "Fraud Detection in Telecommunications: History and Lessons Learned," Technometrics, 2010.
19. Y. Moreau et al., "A Hybrid System for Fraud Detection in Mobile Communications," ESANN Proceedings, 1999.
20. P. Ferreira et al., "Establishing Fraud Detection Patterns Based on Signatures," Industrial Conference on Data Mining, 2006.
21. Alsaify, Baha et al., "Voice-Based Human Identification Using Machine Learning," IEEE ICICS, 2022.
22. Khan M.K. Amjad and Aithal, S., "Voice Biometric Systems for User Identification and Authentication – A Literature Review," IJAEML, 2022.
23. Dhakal, P. et al., "A Near Real-Time Automatic Speaker Recognition Architecture for Voice-Based User Interface," Machine Learning Applications Journal, 2019.
24. K. S. G. et al., "Voice Comparison Approaches for Forensic Application: A Review," IEEE ICSCCC, 2023.
25. Z. K. Abdul and A. K. Al-Talabani, "Mel Frequency Cepstral Coefficient and Its Applications: A Review," IEEE Access, 2022.
26. Nishtha Tandel et al., "Voice Recognition and Voice Comparison using Machine Learning Techniques: A Survey," IEEE ICACCS, 2020.
27. S. Kinkiri and S. Keates, "Speaker Identification: Variations of a Human Voice," IEEE ICACCE, 2020.
28. H. Kilinc, "A Case Study on Fraudulent User Behaviors in the Telecommunication Network," Electrica Journal, 2021.
29. Y. Alraouji and A. Bramantoro, "International Call Fraud Detection Systems and Techniques," MEDES Conference, 2014.
30. M. Sahin and A. Francillon, "Understanding and Detecting International Revenue Share Fraud," Network and Distributed System Security Symposium, 2021.