ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4):1-10

REVIEW ARTICLE

A Review on Real-time Suspicious Call Detection Systems in Telecom Networks

Sandeep Gupta*

Department of Computer Science, Samrat Ashok Technological Institute, Vidisha, Madhya Pradesh, India

Received on: 12-11-2025; Revised on: 10-04-2025; Accepted on: 02-05-2026

ABSTRACT

The rapid evolution of telecommunication networks, driven by digital transformation, has significantly improved connectivity, service quality, and accessibility. However, this growth has also increased vulnerability to fraudulent and nuisance calls, including spam, spoofing, robocalls, and voice phishing, which threaten user privacy, network reliability, and financial security. Traditional countermeasures, such as blocklists and rule-based filters, have proven insufficient against adaptive scam tactics that exploit Voice over IP infrastructures and social engineering techniques. Recent advancements in artificial intelligence (AI), machine learning, and large language models (LLMs) have enabled intelligent, real-time suspicious call detection systems capable of proactive intervention. Approaches such as conversational AI and LLM-based turn-by-turn analysis transcribe and evaluate live conversations, identifying suspicious linguistic cues, anomalies, and scam patterns. These systems issue immediate alerts, allowing users to terminate malicious calls before sensitive data or funds are compromised. Unlike pre-call or post-call methods, real-time AI-driven solutions provide adaptive, context-aware protection that evolves alongside emerging threats. This review explores telecom network architectures, AI-powered detection methods, and their advantages, offering insights into scalable, secure, and effective real-time spam call detection strategies for safeguarding modern communication infrastructures.

Key words: *Conversational AI*, large language models, machine learning, real-time call detection, spam call prevention, telecommunication networks

INTRODUCTION

The importance of communication services, especially the telecommunication services, is growing day by day as an integral part of the overall socio-economic development. Being a major part of the infrastructural base, the telecom industry has both direct and indirect implications on the economy. Over the recent decade, this sector has been a source of sizable investment and a competitive market, which has led to easy access to cheaper and faster telecom services for society at large. This increase in access and technological advancements has a direct impact on the day-to-day activities in areas such as e-governance, telemedicine, online learning, remote work access, financial inclusion, etc. Furthermore, there are indirect impacts through extensive linkages with multiple sectors and industries, such as financial services, machines, education, agriculture, etc.[1]

The integration of technology with telecoms has transformed the way communication networks function and offer services. Internet of Things (IoT) devices, which have sensors and communication capabilities, allow for the real-time capture and exchange of massive volumes of data. In telecommunications, this translates to better network management, more efficiency, and better client experiences. IoT enables proactive maintenance by monitoring network infrastructure, forecasting faults, and automating troubleshooting processes, resulting in reduced downtime and service disruptions.[2,3] Before the onset of digital transformation, telecom infrastructure was predominantly hardware-based, involving extensive use of copper wires, physical switches, and manual operations. Communication services were limited, with fixed-line telephony being the primary mode of connection. The industry was characterized by lengthy setup times, high operational costs, and limited scalability.[4]

Address for correspondence:
Sandeep Gupta
E-mail: sandeepguptabashu@gmail.com

In recent years, numerous news reports have highlighted the devastating impact of fraudulent phone calls, which have caused victims to suffer catastrophic financial losses. Unfortunately, such tragedies continue to occur at an alarming rate. The 2024 Global State of Scams Report reveals that phone scams siphoned $1.03 trillion globally over the past year, highlighting the severity of this issue. The harm caused by phone scams extends beyond financial loss.[5]

Fraud in the telecommunications industry has a serious impact on revenue and customer relationships, especially when losses continue to increase over time. As the telecommunications industry advances, the problem of telecommunications fraud has also grown in recent years. Telecommunications companies often experience huge financial losses due to fraud incidents caused by their services, and this makes the importance of fraud detection to reduce the impact of this risk. Fraud on telecommunications can be divided into several types, and the most typical is accessing calls using the original customer account to make fraudulent calls. Imagine an unknown call from a local number, and that from a friend or family member who lives abroad. It is really strange to receive international calls from a local number; this is essentially a form of fraud.[6] Current technology has provided protection against various attacks, but not many are designed to detect complex fraud operations. When using Voice over IP (VoIP), several problems in security and quality of service will arise; the VoIP infrastructure must be equipped with a security shield to protect itself from various forms of security threats.

Artificial intelligence (AI) and machine learning (ML) have multiple uses within the telecom industry, from analyzing data to predicting outages before happen, optimizing them for peak performance, and adapting in real time to changing conditions.[7] As AI technology has evolved, its applications in telecom have expanded. AI is now central to 5G networks, showing the growing role of AI in future telecom systems. One central area where AI has significantly impacted is detecting network anomalies.[8,9] ML technologies have become an effective weapon in the fight against telecom fraud nowadays.[10] The development of intelligent systems that can learn from data is now possible thanks to ML techniques. ML algorithms have the ability to analyze an enormous amount of data, and using ML-based classification or clustering allows for assessing malicious actions and protecting revenues.

ML is a method of data analytics and a branch of artificial intelligence that permits the machine to learn from the data on its own and to make and perform decisions, or predictions. Over the past few years, ML is widely gaining its popularity in manufacturing for material property prediction,[1-3] distortion and failure predictions, smart manufacturing,[4-6] natural language processing (NLP), and object recognition. With the increase in technological advancements in sensors and other electronic devices components, the machines are now observed and equipped with various sensors and communication devices, which have shown significant potential to improve the process, reduce the operational times, enhance the product quality and improve the level of automation.

Structure of the Paper

This paper structure is organized as follows: Section II explains the architecture and advantages of telecommunication networks. Section III covers foundational concepts in suspicious call detection. Section IV presents AI-driven detection techniques, including conversational AI and large language models (LLMs)-based systems. Section V discusses prevention strategies and algorithms. Section VI concludes the paper, and Section VII outlines future work direction.

TELECOMMUNICATION NETWORK ARCHITECTURE AND OPERATIONS

Telecommunication networks enable seamless voice, video, and data communication across layered infrastructures, including user, access, and core networks. Routing and signaling protocols ensure efficient session management, while challenges such as fraud, high-volume data, and protocol vulnerabilities necessitate robust monitoring and advanced operational frameworks for reliable and secure network performance.

Architecture of Telecommunication Networks

The architecture of telecommunication networks provides a structured framework for seamless communication across devices and services. It

typically consists of multiple layers: the user layer, access networks, and core networks, each with a specific role. The user layer includes internet users, telephone and mobile subscribers, and video service consumers. The service bearer layer comprises public and private networks, such as IP networks, PBX systems, and firewalls, supporting data transmission.[11] Access networks, like metropolitan area networks and public transport systems, connect users to the core network, which handles high-speed routing, switching, and data management. The figure illustrates this layered architecture, showing the flow from end users through access networks to the core network and the interactions among IP networks, telephone and mobile networks, and video conferencing systems.

- User layer: This layer represents end-users and their devices, including internet users accessing online services, fixed-line and mobile telephone subscribers, and participants in video conferencing systems. It focuses on the consumption of network services.
- Service bearer layer: This layer provides connectivity and service support for applications. It integrates technologies such as IP networks with routers, switches, and firewalls for internet access; PSTN for traditional telephony; mobile networks with base stations for cellular communication; and video conferencing systems with servers and gateways for real-time media transmission.
- Transport layer: This backbone layer ensures reliable and efficient transmission of data across the network. It includes access networks (Digital Subscriber Line, fiber, and cellular access), metropolitan area networks, and the high-capacity core network responsible for routing, switching, and interconnecting all services. This layer supports voice, video, and data traffic across heterogeneous networks.

These layers form a cohesive telecommunication network that efficiently connects end-users, supports diverse services, and ensures reliable data transport across the system.

Routing and Signaling in Telecommunications

Routing and signaling are fundamental processes in telecommunication networks, enabling the reliable delivery of voice, video, and data services across complex infrastructures.[13] Routing involves determining the optimal path for a call or data packet from the source to the destination, taking into account network topology, congestion, bandwidth availability, and quality of service requirements. Efficient routing ensures minimal latency, high call quality, and optimal utilization of network resources.

Signaling refers to the exchange of control information between network elements to establish, manage, and terminate communication sessions. Unlike the actual media traffic, signaling messages carry instructions that coordinate network operations, including call setup, routing decisions, and service provisioning.[14] Traditional telephony networks primarily use Signaling System No. 7 (SS7), which supports call management and supplementary services. In contrast, modern IP-based networks utilize protocols such as Session Initiation Protocol (SIP) and H.323 for VoIP and multimedia communications, offering greater flexibility and scalability.

Together, routing and signaling protocols form the backbone of telecommunication networks, ensuring seamless connectivity, proper resource allocation, and interoperability across different network types and technologies.

Challenges in Telecommunication Networks

Telecommunication networks face several critical challenges that impact performance, security, and the ability to detect suspicious activities in real time. The most significant challenges include:

- Fraudulent activities and call spoofing: Unauthorized or malicious calls, including vishing and SIM box fraud, compromise network integrity and pose financial and reputational risks to operators.[15]
- High volume and real-time data processing: Telecom networks generate massive amounts of call data (CDRs, signaling messages), making real-time monitoring and anomaly detection computationally intensive.
- Protocol vulnerabilities: Legacy protocols such as SS7 are susceptible to security exploits, enabling attackers to manipulate call routing or eavesdrop on communications.
- Integration of heterogeneous networks: Modern networks combine PSTN, mobile, and VoIP systems, creating interoperability

challenges and complicating consistent monitoring of suspicious activities.
- Latency and network congestion: Efficient routing and resource allocation are critical; delays or congestion can hinder the performance of real-time detection systems and affect call quality.

These challenges underscore the need for advanced analytics, ML-based monitoring, and robust network security frameworks to ensure reliable and secure telecommunications operations.

FOUNDATIONAL CONCEPTS IN SUSPICIOUS CALL DETECTION

Suspicious call detection in telecommunication networks involves understanding the nature, characteristics, and behaviors of fraudulent or nuisance calls. Foundational concepts include the classification of call types (spam, vishing, robocalls, recorded, and silent), identification of relevant data sources such as CDRs and signaling information, and monitoring techniques for detecting anomalies. Modern approaches integrate AI, ML, and real-time analysis to ensure adaptive, accurate, and proactive detection, thereby protecting users and maintaining network integrity.

Classification of Suspicious Calls

Suspicious calls represent a major concern in modern telecommunication networks, as they disrupt user trust, compromise privacy, and exploit network resources for fraudulent or malicious purposes. Unlike legitimate communications, these calls often rely on deception, automation, or manipulation of signaling protocols to achieve their objectives. They may range from unsolicited marketing attempts to sophisticated fraud schemes designed to extract sensitive information or cause large-scale service disruptions. To better understand their impact, suspicious calls can be classified into the following categories:

- Spam calls: Spam calls are unsolicited communications often linked to telemarketing, fraudulent promotions, or phishing attempts. They target a large number of users simultaneously, creating both inconvenience and security risks.[16] Beyond wasted time and annoyance, these calls may trick recipients into revealing sensitive data or making unauthorized payments, making them one of the most prevalent forms of telecom fraud.
- Vishing (Voice Phishing): Vishing involves deceptive calls that exploit human psychology through social engineering techniques. Attackers often impersonate legitimate organizations such as banks,[17] government agencies, or service providers, persuading victims to disclose personal or financial information. Unlike generic spam, vishing calls are highly targeted and may involve convincing narratives, making them harder to detect without advanced monitoring tools.
- Robocalls: Robocalls are automated calls initiated by autodials and typically deliver pre-recorded or synthetic messages. They can serve legitimate purposes such as appointment reminders or emergency alerts, but their misuse for fraudulent schemes has become widespread. Malicious robocalls often employ spoofed caller IDs and are placed at a massive scale,[18] overwhelming networks and deceiving recipients into engaging with fraudulent campaigns.
- Recorded calls: Recorded calls broadcast pre-prepared messages in bulk, commonly for marketing or fraudulent purposes. These calls exploit VoIP and Internet telephony infrastructure due to its low cost and scalability. In malicious contexts, recorded calls are designed to mislead users into purchasing illegitimate products, sharing personal details, or engaging with financial scams.[19] Their repetitive and intrusive nature makes them a persistent nuisance for users.
- Silent calls: Silent calls are abandoned or empty calls in which recipients hear no audio. While sometimes accidental, they are frequently generated deliberately using autodials to overwhelm users and network infrastructure. In severe cases, silent calls are weaponized as part of denial-of-service (DoS) attacks against telecom systems, reducing service quality and availability. Their ambiguity – whether nuisance or malicious – makes them especially challenging to monitor and classify.

A comprehensive understanding of these categories is crucial for developing effective real-

time detection mechanisms, enabling telecom operators to safeguard users, maintain service quality, and strengthen network resilience against evolving threats.

Call Data Sources and Monitoring

The effectiveness of suspicious call detection relies on diverse data sources and systematic monitoring. These provide the necessary foundation for recognizing abnormal call behaviors, identifying fraudulent activities, and supporting real-time threat detection in telecom networks.

- Call detail records (CDRs): CDRs log essential details such as caller and receiver IDs, call duration, timestamps, and routing paths.[20] Analyzing these records helps reveal unusual calling patterns, frequent short-duration calls, or abnormal routing, which may indicate spam, fraud, or spoofing attempts.
- Signaling data: Generated during call setup, routing, and termination, signaling data from protocols such as SS7 and SIP provides control information. Monitoring this data can expose irregularities such as spoofed caller IDs, unauthorized routing manipulations, or abnormally high call attempts in short intervals.
- Real-time monitoring: Advanced telecom infrastructures deploy systems that analyze call data streams as they occur.[21] These monitoring frameworks integrate anomaly detection algorithms and traffic filtering to flag suspicious activity instantly, reducing reliance on historical records and enabling proactive responses.
- Behavioral indicators: Beyond structural records, behavioral analysis considers usage trends such as call frequency, time-of-day patterns, and sudden deviations in user activity. These insights help differentiate between legitimate high-volume usage and potential fraudulent or automated calling schemes.

In combination, these data sources provide telecom operators with a layered approach, ensuring accurate detection of suspicious activities and maintaining network security.

Techniques for Suspicious Call Detection

Suspicious call detection techniques leverage advanced AI-driven methods to identify and mitigate fraudulent, spam, and scam calls before they impact users. Modern systems integrate ML, NLP, and real-time monitoring to address the limitations of traditional static approaches, such as blocklists or rule-based filtering.[22] By combining multiple detection frameworks, these methods provide adaptive, context-aware protection for telecom networks and subscribers.

AI-based cybersecurity systems

AI plays a critical role in preventing scam calls and protecting users from fraudulent activities. AI-based systems can automatically detect key threats, generate mitigation strategies, and respond in real time, even to novel attack patterns that traditional human monitoring might miss.[23] The adaptability and automated capabilities of AI make it particularly effective in dynamic telecommunication environments where threats constantly evolve.

VoIP spam detection

Detection of spam in VoIP networks requires a multi-layered approach, as no single technique is sufficient. At different stages, spam calls are filtered or quarantined based on the specific detection method applied.[24] Protocols such as SIP and Secure Real-Time Transport Protocol secure voice communication, but attackers with basic network knowledge can intercept SIP messages and RTP streams, making layered detection essential.

Kernel-based online anomaly detection (KOAD)

The KOAD technique does not assume predefined models for normal or abnormal behavior. Instead, it incrementally builds a flexible dictionary representing typical network activity. When deviations occur, the system triggers an alert immediately. The dictionary adapts over time, removing outdated patterns, which allows the algorithm to detect anomalies while accommodating evolving traffic behavior.

Pattern recognition and known scam numbers

AI-driven NLP algorithms analyze call content or messaging traffic to detect fraudulent attempts.[25] By identifying suspicious keywords, phrases, or previously reported scam numbers, these systems

can proactively flag high-risk calls. Continuous monitoring of behavioral and contextual indicators enhances detection precision, reducing false positives and improving overall system reliability.

Conversational AI-based detection

Conversational AI models are trained on large datasets of spam and legitimate calls to detect suspicious activity automatically.[26] With user permission, these systems can transcribe calls in real time, analyze content for scam indicators, and even interact with the caller using AI agents. This reduces user exposure to fraud and allows adaptive learning as scammers change tactics.

LLM-based real-time spam call detection

LLM-based systems provide turn-by-turn monitoring of live conversations.[27] Speech is converted to text and analyzed for suspicious keywords, conversational anomalies, and contextual cues. The system issues immediate alerts upon detecting threats, allowing users to terminate calls before sensitive information is disclosed. Unlike pre-call blocking or post-call analysis, this method provides proactive, context-aware protection during the interaction itself.

APPLICATIONS OF SUSPICIOUS CALL DETECTION SYSTEMS IN TELECOM NETWORKS

Suspicious call detection systems play a critical role in enhancing the security, reliability, and efficiency of telecommunication networks. Their applications extend across multiple areas of telecom operations, combining technical and user-centric benefits.

- Fraud prevention: Detection systems help prevent a wide range of fraudulent activities, including SIM box fraud, caller ID spoofing, and voice phishing. Real-time monitoring enables telecom operators to block or quarantine suspicious calls before they reach end-users, minimizing financial and reputational risks.[28]
- Spam and Robocall mitigation: Automated spam filtering and robocall detection reduce the volume of unsolicited calls reaching subscribers. This protects users from scams, phishing attempts, and intrusive marketing campaigns, while preserving their trust and satisfaction.
- Network protection and service continuity: Detection systems monitor signaling traffic and call patterns to identify anomalies such as sudden spikes in call attempts or silent call floods. This protects network infrastructure from overloads, DoS attacks, and other disruptions, ensuring continuous service availability.
- Regulatory compliance and user safety: Many regions mandate the deployment of systems to detect and mitigate spam, fraudulent, and nuisance calls. Detection systems enable operators to comply with such regulations, safeguard sensitive customer information, and maintain transparent communication practices.
- Operational efficiency and resource optimization: By filtering malicious or high-risk calls, these systems reduce unnecessary network load, improving routing efficiency and call quality. This allows operators to allocate resources effectively and enhance overall network performance.

In practice, the integration of suspicious call detection systems ensures that telecom networks remain resilient, secure, and user-friendly. Figure 1 illustrates the underlying telecommunications network architecture that supports such systems.
Work, typically using web services. Most modern web APIs comply with the REST architectural style, being referred to as RESTful web APIs. RESTful web APIs provide access to data and services by means of create, read, update, and delete (CRUD) operations over resources (e.g., a video in the YouTube API or a playlist in the Spotify API). RESTful APIs are ubiquitous in the modern-day society: public institutions such as the American government[3] expose their existing assets as a set of RESTful APIs; software companies such as Microsoft[29] and Netflix[30] base many of their systems communications on their RESTful APIs; even non-software companies such as Marvel[28] provide APIs for developers to build applications on top of them. The importance and pervasiveness of web APIs are also rejected on the size of popular API repositories such as ProgrammableWeb and RapidAPI, which currently index over 24K and 30K APIs, respectively.

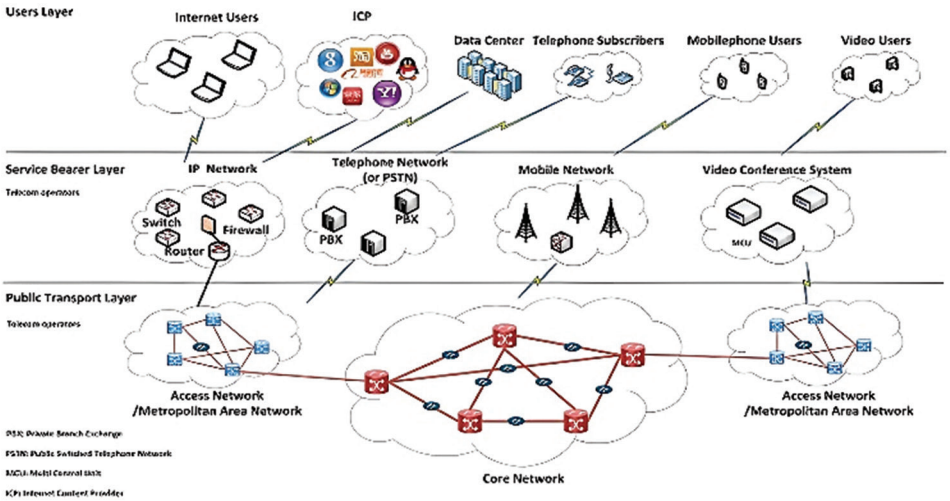

Figure 1: Telecommunications network architecture[12]

LITERATURE REVIEW

This section presents a literature review on real-time suspicious call detection systems. It examines various methods and technologies used to detect and prevent fraudulent calls, highlighting approaches that improve detection accuracy, system efficiency, and overall user security in telecom networks.

Tiwari and Pratap (2025) are developing a fraud call detection site to combat the pervasive threat of fraudulent calls. The site uses advanced technologies such as ML and anomaly detection to accurately identify and block fraudulent calls in real-time. The project includes extensive research on detection methodologies, a user-friendly interface for reporting suspicious activities, and robust algorithms to enhance detection accuracy. The goal is to reduce financial fraud incidence, protect potential victims, and contribute to a safer communication environment. The outcomes of this project are expected to offer valuable insights and practical solutions in the ongoing battle against fraud in the telecommunications sector.[29]

Varma *et al.*, (2025), highlight the importance of fraud detection in securing communication networks and protecting users from malicious activities. By combining cybersecurity techniques and ML algorithms, they can effectively detect and reduce fraud-related activities in real-time. ML models analyze patterns, behaviors, and anomalies for incoming calls, including call metadata, voice features, and interaction history. The existing model has an accuracy of 90%, which can be improved by 3% to 5% or more through advanced techniques and optimizations like hybrid algorithm approaches, feature engineering, and deep learning models.[30]

Durga Bhavani *et al.* (2024) highlight the need for AI-driven solutions to detect and prevent fraudulent calls. Traditional methods, such as rule-based algorithms and static blacklists, have been ineffective in detecting sophisticated fake calls. Instead, AI-driven solutions can improve user safety and confidence by quickly and reliably detecting and mitigating fraud. By analyzing call patterns, voice features, and contextual data in real-time, AI-driven solutions can react swiftly to new fraud strategies, ensuring the safety and security of users. This approach can help prevent financial losses and security breaches associated with sophisticated fraud.[31]

Nicholas and Ng (2024) study introduces a fine-tuned LLM for detecting scam calls in response to the increasing severity of telecommunication fraud in Singapore. The approach enhances scam detection capabilities by strategically augmenting datasets with generative AI. The augmented dataset is used to fine-tune pretrained LLMs, including GPT-2 and Llama. Experiments show that the fine-tuned LLM outperforms traditional models in inference accuracy while maintaining acceptable inference times, making it a practical tool for real-time scam detection.[32]

Malhotra, Arora, and Bathla, (2023), highlight the growing concern of fraudulent calls in the telecommunication industry, causing millions of global financial losses annually. AI and ML have emerged as powerful tools for detecting and analyzing these calls. Their study proposes a novel fraud call detection approach that

Table 1: Literature review on real-time suspicious call detection systems in telecom networks

References	Study on	Key findings	Challenges	Limitations	Future work
Tiwari and Pratap (2025)	Fraud call detection site	Real-time fraud detection using ML and anomaly detection; user-friendly reporting interface	Handling evolving fraud patterns	Limited large-scale evaluation; potential false positives	Improve detection with hybrid ML algorithms and wider deployment
Varma *et al*., (2025)	ML-based fraud call detection	ML models (decision trees, SVM, Neural Networks) analyse metadata and voice features; 90% accuracy	Complex fraud patterns; computational cost	Accuracy varies with dataset quality	Boost accuracy by 3–5% with hybrid algorithms and feature engineering
Durga Bhavani *et al*., (2024)	Evolution of fraud call detection	AI/ML and NLP detect sophisticated fraud; adapt to new strategies	Integrating AI in real-time, zero-day fraud	Legacy systems fail for complex fraud	Develop adaptive AI with continuous learning
Nicholas and Ng (2024)	LLMs for scam calls detection	Fine-tuned LLMs outperform ML/DL models in accuracy; dataset augmentation improves context	Cultural specificity; inference time	High computational needs; limited generalizability	Optimize LLMs for real-time detection globally
Malhotra, Arora and Bathla (2023)	AI-based fraud/spam calls detection	AI/ML achieves high accuracy; insights into fraud tactics	Real-time adaptation; data privacy	Limited scalability; dataset coverage	Incorporate adaptive ML models with larger datasets
Brijith (2023)	AI for scam calls	CNN and AI improve detection; highlights social engineering	Detecting socially engineered calls; integration with regulations	Limited live network evaluation	Combine AI with awareness campaigns and advanced DL

AI: Artificial intelligence, ML: Machine language, CNN: Convolutional neural networks, DL: Deep learning, SVM: Support vector machine, NLP: Natural language processing, LLMs: Large language models

achieves high accuracy and precision, identifying potential indicators of frauds or spams. The analysis provides insights into fraudsters' tactics and methods, which can be used to develop countermeasures, enhancing the overall security of the telecommunication industry.[33]

Brijith, (2023) highlights the growing issue of scam calls in the telecommunications industry, affecting both revenue and service quality. The paper emphasizes the need for reliable fraud detection algorithms, including the convolutional neural networks algorithm, public awareness, regulatory measures, and global cooperation. It also highlights the pivotal role of AI in combating scam calls. While scams may persist and adapt, the collaborative effort to leverage AI and other cutting-edge tools is a robust defense against this contemporary threat. The ongoing strides in technological advancements bring closer to a future devoid of scam calls, highlighting the collective resolve to safeguard individuals and society from this pervasive danger.[34]

Table 1 provides a structured overview of key research on real-time suspicious call detection systems, summarizing study focus, major findings, challenges, limitations, and contributions.

CONCLUSION AND FUTURE WORK

Real-time suspicious call detection has become an essential component of modern telecommunication security as fraud tactics grow more sophisticated and adaptive. The rapid shift from traditional rule-based filtering to AI-driven, context-aware detection methods demonstrates how critical ML, NLP, and LLMs have become in safeguarding users and networks. Existing research highlights strong progress – such as improved anomaly detection, conversational analysis, and LLM-based turn-by-turn monitoring – yet challenges remain in ensuring scalability, handling zero-day fraud patterns, reducing false positives, and integrating solutions across heterogeneous telecom infrastructures. The reviewed studies consistently show that combining behavioral analytics, voice features, call metadata, and linguistic cues significantly enhances detection accuracy. However, successful deployment in live networks requires continuous learning mechanisms capable of adapting to evolving fraud strategies. Real-world constraints such as computational cost, dataset variability, cultural context, and privacy concerns still limit the widespread adoption of advanced AI systems.

Future work can focus on several promising directions. First, hybrid AI architectures – combining classical ML, deep learning, and LLM-based inference – should be explored to improve robustness and reduce latency during real-time call monitoring. Second, expanding high-quality, multilingual, and culturally diverse training datasets can improve generalizability across global telecom environments. Third, privacy-preserving AI techniques such as federated learning and encrypted inference may enable

secure data processing without compromising user confidentiality. Finally, there is growing potential for integrating conversational AI agents directly into telecom networks to interact with suspicious callers, gather signals, and minimize user exposure to scams. Advancements in these areas will support the development of scalable, intelligent, and proactive detection systems capable of protecting billions of users as telecommunication fraud continues to evolve.

REFERENCES

1. Karonnon P, Rajeev M. The Role of Telecommunication Service Sector in Indian Economy-an Analysis of Output and Employment Linkages. Karnataka: Institute for Social and Economic Change; 2023.
2. Dodda S, Kamuni N, Nutalapati P, Vummadi JR. Intelligent Data Processing for IoT Real-Time Analytics and Predictive Modeling. In: 2025 International Conference on Data Science and its Applications (ICoDSA); 2025. p. 649-54.
3. Illakya T, Keerthana B, Murugan K, Venkatesh P, Manikandan M, Maran K. The Role of the Internet of Things in the Telecom Sector. In: 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT). IEEE; 2024. p. 1-5.
4. Manda JK. Digital Transformation Impact on Telecom Infrastructure: Analyzing the implications of digital transformation initiatives on telecom infrastructure and operational strategies, based on your experience in digital transformation projects. SSRN Electron J 2024;5:5-17.
5. Shen Z, Yan S, Zhang Y, Luo X, Ngai G, Fu E. It warned me just at the right moment: Exploring LLM-based Real-time Detection of Phone Scams. 2025.
6. Abdul Jabbar M, Suharjito S. Fraud detection call detail record using machine learning in telecommunications company. Adv Sci Technol Eng Syst 2020;5:63-9.
7. Thangavel S, Srinivasan S, Naga SB, Narukulla K. Distributed machine learning for big data analytics: Challenges, architectures, and optimizations. Int J Artif Intell Data Sci Mach Learn 2023;4:18-30.
8. Chandra Bikkasani D. Data Science and Machine Learning for Network Management in Telecommunication Systems: Trends and Opportunities. 2024.
9. Rahul Dattangire AJ, Vaidya R, Biradar D. Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality. In: 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET). IEEE; 2024. p. 1-6.
10. Majumder RQ. Machine learning for predictive analytics: Trends and future directions. Int J Innov Sci Res Technol 2025;10:3557-64.
11. Debbabi F, Jmal R, Fourati LC, Aguiar RL. An overview of interslice and intraslice resource allocation in B5G telecommunication networks. IEEE Trans Netw Serv Manag 2022;19:5120-32.
12. Qian F, Ye Y, Shan N, Su B. A novel architecture of telecommunication networks for next generation internet. MATEC Web Conf 2018;173:03036.
13. Kapadia HP. Voice and conversational interfaces in banking web apps. J Emerg Technol Innov Res 2021;8:g817-23.
14. Shah V. Analyzing traffic behavior in IoT-cloud systems: A review of analytical frameworks. Int J Sci Res Comput Sci Eng Inf Technol 2023;9:877-85.
15. Verma V. Deep learning-based fraud detection in financial transactions: A case study using real-time data streams. ESP J Eng Technol Adv 2023;3:149-57.
16. Shah SB. Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection. In: 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE; 2025. p. 1-7.
17. Patel D. Enhancing banking security: A blockchain and machine learning- based fraud prevention model. Int J Curr Eng Technol 2023;13:576-83.
18. Akinyemi BO, Odukoya OH, Sanni ML, Sewagnon G, Aderounmu GA. Performance evaluation of machine learning-based robocalls detection models in telephony networks. Int J Comput Netw Inf Secur 2022;14:37.
19. Kali H. Optimizing credit card fraud transactions identification and classification in banking industry using machine learning algorithms. Int J Recent Technol Sci Manag 2024;9:85-96.
20. Zhao Q, Chen K, Li T, Yang Y, Wang X. Detecting telecommunication fraud by understanding the contents of a call. Cybersecurity 2018;1:8.
21. Xu L, Shao G, Cao Y, Yang H, Sun C, Zhang T. Research on telecom big Data Platform of LTE/5G Mobile Networks. In: 2019 IEEE International Conferences on Ubiquitous Computing \& Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS); 2019. p. 756-61.
22. Prajapati N. The role of machine learning in big data analytics: Tools, techniques, and applications. ESP J Eng Technol Adv 2025;5:16-22.
23. Prajapati V. Enhancing threat intelligence and cyber defense through big data analytics: A review study. J Glob Res Math Arch 2025;12:1-6.
24. Gupta S. An intelligent system for identifying fraud phone calls using machine learning algorithms. J Glob Res Electron Commun 2025;1:.
25. Rao KM, Patel B. Suspicious Call Detection and Mitigation Using Conversational AI. Defensive Publications Series; 2023.
26. Karri SB, Gawali S, Rayankula S, Vankadara P. AI Chatbots in Banking: Transforming Customer Service and Operational Efficiency. 2025.
27. Ande BR. A unified optimization framework for large language models in enterprise applications using python. J Comput Anal Appl 2024;33:2111-22.
28. Malali N. Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in

Finance. In: 2025 International Conference on Advanced Computing Technologies (ICoACT). IEEE; 2025. p. 1-6.
29. Tiwari V, Pratap A. Fraud Call Detection using Pre-Data Feeding Method by Financial Institution. In: 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN); 2025. p. 990-993.
30. Varma GA, Kumar DH, Ankitha G, Rahul G, Varma B, Kumar AB. Enhanced fraud call detection through cybersecurity and machine learning integration. Int J Res Public Rev 2025;6:16935-41.
31. Durga Bhavani B, Nikitha U, Nandini P, Reddy Gogu N, Student UG. Artificial intelligence based fake or fraud phone calls detection. J Educ Teach Trainers 2024;15:318-27.
32. Nicholas PY, Ng PC. ScamDetector: Leveraging Fine-Tuned Language Models for Improved Fraudulent Call Detection. In: TENCON 2024 - 2024 IEEE Region 10 Conference (TENCON); 2024. p. 422-5.
33. Malhotra S, Arora G, Bathla R. Detection and Analysis of Fraud Phone Calls using Artificial Intelligence. In: 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON); 2023. p. 592-5.
34. Brijith A. Unmasking Scam Calls: Analysing and Detecting Scammers using AI; 2023. AQ8

Author Queries???
AQ8: Kindly provide complete reference