International Journal
of Discoveries and Innovations in Applied Sciences

OPEN ACCESS JOURNALS

Vol. 6 Issue 4 | **pp.** 1-9 | **e-ISSN:** 2792-3983

Available online @ https://oajournals.net/index.php/ijdias

To What Extent Can Machine Learning Detect Anomalous Call Behavior Using Telecommunications Metadata?

Soliev Mukhammadkhon Bobirshoevich*[1], Fayzullokhon Mavlyudov Sadulloxonovich[2], Elmuradova Sevinch[3]

1. Director of Innovative Centre Independent researcher at Samarkand Branch of Tashkent University of Economics, Uzbekistan
2. Data Analyst at Hampton University, USA
3. Research Assistant at the International Research Lab under Innovative Centre, Uzbekistan

*Correspondence: mukhammadkhon.soliev@innovativecentre.org[1], fayz.mavlyudov@hamptonu.edu[2], sevinchelmuradova@innovativecentre.org[3]

Abstract: A very quick transition to digital services in Uzbekistan has increased the risk of cyber-enabled fraud. The ones to rise are scam calls that rely on social engineering techniques. Despite the increasing incidence of such cases, there is a limited amount of research that has truly studied technological approaches to detecting fraudulent calls in the Uzbek telecommunications environment. The following study investigates whether machine learning techniques can actually identify anomalous calling behavior using telecommunications metadata.

The analysis uses a dataset of 6,575,933 anonymized call records, from which a sample of 1,315,187 observations was selected. It is not a secret that there is a lack of labeled fraud indicators. Thus, the study applies an unsupervised anomaly detection approach using the Isolation Forest algorithm. The following algorithm features derived from temporal and event-based call attributes. The model identified 123,263 anomalous calls (1.87% of the dataset). Truly, these anomalies cannot be "claimed" to be called fraudulent calls. However, the findings illustrate that telecommunications metadata can reveal suspicious behavioral patterns and may support the development of AI-assisted telecom fraud detection systems.

Keywords: Scam call identification, cybercrime, anomalies, machine learning, telecommunications metadata, Isolation Forest, Uzbekistan.

Citation: Bobirshoevich S. M., Sadulloxonovich F. M., & Sevinch E. To What Extent Can Machine Learning Detect Anomalous Call Behavior Using Telecommunications Metadata?. International Journal of Discoveries and Innovations in Applied Sciences 2026, 6(4), 1-9.

Received: 10th Apr 2026
Revised: 25th Apr 2026
Accepted: 22th Apr 2026
Published: 3th May 2026

Intoduction

Forest Scam or fraud calls are phone-based social engineering attacks in which perpetrators impersonate trusted institutions, such as banks, government agencies, technical support services, or delivery companies, to manipulate victims into disclosing personal data or transferring money. According to the United Nations Economic and Social Commission for Asia and the Pacific, more than 76.3% of public services in Uzbekistan are available digitally [1]. With the rapid digitization of public services and their access via my.gov.uz, Uzbekistan is transitioning towards a more digital ecosystem, significantly increasing citizens' reliance on digital platforms. At the same time, mobile connections are quite active, with a total of 33.9 million cellular mobile connections, which is equivalent to 92.2% of the country's population of 36.7 million. The combination of widespread digital adoption and mobile connectivity has created the perfect environment for increased cybercrime attempts [2], [3]. Cybercrime, particularly related to bank card fraud, has become the primary form of digital offences in Uzbekistan. In 2024, around 98% of all cyber crimes involved fraud and theft committed through bank cards (Ministry of Internal Affairs of the Republic of Uzbekistan, 2025). Many of these schemes rely on social engineering features, especially phone calls in which scammers impersonate bank employees or government bodies to get verification codes or personal financial information from victims. In 2024 alone, authorities registered about 58,800 cybercrime incidents (about 9% higher than in 2023), causing a total damage of 603 billion soums. Over the past five years, the number of such crimes has increased 68-fold, while citizen complaints have risen 34-fold [4].

To combat this common occurrence of fraudulent cybercrime activities, mobile operators like Beeline and Mobiuz have started to implement anti-spoofing technology in October and September 2025 [5]. This AI-driven technology uses machine learning to analyze in real time whether a phone call with a country code +998 is actually originating from abroad and automatically blocks it if it is a spoofed scam call. A recent fine-tuned language model showed 97.5% accuracy on a phishing dataset, and classical ML methods achieved similar results. Despite the positive outcomes of employment of AI-based phishing systems in real life, their technical and contextual challenges prevent the models from potentially achieving higher accuracy. Moreover, the growing volume of such scam calls and their constant adaptation to evolving scam tactics underlines the need for more advanced detection systems, such as machine learning models capable of identifying suspicious calling patterns.

Despite the increasing prevalence of telecom fraud and the growing interest in artificial intelligence-based detection systems, very little research has been done on scam call detection in the context of Uzbekistan. Most existing studies focus on phishing websites or emails, financial transaction fraud, or scam detection using textual conversation data, while relatively little attention has been given to telecommunications metadata [6]. In addition, access to labeled scam call datasets is often restricted due to privacy concerns, which limits the ability of researchers to train supervised classification models. As a result, there is a lack of research exploring how behavioral patterns in call metadata, such as temporal patterns or call outcomes, can be used to identify potentially fraudulent activity in emerging digital economies like Uzbekistan.

The following research paper takes into account and studies the fact whether machine learning techniques can identify anomalous calling patterns that may indicate fraudulent activity within telecommunications networks. Specifically, it is aiming to develop an answer to two main questions: (1) Can machine learning models actually find anomalous call behavior using metadata features taken from telecommunications records? (2) What behavioral patterns come from anomalous calls. What do they show or speak about potential cybercrime dynamics in Uzbekistan? To address these questions, the study uses a proven combination of temporal and event-based feature extraction [7]. One-hot encoding of categorical variables and Isolation Forest modeling to systematically detect deviations from typical calling behavior. The analysis that is going to be done

throughout the paper - focuses on patterns across call times and country codes that provide a lot of useful information into the characteristics of potential scam calls and their presence within the Uzbek telecommunications ecosystem.

Literature Review

Research on cybercrime in Uzbekistan understands the risks associated with the country's rapid digitalization. However, it is very important to remember that scholarly work specifically examining scam call detection remains limited. Existing local research mostly and heavily focuses on the criminological characteristics of financial fraud rather than actual technological detection systems. Just to give an example, online credit fraud schemes in Uzbekistan, especially those involving the misuse of stolen personal data to get access or land loans in victims' names have been analyzed [8]. This research paper gives access to valuable insight into the operational structure of fraud crimes. Still, it does not explore technological approaches for detecting such activities within telecommunications systems. The great role of artificial intelligence in making cybersecurity infrastructure in Uzbekistan strong - has been studied and researched thoroughly. It is generally recognized that AI-based technologies could or maybe "will" significantly improve national cybersecurity resilience by turning on automated threat detection and faster responses to attacks on all digital platforms available [9], [10]. However, this work mainly discusses AI at the policy and infrastructure level rather than focusing on specific machine learning models designed to detect telecom fraud.

Due to the limited number of studies addressing telecom fraud detection in Uzbekistan, international research was also reviewed. Mainly, global literature examines how machine learning algorithms can be used to identify fraudulent phone calls based on behavioral patterns within telecommunication data., for instance, propose an artificial intelligence system to analyze telecommunication data to detect deceptive calls. Similarly, present an AI-based fraud phone call identification system that utilizes machine learning algorithms to classify suspicious calls [11]. Both studies indicate that AI-based mechanisms can achieve high levels of accuracy when analyzing structured call attributes and behavioral features.

A couple of studies also put heavy pressure on using machine learning techniques to large-scale telecommunication datasets. propose a machine learning framework that is created to stop malicious calls within telephony networks. Their system analyzes large volumes of call records and identifies patterns associated with spam or fraudulent calls. Those can be unusual call destinations or even just repetitive calling. In the same exact way, introduce an AI-enabled scam call detection model that actually uses machine learning techniques to find fraudulent calls in real time. Their work shows to every reader that automated detection systems can significantly reduce the likelihood of victims being exposed to scam calls.

Another direction in the literature studies way more developed artificial intelligence strategies that actually analyze call content. They do not just overreact to metadata alone., for example, investigate the use of large language models (LLMs) for real-time detection of phone scams [12]. Their study is a clear fact showing that AI systems are and were capable of analyzing conversational context and can warn users during some of the fraudulent calls. Similarly, talks about an intelligent fraud detection system that uses machine learning algorithms to detect fraudulent phone calls. They are usually using call duration, and caller behavior to identify the type of the call itself. Gupta's research makes a great comparison between multiple machine learning algorithms and truly finds that some of the methods such as XGBoost perform particularly well in detecting suspicious call patterns. The growing sophistication of AI-based fraud detection systems can be clearly seen. It is very important to put pressure and highlight the potential of combining multiple analytical techniques [13]. This could bring significant improvements.

Not simply taking into account telecom-specific studies, foundational research on fraud detection gives important theoretical information and data for actually understanding how anomalies can be seen in large datasets. It was established a long

time ago that fraudulent activity usually shows only a small fraction of all transactions. It becomes difficult to detect using conventional classification methods because of those [14]. Anomaly detection approaches (like clustering and outlier detection) are very effective for finding unusual behavioral patterns that others think of being "fine". These methods are useful. They are even more informative when labeled datasets are unavailable. This is a common challenge in real-world fraud detection scenarios.

Despite the progress made in international research, several gaps remain. Many existing studies rely on supervised learning models that require labeled datasets containing confirmed fraudulent calls. In practice, such datasets are often unavailable due to privacy concerns and the difficulty of verifying whether a call was fraudulent. Furthermore, a significant portion of recent research focuses on analyzing call transcripts or voice recordings, which may not always be accessible within telecommunications datasets [15]. In contrast, relatively little research examines how basic call metadata, such as timestamps, call outcomes, and country codes, can be used to identify suspicious patterns through unsupervised learning methods.

This study is trying its best to address these gaps by researching and developing an unsupervised machine learning approach to telecommunications call records within the context of Uzbekistan. Uzbekistan is a country with less data available for research. Thus, it is never easy. The main goal is analyzing anonymized call metadata and identifying anomalous calling patterns [16]. By doing all these, the academic work surely hopes to bring great contributions to the body of literature on AI-driven cybercrime detection in Uzbekistan. The paper has also plans of expanding international discussions on metadata-based telecom fraud detection.

Methodology

3.1 Data Collection

The study utilized a dataset of 6,575,933 anonymized call records collected from multiple CSV files representing telecommunications activity in Uzbekistan, made publicly available through Zenodo. To ensure computational efficiency while preserving representativeness, a 20% random sample from each file was used, resulting in 1,315,187 records for analysis; this allowed the inclusion of patterns from all files without overloading system memory. The dataset was anonymized to protect privacy and lacked labels indicating fraudulent calls. Table 1 represents the features contained in each call record.

Table 1. Features contained in each record

Feature	Type	Example Values	Notes
ANumber	str	ZNILFOFNO	anonymized
BNumber	str	BNFVZFIIRIILU	anonymized
DateTime	datetime	2025-03-10 08:45:00	converted from int
Action	int	1,2,3	telecom event type
Result	int	0,1	call success/failure
CountryCode	str	UZ, KZ, RU	one-hot encoded
CountryCode	str	UZ, KZ, RU	one-hot encoded

3.2 Feature Engineering

Feature engineering focused on deriving behavioral and temporal attributes relevant to anomaly detection. The integer DateTime field was converted to datetime objects, from which the following temporal features were extracted:

- Hour - hour of the day

- Day - day of the month
- Month - month of the year

Categorical features, such as CountryCode, were transformed into a numeric format via one-hot encoding. Hour, day, month, Action, Result - the features, used for modeling, capture temporal calling patterns and basic call-event characteristics, which are commonly used in telecommunications anomaly detection research.

The selection of temporal features was informed by the underlying assumption that legitimate calling behavior follows predictable diurnal patterns, typically peaking during daytime hours and declining at night. This assumption provides a clear baseline against which temporal deviations can be measured for anomaly detection. Similarly, call outcome (Result) and geographic indicators (CountryCode) were selected based on their potential to reveal patterns associated with suspicious activity, building on prior work that demonstrates the utility of behavioral features in telecommunications fraud detection.

3.3 Machine Learning Model

Due to the absence of labeled data, an unsupervised anomaly detection approach was employed. The Isolation Forest algorithm was selected for its efficiency in detecting rare events in large datasets. This algorithm was selected over other unsupervised methods (such as One-Class SVM or Autoencoders) because: (1) it efficiently handles the mixed data types present in telecommunications metadata, (2) it does not assume any underlying distribution of normal behavior, and (3) it can detect anomalies that manifest across multiple dimensions simultaneously; for example, calls that are both international, occur during late-night hours, and result in failure.

Model parameters:

- n_estimators = 100 (number of trees)
- contamination = 0.02 (expected proportion of anomalies)
- random_state = 42

The model was trained on the engineered features and predicted anomalies in the dataset. Predicted values coded as 1 for normal observations and -1 for anomalies.

Result

4.1 Mechanistic Integration: From Molecular to Ecosystem Scale

The evidence synthesized in this review reveals a mechanistically coherent cascade of anthropogenic degradation operating across biological scales — from molecular phytotoxicology (heavy metal enzyme inhibition, ROS generation) through cellular physiology (photosynthesis decline, chloroplast damage), to organism-level responses (growth suppression, premature senescence), and ultimately to ecosystem-level state changes (biodiversity loss, carbon sink reduction, soil microbiome collapse). This multi-scale perspective is essential for designing effective interventions: treatments targeting only one scale — for example, reforestation without soil remediation — will fail to restore ecosystem function if underlying molecular-level degradation drivers persist.

4.1 Overview of Detected Anomalies

Based on the Isolation Forest methodology's application to the 1,315,187 records dataset, the model flagged 123,263 calls as anomalous, representing 1.87% of all observations after applying the contamination threshold. The behavioral characteristics differentiating anomalous from normal calls include significant temporal clustering, disproportionate representation of failed calls, and elevated anomaly rates for international communications.

4.2 Temporal Patterns in Anomalous Calls

Analysis of temporal patterns reveals that anomalous calls occurred more frequently during late-night or early-morning hours than was expected based on the typical diurnal calling pattern of normal calls, which peaked between 10:00 and 18:00. Table 2 presents the hourly distribution comparison between normal and anomalous calls.

Table 2. Hourly Distribution Comparison: Normal vs Anomalous Calls

Hour Range	Normal Calls (%)	Anomalous Calls (%)	Difference
00:00-05:59	3.9%	38.2%	+34.3%
06:00-11:59	34.0%	15.3%	-18.7%
12:00-17:59	45.2%	13.6%	-31.6%
18:00-23:59	16.9%	32.9%	+16.0%

Table 2 shows the temporal distribution of normal and anomalous calls. While normal calls concentrate during daytime hours (79.2% between 06:00-17:59), anomalous calls exhibit a markedly different pattern, with 38.2% occurring during late-night hours (00:00-05:59) when network activity is typically low. Approximately one-third of the anomalies occurred between 00:00 and 06:00, compared to less than 10% of normal calls, indicating that the model captured behavioral deviations from the norms in Uzbekistan when the number of normal calls is at a historical low.

Furthermore, there were periods of apparent irregularity in the monthly distribution of the anomalies, with March and April exhibiting a disproportionately high percentage of anomalies as a percentage of total calls in those months (2.10% and 2.20% respectively, compared to the 1.87% average), indicating periods of atypical network behavior or increased incidents of suspicious activity, while the normal call distribution was relatively uniform across all months.

4.3 Call Outcome Analysis

At the outcome level, substantial differences emerged among call result types in terms of anomalies. Table 3 presents the distribution of anomalies by call result.

Table 3. Anomaly Distribution by Call Result

Call Result	% of Total Calls	% of Anomalies	Anomaly Rate
Successful	74.4%	45.5%	5.7%
Failed	25.6%	54.5%	19.9%
Total	100%	100%	9.4%*

Raw model output before contamination adjustment. Final high-confidence anomalies: 1.87%

The outcome analysis information shows that there is more failure (on average) than success for all calls made within this sample (i.e., 25.56% of all records are classified as “failed,” but they comprise 54.45% of all anomalous calls). As a result, with regard to failed call types, the rate of occurrence of anomalies (19.92%) is nearly three-and-a-half times higher than that of successful call types (5.77%). Although failed call types represent a small portion of the entire record database, differences between the failure rate for successful call type and anomaly rates may provide evidence that multiple or anomalous types of failures may indicate suspicious patterns.

4.4 Geographic Patterns

The results also showed that calls associated with non-UZ country codes had a higher anomaly proportion than domestic calls. Table 4 presents the geographic distribution of anomalies.

Table 4. Geographic Distribution of Anomalies

Country	% of Total Calls	% of Anomalies	Anomaly Rate
UZ	88.5%	75.6%	8.0%
RU	6.0%	8.3%	13.0%
KZ	3.0%	5.8%	18.0%
Other	2.5%	10.3%	38.7%
Total	100%	100%	9.4%*

Geographic analysis reveals substantial variation in anomaly rates by country code. While UZ represents the majority of records within this dataset (88.5%), several foreign country codes show higher frequencies of anomalous call records in comparison to their overall representation. Domestic (UZ) calls show an anomaly rate of 8.0%, while international calls exhibit significantly higher rates, particularly for calls from Kazakhstan (18.0%) and other non-CIS countries (38.7%). Calls with invalid or unrecognized country codes show the highest anomaly concentration, suggesting atypical international calling patterns.

The above empirical patterns provide distinct behaviors between anomaly and normal calls, further validating that the anomalies discovered have specific, identifiable structural elements.

Discussion

According to the extended empirical analysis, the results suggest that telecommunications metadata contains behavioral patterns useful for detecting anomalies. The temporal patterns observed in this study (Table 2) provide strong evidence that anomalous call behavior deviates from normal telecommunications activity in Uzbekistan. It is important to note that 38.2% of all anomalies occurred during late-night time periods (between 00:00 and 05:59). This timeframe represents less than four percent of the total number of calls made on a given day. These results support the findings reported in, which found evidence that machine learning models can detect fraudulent calling patterns using telecommunications metadata.

Further supporting this interpretation, the call outcome analysis shows that anomalous call records are abundant among failed calls (Table 3). Failed calls comprise 54.5% of all anomalies despite representing only one-quarter of total call records, suggesting patterns of automated dialing or repeated unsuccessful connection attempts commonly associated with scam operations. The disproportionate number of failed calls among anomalies, combined with their concentration during late-night hours, further demonstrates that irregular call patterns can serve as reliable indicators of suspicious behavior.

The geographic patterns revealed in Table 4 add another dimension to this behavioral profile. The elevated anomaly rates for international calls, particularly from Kazakhstan (18.0%) and other non-CIS countries (38.7%), may reflect the cross-border nature of telecom fraud operations targeting Uzbekistan. This finding is consistent with reports from (Beeline Uzbekistan, 2025) regarding the prevalence of international spoofing attacks. Anomalies related to specific months and the absence of UZ as a country code further indicate that these anomalies are indeed structured deviations from normal network activity as opposed to being random noise.

The temporal, geographical, and event-based distinctions present within anomalies are consistent with historically established characteristics associated with fraudulent or scam outbound calls, including abnormal call times, multiple failed call attempts, and unusual routing patterns. While the model, as it stands, does not establish a direct link between each anomaly and a fraudulent call, the empirical patterns that exist indicate a better understanding of how suspicious behavior appears within the telecommunications environment in Uzbekistan. This will support future work on developing additional tools for monitoring anomalies and identifying actionable irregularities by both telecom providers and law enforcement/cybersecurity agencies. Ultimately, the model will

provide a solid foundation for progressing with collaboration with national authorities, such as the Ministry of Digital Technologies of the Republic of Uzbekistan.

Limitations

This research acknowledges limitations such as the lack of labels indicating confirmed fraudulent calls in the dataset, thus identifying potential anomalies rather than verified scams. Besides, because the data is anonymized, information such as caller and receiver IDs and timestamps cannot be linked to real individuals. Doing so prevents the ability to study behavior patterns of specific users or verify unusual activity with real-world records. The feature set used for modeling was relatively simple: it focused on temporal and event-based attributes and excluded other potentially informative variables, such as call frequency, unique contacts, duration, or network routing. Additionally, the model may slightly over- or under-estimate the number of anomalous events because the Isolation Forest contamination parameter was set to 2% based on an estimate of anomaly prevalence. To achieve concrete results, government authorities should test the model's performance in real-time monitoring environments.

Future Research

While this study provides initial insights, future research is needed to deepen the analysis in several ways. For one, having access to labeled datasets of confirmed scam calls would make it possible to train and evaluate supervised learning models that can more accurately classify fraud activities. Besides, folding in extra behavioral features such as call duration, repeated calling attempts, and the number of unique contacts per caller would significantly improve detection accuracy. Also, integrating telecommunications metadata with other forms of analysis, like natural language processing of call transcripts or voice pattern recognition, could build hybrid systems that can detect fraud more precisely. Future studies could also explore the use of publicly available datasets containing conversational content of scam calls. For example, datasets such as TeleAntiFraud-28k, which include audio recordings and textual transcripts of telecom fraud scenarios, may enable the training of language models capable of detecting fraudulent intent directly from call conversations. Combining such content-based analysis with metadata-based anomaly detection could lead to more robust and accurate telecom fraud detection systems. Importantly, exploring real-time implementation of anomaly detection systems within telecommunication infrastructure could shift the approach from reactive to genuinely proactive and build systems that can grow at the same pace as attackers.

Conclusion

This study shows that machine learning can identify significant telecommunications metadata irregularities occurring in Uzbekistan according to this study. Using a large anonymized call record database and Isolation Forest analysis, it was determined that 1.87 percent of telephony calls were classified as abnormal based on temporal, event-driven, or geographical characteristics. The observed concentrations of anomalies during late-night hours, among failed calls, and within certain country code categories (as detailed in Tables 2-4) suggest that suspicious activity leaves detectable behavioral traces even without labeled fraud data.

Furthermore, the results show that these types of anomaly detection systems based on metadata can serve as solid foundations for more sophisticated fraud detection systems in Uzbekistan's evolving digital environment. Future improvement to the reliability and practical value of these systems could be realised through the incorporation of additional behavioural characteristics, supervised learning using confirmed scam identifiers, or hybrid (both metadata and content) approaches.

REFERENCES

[1]. United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP). 2025. Uzbekistan Foresight on Digital Public Services for Small and Medium-Sized Enterprises.

[2]. Kemp, Simon. 2025. *Digital 2025: Uzbekistan*. DATAREPORTAL.

[3]. Ministry of Internal Affairs of the Republic of Uzbekistan. 2025. *Cybercrime Statistics Report*.

[4]. Beeline Uzbekistan. 2025. *Beeline Introduces Anti-Spoofing Technology to Prevent Fraudulent Calls.*

[5]. Mobiuz. 2025. *Mobiuz Implements Anti-Spoofing Technology to Protect Subscribers.*

[6]. Norbaev, Kattabek. 2025. *Machine Learning Approaches for Phishing Detection*. AI-powered phishing detection in Uzbekistan: implementation strategies and challenges. American Journal of Education and Learning.

[7]. Abdullayev, Bilol. 2024. *Enhancing Cybersecurity in Uzbekistan: Leveraging Artificial Intelligence Solutions.*International Journal of Innovation Science and Research Technology.

[8]. Anand, Adwaith, Arun Kumar, Hariharan N., Harshavaradan A., Ishika Saxena, K. J. Rajendraprasad, and Skanda Prasad H. 2022. *AI Enabled Scam Call Detection.*

[9]. Bolton, Richard J., and David J. Hand. 2002. "Statistical Fraud Detection: A Review." *Statistical Science* 17 (3): 235–255.

[10]. Gupta, Sandeep. 2025. "An Intelligent System for Identifying Fraud Phone Calls Using Machine Learning Algorithms." *Journal of Global Research in Electronics and Communication.*

[11]. Karri, Jaya Sri, L. Dasarada Ramiah, and V. Anil Santhosh. 2023. "Artificial Intelligence-Based Fraud Phone Call Identification and Analysis." *International Journal of Novel Research and Development.*

[12]. Li, Huichen, Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, and Dawn Song. 2018. "A Machine Learning Approach to Prevent Malicious Calls over Telephony Networks."

[13]. Muminov, Azamat Solijonovich. 2023. "Criminalistic Characteristics of Online Credit Fraud: Issuing Loans Based on Stolen Personal Data." *International Scientific Journal "News of Education: Research in the 21st Century"* (in Uzbek).

[14]. Ratnakumar, J., Shaik Nailo Asmin Thahenath, Tolusuri Sri Lakshmi, Peravali Naga Dileep Kumar, and Kadiyam Veeraiah. 2021. "Detection of Fraudulent or Deceptive Phone Calls Using Artificial Intelligence." *Turkish Journal of Computer and Mathematics Education.*

[15]. Zitong Shen, Sineng Yan, Youqian Zhang, Xiapu Luo, Grace Ngai, Eugene Yujun Fu. 2025. "It Warned Me Just at the Right Moment": Exploring LLM-Based Real-Time Detection of Phone Scams."

[16]. Zhiming Ma, Peidong Wang, Minhua Huang, Jinpeng Wang, Kai Wu, Xiangzhao Lv, Yachun Pang, Yin Yang, Wenjie Tang, Yuchen Kang. 2025. "TeleAntiFraud-28k: An Audio-Text Slow-Thinking Dataset for Telecom Fraud Detection".