JPEPFM Journal of Public Economy and Public Financial Management

Journal of PublicEconomyandPublic Financial Management
Cilt/Volume: 5
Sayı/Issue: 2
Ekim/October 2025

Makale İlk Gönderim Tarihi/Received (First): 04.03.2025

Makale Kabul Tarihi /Accepted: 30.04.2025

Citation / Atıf: Yıldırım, H., Bütüner, Y., & Ünal, C. (2025). Use of Artificial Intelligence Tools For Telephone Scams And Countermeasures. *Journal of PublicEconomy and Public Financial Management*, 5(2), 223-246. https://doi.org/10.71284/jpepfm.202527.

RESEARCH ARTICLE / ARAŞTIRMA MAKALESİ

USE OF ARTIFICIAL INTELLIGENCE TOOLS FOR TELEPHONE SCAMS AND COUNTERMEASURES

Hakan YILDIRIM[1]
Yeşim BÜTÜNER[2]
Cihan ÜNAL[3]

Abstract

The use of artificial intelligence technologies has brought a new and more sophisticated dimension to telephone scams. These technologies allow scammers to target their victims more effectively. This article examines the impact of AI on victim profiling, sentiment analysis, voice mimicry technologies, and AI-assisted conversation methods in fraud. AI algorithms can make targeting more precise by profiling individuals through social media and digital traces.

Sentiment analysis can detect fraudulent intentions by analysing the content of scam messages and adapt strategies in real-time. Voice mimicry technologies allow scammers to manipulate their victims using trustworthy voices. AI-assisted conversation systems make fraud scenarios more convincing and effective.

These developments necessitate the evolution of fraud detection and prevention strategies. Fraud filters and AI detection applications should be developed to prevent the misuse of AI technologies. In addition, the development of AI-assisted applications for smartphones can help individuals and institutions be more prepared against fraud attempts. Such applications can more effectively detect fraud by offering features such as real-time sentiment analysis, voice mimicry detection, and profile analysis.

By ensuring the ethical and responsible use of AI products, security in the digital world can be increased. These types of systems, which will be developed, will protect users by detecting fraud attempts at an early stage and will increase trust in the digital world.

Keywords: Telephone Scams, Sentiment Analysis, New Methods, Countermeasures, AI-Assisted Applications, Security Protocols.

[1] Dr., Ankara Bilim Üniversitesi Maltepe Kampüsü, hakanyildirim72@gmail.com, ORCID: 0000-0002-5959-2691
[2] Konya Selçuklu İlçe Milli Eğitim Müdürlüğü, ayhanbutuner@gmail.com, ORCID: 0009-0000-9170-5097
[3] Dr., Hacettepe Üniversitesi , cihan.unal@hacettepe.edu.tr, ORCID: 0000-0002-5255-4078

1. INTRODUCTION

Telephone scams have become more sophisticated and complex with the rapid development of technology. Scammers can now target and manipulate their victims more effectively using artificial intelligence (AI) and machine learning techniques. This article examines how telephone scams have evolved to a new and advanced level using AI methods, the role of sentiment analysis, voice mimicry technologies, and AI-assisted conversation methods. (IdentityIQ, 2023)

One of the most common methods fraudsters use is voice imitation via artificial intelligence technologies, known as deepfake voices. These technologies have been evolving and becoming more widespread at a rapid pace in recent years. Scammers utilize these techniques to fabricate ambient sounds, making it appear as if they are speaking from a 'police station,' prosecutor's office, or similar official environments. Such methods are particularly effective in misleading and manipulating victims. For instance, fraudsters can simulate entire phone conversations where a victim believes they are speaking to law enforcement. These sophisticated schemes not only involve voice imitation but also include falsified background noises, thereby reinforcing the illusion of authenticity. As fraud techniques evolve, it becomes crucial to detail the specific methods used to enhance both public awareness and preventive measures. (American Psychological Association, 2020)

The use of AI algorithms by scammers to identify the profiles of target individuals is also of great importance. By profiling individuals through social media, email, internet browsing history, and other digital traces, scammers can make targeting more precise. Scammers can target their victims with customized fraud scenarios based on age, financial situation, or interests. Sentiment analysis can detect fraudulent intentions by analysing the language used in scam messages and adapt fraud activities instantly. (Blauth et al., 2022)

AI products can now mimic voices, using the voices of loved ones or trusted individuals, increasing the credibility of fraud scenarios. AI-assisted conversation systems allow the scammer to respond instantly to the victim's reactions and change their strategy, making fraud attempts more convincing and effective. Automated scam calls can call numerous people automatically using AI-based call systems and commit fraud with pre-recorded messages. These systems can analyse the victim's reactions and adapt the conversations in real-time, increasing the success rate of the fraud. (Insights2Techinfo, 2024)

AI can be used to create fake websites and emails, directing victims to these sites to steal personal information. AI can personalize the content of emails to make them more convincing. Creating fake identities and business cards is also among these methods. (IdentityIQ, 2023)

AI can use sentiment analysis to understand and manipulate the victim's reactions. For example, analysing victims' emotional states such as fear, panic, or anxiety and further fuelling these emotions can increase the impact of the fraud. AI can reach large audiences through social media platforms and spread fake news or deceptive information. Such information can be used to support a specific fraud campaign, gain the victim's trust, or manipulate them into a particular action.

These developments necessitate the evolution of fraud detection and prevention strategies. Fraud filters and AI detection applications should be developed to prevent the misuse of AI technologies. By ensuring the ethical and responsible use of AI products, security in the digital world can be increased. The best way to combat all the methods briefly mentioned above is again to use AI

tools. For instance, AI tools that analyse voices created by deepfake are also available. Applications that perform sentiment analysis can be used for the opposite purpose. Just as fraudsters can understand the extent of fear in the person, they are targeting through sentiment analysis, the targeted person can also have an idea about the real intentions of the person they are talking to. (Milani et al., 2024)

The role of AI technologies in combating fraud requires continuously developing innovative strategies against the development of fraud methods. Therefore, individuals and institutions should be more careful and aware of telephone scams and effectively use existing technological tools. This article examines AI methods developed against telephone scams in detail and focuses on the measures that can be taken against such scams.

2.1. TYPES OF TELEPHONE SCAMS

In this article, among various fraud techniques, 'telephone scams' have been selected as the focus of study. Therefore, next-generation methods developed by scammers using AI in telephone scams will be examined. Following this, both currently developed methods and potential future techniques using AI to combat these scams will be explored. Additionally, studies in the literature focusing on different types of scams, particularly those involving persuasion, will be incorporated to provide a comprehensive understanding.

The psychology of fraud and persuasion techniques is a topic of great interest in both criminology and psychology. Scammers use various techniques to manipulate people's behaviour and deceive them. Understanding these techniques can help protect individuals and prevent such crimes. (FightCybercrime.org, 2023).

2.1.1. Social Engineering

Social engineering is a sophisticated and highly effective method used by scammers to manipulate individuals into revealing confidential or personal information, often without the target being aware of the breach. It relies on psychological manipulation rather than traditional hacking techniques, using human behavior as the primary tool for exploitation. Scammers often exploit trust, fear, urgency, curiosity, or even the victim's desire to be helpful. These emotional triggers are designed to cloud the victim's judgment, making them more susceptible to manipulation.

One of the core tactics in social engineering is phishing, where scammers pose as legitimate entities such as banks, government agencies, or well-known companies in order to deceive targets into disclosing sensitive information like passwords, credit card numbers, or Social Security numbers. Phishing can occur via email, phone calls (vishing), or even text messages (smishing).

Another prevalent tactic is pretexting, where fraudsters create a fabricated scenario to obtain information. For instance, they might impersonate a trusted colleague or authority figure, like an IT support representative, to persuade the victim to share login credentials or other sensitive data. This tactic often leverages the victim's sense of duty or obligation to comply with authority or help resolve a fabricated issue.

In baiting, scammers lure victims into a trap by offering something enticing, such as free downloads, which in reality contain malware designed to steal data or compromise systems. Baiting often targets individuals who are unaware of the risks associated with downloading from unknown sources or inserting unknown USB devices into their computers.

Another technique, quid pro quo, involves offering a service or benefit in exchange for information. A common example is when scammers promise technical support or troubleshooting help, but their real goal is to gain access to a system or sensitive data under the guise of providing assistance.

In all of these techniques, victim profiling plays a critical role. Scammers often gather personal information from publicly available sources, such as social media profiles, job postings, or online forums, to craft a tailored approach. By understanding the target's background, interests, and vulnerabilities, fraudsters can develop a highly convincing narrative, making the deception far more effective. This profile helps them exploit specific weaknesses, whether it’s through impersonating a trusted figure or exploiting the target's urgency to solve a fabricated problem.

Social engineering attacks are particularly dangerous because they bypass traditional security measures like firewalls and encryption by exploiting human weaknesses. Unlike brute-force attacks, which rely on technological loopholes, social engineering leverages trust and psychological manipulation, making it difficult for traditional security systems to detect. This makes raising awareness and educating individuals on common social engineering techniques one of the most important defenses against such attacks.

To combat these threats, organizations and individuals alike must focus on education and awareness. By understanding how social engineering works, people can be more vigilant when confronted with suspicious requests or urgent demands for personal information. Additionally, companies can implement training programs that simulate social engineering attacks, helping employees recognize and respond to potential threats. Implementing two-factor authentication (2FA) and maintaining strong, unique passwords also adds an extra layer of protection against these tactics.

Social engineering is a growing threat that takes advantage of human psychology and behavior. By profiling their targets and exploiting emotional triggers, scammers can gain access to sensitive information or resources with alarming ease. As social engineering tactics evolve, it becomes increasingly important for individuals and organizations to stay informed and develop robust defenses against these insidious methods. (Shaukat et al., 2020).

2.1.2. Fraud via Email or Fake Websites

This type of fraud, commonly referred to as phishing, involves tricking victims into providing their personal or financial information through deceptive emails or websites. The fraudsters typically create fake but convincing websites that closely resemble legitimate organizations, such as banks, government agencies, or well-known companies. These sites often prompt the victim to enter sensitive details, including login credentials, credit card numbers, or personal identification information.

The scam often begins with an unsolicited email that appears to come from a trusted source. These emails use persuasive language to create a sense of urgency, warning the recipient of potential account closure, fraudulent activity, or a missed payment. The email usually contains a link that directs the victim to a fake website designed to capture their personal information.

Another common tactic is to include malicious attachments within the email. When the victim opens these attachments, malware is installed on their device, giving the scammer access to private data or enabling them to monitor the victim's activities remotely.

2.1.3. Key Characteristics of This Type of Fraud Include

Urgency and Threats: The fraudsters often use threats of account suspension or legal consequences to create a sense of urgency, prompting the victim to act quickly without thoroughly inspecting the legitimacy of the email or website.

Spoofed Email Addresses and Websites: Phishing emails and fake websites are crafted to look authentic. Fraudsters might use email addresses or domains that appear almost identical to those of legitimate organizations, with only slight alterations that are easy to overlook.

Malware Deployment: In some cases, clicking on a link or opening an attachment in the email triggers malware installation, which can lead to the theft of personal data or financial information without the victim's knowledge.

To combat this form of fraud, individuals and organizations must adopt strict security measures, including training to recognize phishing attempts, verifying the authenticity of emails before clicking on links or providing information, and using multi-factor authentication (MFA) to secure accounts. In addition, keeping software and security systems up-to-date is crucial for preventing the installation of malware that could result from these fraudulent activities.

2.1.4. Deception by Reward

Deception by reward is a common method used by scammers where they lure victims by promising large rewards, financial gains, or lucrative opportunities. This type of fraud often plays on the victim's desire for wealth or quick success, encouraging them to act without fully considering the legitimacy of the offer. These scams are typically carried out through various schemes, with one of the most well-known examples being the "Nigerian Prince" scam.

In the "Nigerian Prince" scam, the victim is contacted by someone claiming to be a wealthy individual often a prince or government official—who needs help transferring a large sum of money. In return for the victim's assistance, they are promised a substantial reward. However, before receiving the supposed reward, the victim is asked to pay various fees, such as legal or transaction costs. As the scam progresses, the demands for additional payments increase, with the victim never receiving the promised reward.

Another common example is the lottery or sweepstakes scam, where the victim is informed that they have won a significant prize. However, in order to claim the prize, they must first pay taxes, processing fees, or other related costs. Victims, excited by the possibility of their winnings, often comply with these requests, only to realize that no such prize exists.

2.1.5. Key Characteristics of Deception by Reward Include

Promise of Unlikely Gains: The fraudsters offer rewards that are often too good to be true, such as sudden wealth, inheritance from unknown relatives, or large lottery winnings that the victim did not participate in.

Urgency and Pressure: The scammers frequently apply pressure on the victim to act quickly, emphasizing that the opportunity is time-sensitive or that their help is urgently needed. This tactic is designed to prevent the victim from thoroughly investigating the offer.

Advance Payments: A hallmark of these scams is the request for upfront payments, whether for transaction fees, legal paperwork, or taxes. Once the victim makes the initial payment, the

scammer continues to ask for more, stringing the victim along with the promise of eventual reward.

2.1.6. Prevention and Awareness:

To avoid falling victim to these types of scams, it is essential to maintain a healthy skepticism of unsolicited offers of large rewards or financial gains. Individuals should be cautious of anyone requesting advance payments in exchange for promised rewards and should never provide personal or financial information to unknown sources. Verifying the legitimacy of such offers through official channels and conducting thorough research are critical steps in preventing deception by reward scams.

2.1.7. Fraud Through Fear and Anxiety

Fear and anxiety are powerful emotions that can cause individuals to act hastily, often without rational consideration. Scammers exploit these emotions by creating urgent and threatening situations, forcing their victims to make quick decisions out of fear. This manipulation technique is highly effective because it leverages the victim's emotional response rather than their logical thinking.

One common method is the impersonation of authority figures. Scammers often pose as law enforcement officials, tax authorities, or legal representatives, claiming that the victim is in legal trouble or that they owe a significant amount of money. They create a sense of urgency by threatening immediate arrest, legal action, or financial penalties if the victim does not comply. Under pressure, victims may provide personal information, such as social security numbers or bank details, or make hasty payments to avoid the fabricated consequences.

Another tactic involves fraudulent medical emergencies or family crises. In these scenarios, scammers contact victims claiming that a loved one has been injured or is in danger and needs immediate financial assistance. The victim, overwhelmed by fear for their family member, may transfer money without verifying the authenticity of the claim. This type of scam exploits the victim's emotional vulnerability, making them more susceptible to manipulation.

2.1.8. Key Characteristics of Fear and Anxiety-Based Fraud Include

Urgent and Threatening Language: Scammers use intense and alarming language to create a sense of fear and panic. They emphasize the immediate consequences of inaction, often fabricating emergencies or legal penalties that demand the victim's immediate response.

Limited Timeframes: Victims are often told they have only a short amount of time to act, which prevents them from thinking critically or seeking help. The goal is to rush the victim into making decisions under stress.

Impersonation of Authorities: By impersonating trusted figures such as police officers, lawyers, or government officials, scammers lend credibility to their threats, making it more difficult for victims to question the validity of the situation.

2.1.9. Preventive Measures and Awareness

To protect against fear-based scams, individuals should always take a moment to verify the legitimacy of any claim that induces panic or anxiety. Contacting the alleged authority directly through official channels, such as a government website or law enforcement office, is crucial. Additionally, individuals should be wary of any communication that demands immediate action,

payment, or personal information, especially if it comes from an unsolicited source. Educating oneself about common tactics used in fear-based scams can also reduce susceptibility to these fraudulent schemes. (IdentityIQ, 2023)

2.1.10. Fear of Crime

The concept of fear of crime is one of the most commonly exploited methods by scammers today. The exact nature of the scam varies depending on the country and period, but the psychological impact on the victim remains the same: fear of being associated with a crime leads them to comply with the scammer's demands. In Turkey, for instance, scammers have adapted their language to reflect the types of crimes that are prevalent in media reports. Before 2014, scammers would claim, "Your name is involved in PKK operations," whereas after 2014, this changed to "Your name is involved in FETO operations" (Çalışkan, 2018). (PKK and FETO are terrorist organizations)

Similarly, in the USA, scammers frequently use the fear of tax evasion as a tactic (Global Engagement, n.d.). In Germany, scammers focus on customs-related fraud, creating anxiety around the possibility of legal action or penalties from customs authorities (European Public Prosecutor's Office, 2021).

Phrases commonly used to instill fear include terms such as "Urgent," "Immediately," "At once," "Suspicious," "Danger," "Violation," "Arrest," "Suspension," and "Cancellation." These key terms are often detected in fraud attempts through sentiment analysis methods, allowing security systems to flag potentially fraudulent communication.

Starting from this section, the explanations correspond to Table 1. Types and Methods of Telephone Frauds. The data presented in this subheading and subsequent sections are defined based on the categorization and methods detailed in Table 1, as shown below:

Table 1. Types and Methods of Telephone Scams

Fraud Type	Methods	Used Example Phrases
Fear of Crime	Claims of involvement in PKK/FETO operations, fear of tax evasion	"Your name is involved in Feto operations"
Pressure of Emergency	Urgent transaction pressure, claims of being at great risk	"You need to take immediate action"
Fears Related to Family and Friends	Claims that a close relative had an accident, child's safety is at risk	"Your child's safety is at risk"
Health and Social Security Fears	Positive Covid-19 test result, cancellation of health insurance	"Your health insurance has been canceled"

2.1.11. Creating Emergency Pressure

Putting pressure on victims to hurry or do something immediately is a common tactic used by scammers. This prevents the victims from thinking rationally and leads them to make quick decisions. Phrases like "You need to take immediate action" and "You are at great risk right now" are used to keep the victim under pressure to make urgent decisions.

2.1.12. Creating Fears Related to Family and Friends

In these types of fraud techniques, phrases like "A close relative of yours had an accident. Call this number immediately." "Your child's safety is at risk. Respond to this message immediately." "Your daughter has been kidnapped. Call this number for ransom payment."

2.1.13 Health and Social Security Fears

In this type of fraud, fear is created through common health issues or epidemic situations to make the victim do what is wanted. For example, "Your Covid-19 test result is positive. Visit the health centre immediately." "Your health insurance has been cancelled. Call immediately for a new policy." "Due to an urgent health situation, call this number immediately." Such phrases are used for this purpose.

2.3. PERSUASION TECHNIQUES

2.3.1. Relying on Authority

One of the most effective methods scammers use is exploiting people's inherent trust in authority figures. Research by Cialdini (2006) demonstrates that individuals are more likely to comply with requests when they believe they come from a figure of authority. This tendency is rooted in social norms and cultural values, which associate authority with legitimacy and trustworthiness. In the context of fraud, scammers often impersonate law enforcement officials, bank representatives, or healthcare professionals to convince their victims to share sensitive information. For instance, statements like, "I am officer Ahmet; we need to verify your identity information," or "I am calling from your bank; we have detected suspicious activities in your account," are designed to evoke immediate compliance from the victim. (Cialdini, 2006)

2.3.2. Reciprocity

The principle of reciprocity suggests that people feel obligated to return favors. According to Gouldner (1960), reciprocity is a social norm where individuals who receive something of value feel compelled to offer something in return. Scammers exploit this by offering small favors, such as a "free consultation" or a "special discount," making the victim feel indebted. This technique increases the likelihood of the victim complying with further requests, such as sharing personal information or making a payment. An example might be, "We have prepared a free credit report for you; now we need to verify your credit card information." (Gouldner, 1960)

2.3.3. Fear of Missing Out on a Product or Service

Fear of missing out (FOMO) is a psychological phenomenon where individuals feel compelled to act quickly to avoid losing an opportunity. According to Przybylski et al. (2013), FOMO is linked to anxiety and the fear that others might benefit from opportunities the individual has missed. Scammers take advantage of this by creating a sense of urgency, using phrases such as "This offer is valid only today," or "Hurry up, only the last three people get the discount!" By doing so, they pressure the victim into making hasty decisions without critical evaluation. (Przybylski et al. 2013)

2.3.4. Building Trust Through Consistency

People strive for consistency in their actions and beliefs. Scammers leverage this by first asking for small commitments, such as filling out a simple form or survey, and then escalating their demands. Research by Cialdini and Goldstein (2004) shows that individuals who commit to small

actions are more likely to comply with larger, related requests to remain consistent with their initial actions. For example, after filling out a brief form, the scammer might ask for additional personal details, building on the trust established through the initial interaction. (Cialdini & Goldstein, 2004)

Manipulation involves the use of deceitful psychological tactics to control or influence another person's decisions without their awareness. Scammers use manipulation to create an illusion of trust, safety, or urgency, often by providing misleading or false information. According to Alzahrani (2023), manipulative techniques can include exploiting emotions such as fear, hope, or even greed to get the victim to act in the scammer's favor. By crafting convincing narratives or fabricating situations that seem plausible, scammers lower the victim's defenses.

For example, they may reference past interactions to build familiarity ("I've helped you before; do you remember?") or assure the victim that their information is being handled securely to build trust ("We are recording this conversation for your security"). Scammers may also appeal to the victim's emotions by using a sincere or friendly tone, making the victim feel more comfortable and less likely to question the validity of the request.

Furthermore, scammers manipulate by creating extraordinary situations that seem urgent and dangerous, such as claims of a breach in the victim's bank account or the discovery of fraudulent activity. Statements like, "We detected a security breach in your account, and you need to act immediately to prevent serious losses," are designed to provoke immediate action, bypassing the victim's rational thought processes and leading them to comply without considering the potential for fraud. (Alzahrani, 2023).

2.4. NEW METHODS

2.4.1. AI-Assisted Fraud Techniques

Recent advancements in artificial intelligence (AI) have given scammers new tools to enhance their fraudulent activities. These emerging AI-assisted techniques are used to manipulate victims more effectively and make it harder for traditional detection systems to identify fraud attempts. As detailed in Table 2. Emerging AI-Assisted Telephone Fraud Techniques, these methods focus on exploiting human emotions and trust through AI-driven strategies. The following sections explain how each method works and where it is applied.

2.4.2. Sentiment Analysis

One of the emerging tools used in AI-assisted fraud is sentiment analysis, which helps scammers detect the emotional state or intentions of the victim by analyzing the language used in conversations. This method is primarily used in social engineering and phishing attacks, where the scammer needs to adjust their approach based on how the victim reacts. By detecting fear, anxiety, or hesitation in the victim's responses, the scammer can fine-tune their strategy in real-time to increase the likelihood of success (Alzahrani, 2023; Przybylski et al., 2013) (see Table 2).

2.4.3. Voice Mimicry Technology

Another powerful AI tool is voice mimicry technology, which allows scammers to replicate the voice of trusted individuals, such as bank employees or law enforcement officers. This technology is used to build trust with the victim by simulating the voice of someone they are likely to believe or respect. By impersonating authority figures, scammers can convince the victim to share sensitive information or take immediate action. The usage of voice mimicry has made it

increasingly difficult for victims to distinguish between real and fake calls, making it a preferred method in high-stakes telephone fraud (Cialdini, 2006) (see Table 2).

2.4.4. AI-Assisted Conversations

AI-assisted conversations enable scammers to respond instantly to a victim's reactions during live calls. By using machine learning algorithms, scammers can adjust their tactics mid-conversation, ensuring that the scam remains convincing even when the victim shows hesitation or skepticism. This adaptive method allows scammers to create more fluid and personalized interactions, making the scam harder to detect and evade. As outlined in Table 2, this technique is primarily used in live scam calls, where real-time responses are critical for maintaining the ruse (Gouldner, 1960).

Table 2. Emerging AI-Assisted Telephone Fraud Techniques

Method	Description	Usage Area
Sentiment Analysis	Detecting intentions by analyzing the language used in scam messages	Social engineering, phishing
Voice Mimicry Technology	Manipulating victims using trustworthy voices	Impersonating police or bank employees
AI-Assisted Conversation	Responding instantly to reactions and changing strategy	Live scam calls

2.4.5. AI-Assisted Victim Profiling

AI algorithms can profile individuals through social media, email, internet browsing history, and other digital traces. This profiling process allows scammers to target their victims more effectively. For example, elderly individuals, young people without financial knowledge, or people interested in specific topics can be targeted with specially designed scam scenarios. (Subex.com/ai, 2023)

2.4.6. Real-Time Strategy Setting with Sentiment Analysis

Sentiment analysis (sentiment analysis) can play a significant role in fraud detection and prevention strategies by analysing the emotions and intentions in digital communication. Scammers try to evoke certain emotional reactions to manipulate their targeted individuals. Sentiment analysis can help detect fraudulent intentions by analysing the language used in such messages. (FightCybercrime.org, 2023)

2.4.7. Voice Mimicry Technologies

AI products can now mimic voices, using the voices of loved ones or trusted individuals. These technologies are developed using deep learning and neural networks. Recently developed new generation voice mimicry products can mimic the pauses and thinking times within normal speech. (IdentityIQ, 2023)

2.4.8. AI-Assisted Conversation

AI can speak naturally and fluently in real-time. AI-assisted conversation systems make the interaction with the victim more convincing and effective. These systems allow the scammer to respond instantly to the victim's reactions and change their strategy. For example, an AI system

can use a more persuasive and reassuring language if it detects that the victim is starting to suspect. For example, a scammer can easily manipulate the victim by mimicking the voice of a close friend or family member. These voice mimicry technologies increase the credibility of fraud scenarios. The difference from imitation systems in this type of fraud is that it is used in a part where trust needs to be gained, not in the whole process. (Smith, 2020).

2.5. COUNTERMEASURES

2.5.1. Sentiment Analysis and AI Integration

Fraud detection systems can be significantly enhanced by integrating sentiment analysis with machine learning and AI techniques. These systems can automatically detect fraudulent communications, alert the relevant parties, and take necessary precautions. As detailed in Table 3. Countermeasures Against Telephone Fraud, AI-driven tools such as sentiment analysis and voice analysis are crucial in identifying phone scams and fraudulent activities.

Sentiment analysis plays a particularly important role in detecting the emotional tone and intent behind messages, helping to identify potential scams early. When paired with AI, it can monitor large volumes of communication data and flag interactions that exhibit suspicious patterns. This combination not only aids in real-time fraud detection but also supports the development of more robust prevention strategies. The relationship between sentiment analysis and phone scams can be pivotal in detecting fraudulent communications by analyzing the emotions and intentions present in digital conversations (Singh & Jain, 2020) (see Table 3).

AI systems such as those employing behavior analysis can continuously monitor user behavior to detect abnormalities. For instance, when an account exhibits unusual or suspicious activities—such as a high number of login attempts or sudden changes in communication patterns—the system can automatically trigger alarms. This is particularly useful in protecting vulnerable populations, such as elderly individuals, from fraud. Family members or caregivers may use these filters to monitor interactions and intervene when suspicious activities are detected (IdentityIQ, 2023).

Table 3. Countermeasures Against Telephone Fraud

Tool/Method	Description	Usage Area
AI and Sentiment Analysis	Fraud detection with emotional and language analyses	Telephone scams, email scams
Voice and Speech Analysis	Fraud detection by analyzing the tone, speed, and other linguistic features	Live calls
Feedback Mechanisms	Quickly reporting fraud attempts	All digital platforms
Behavior Analysis	Detecting abnormal activities by monitoring user behaviors	Social media, email

2.5.2. Fraud Filters in AI Products

Behavior analysis is just one of the several layers of defense in AI products designed to prevent fraud. By defining predetermined criteria for what constitutes abnormal behavior, AI systems can more effectively filter and detect potential fraudulent activities.

In addition to behavior analysis, security protocols play a critical role in preventing fraudulent activities. AI products can use content filters to detect and block specific keywords or phrases commonly used in scams. This prevents scammers from effectively reaching their targets.

Another key defense mechanism is user verification. AI systems can employ multi-factor authentication and biometric verification methods to ensure that only legitimate users gain access to sensitive information or services. This makes it more difficult for scammers to use fake accounts or stolen identities.

Finally, detection of fraud messages through sentiment analysis helps in identifying manipulative language and emotional cues commonly used by telephone scammers. This can serve as an early warning system, flagging potentially fraudulent interactions and protecting users from falling victim to scams. (IdentityIQ, 2023)

2.5.3. Security Protocols

AI products should have various security protocols to prevent users from engaging in fraudulent activities. For example, content filters can be applied to limit the use of specific keywords or phrases.

2.5.4. User Verification

AI systems can make it more difficult for scammers to access systems with fake accounts or identities by tightening user identity verification. Multi-factor authentication and biometric verification methods can be effective in this regard.

2.5.5. Detection of Fraud Messages

Telephone scammers often try to manipulate their targets by evoking specific emotional reactions. Sentiment analysis can help detect fraudulent intentions by analysing the language used in such messages.

2.6. APPLICATIONS DETECTING SCAMMERS

Voice and Speech Analysis

Applications based on voice and speech analysis can be developed to prevent scammers from deceiving their victims using AI. These applications can analyze the tone, speed, and other linguistic features of speech to determine whether the speaker is an AI product or a real person. Not only that, but they can also detect fraud by identifying specific keywords associated with scam attempts. As shown in Table 4. Products Used for Emotion Analysis and Key Features, there are various well-known and commonly used sentiment analysis tools designed for different sectors and use cases, which aid in fraud detection.

These applications are particularly effective in detecting emotional manipulation, which is a common tactic in scams. By analyzing the emotional state of the speaker or detecting abnormal speech patterns, such tools can provide early warnings for fraudulent communications. Sentiment analysis and speech biometrics are crucial components of these fraud detection systems, especially in sectors like customer service, healthcare, and financial services, where trust and communication are key (IdentityIQ, 2023).

Table 4. Products Used for Emotion Analysis and Key Features

Tool/Platform	Description	Usage Area	Key Features
Cogito	An application used in customer service and healthcare sectors.	Call center, healthcare sector	Evaluates emotional state and tone of speech by analyzing conversations.
Affectiva	A technology that can analyze emotions through facial expressions and voice tones.	Marketing research, automotive, healthcare sector	Analyzes facial expressions and voice tones.
Beyond Verbal	An application that can detect emotions based on speech analysis.	General use	Determines emotional state by analyzing voice tones.
Emotient (Apple)	A technology that determines emotional reactions by analyzing facial expressions.	Various applications	Analyzes facial expressions.
VoiceSense	An application that creates personality and behavior profiles by analyzing voice tones.	Financial services, human resources, customer service	Creates personality and behavior profiles by analyzing voice tones.
Converus EyeDetect	A lie detection technology that analyzes eye movements and pupil reactions.	Lie detection	Analyzes eye movements and pupil reactions.
iMotions	A multimodal biometric research platform.	Biometric research	Analyzes facial expressions, eye movements, heart rate, and skin conductivity.
Truthify	A mobile emotion analysis and lie detection application.	Mobile devices	Determines emotional reactions and accuracy levels by analyzing facial expressions.
IDRND	A technology for emotion and lie detection based on voice analysis.	Speech analysis	Analyzes changes in voice tone.
Pindrop	A technology that detects fraud using voice analysis and speech biometrics.	Fraud detection	Analyzes voice tone, speech patterns, and other biometric data.
NICE Actimize	A platform used for fighting financial crimes and detecting fraud.	Financial crimes, fraud detection	Uses emotion analysis and behavioral analysis techniques.
CallMiner	Analyzes customer interactions and performs emotion analysis and speech analysis.	Call centers	Analyzes call center conversations and detects suspicious activities.
Feedzai	Detects fraud by analyzing users' behavior patterns.	General use	Detects unusual behaviors.

Verint Systems	A platform that analyzes customer interactions and performs emotion analysis.	Customer service	Performs speech analysis and emotion detection.

2.7. EMOTIONAL ANALYSIS TOOLS

2.7.1. Cogito

Cogito is an application used in the customer service and healthcare sectors. It evaluates the emotional state and tone of speech by analysing conversations of call centre employees, helping them provide better service to customers. (https://cogitocorp.com)

2.7.2. Affectiva

Affectiva offers a technology that can analyse emotions through facial expressions and voice tones. This technology is particularly used in marketing research, automotive, and healthcare sectors. (https://www.affectiva.com)

2.7.3. Beyond Verbal

Beyond Verbal is an application that can detect emotions based on speech analysis. It determines users' emotional states by analysing voice tones and provides feedback by processing this data. (https://thedube.com)

2.7.4. Emotient (Apple)

Emotient is an emotion analysis technology acquired by Apple. It determines emotional reactions by analysing facial expressions and uses this data in various applications. (https://appleinsider.com/articles/16/01/07/apple-acquires-facial-recognition-expression-analysis-firm-emotient---report)

2.7.5. VoiceSense

VoiceSense is an application that can create personality and behaviour profiles by analysing voice tones. This technology is used in financial services, human resources, and customer service fields. (https://voicesense.com)

2.7.6. Converus EyeDetect

Converus EyeDetect is a technology for lie detection that analyzes eye movements and pupil reactions. It uses scientific methods to determine users' accuracy levels. (https://converus.com)

2.7.7. iMotions

iMotions is a multimodal biometric research platform. It collects biometric data such as facial expressions, eye movements, heart rate, and skin conductivity, performing emotion analysis and lie detection. (https://imotions.com)

2.7.8. Truthify

Truthify is a mobile application for emotion analysis and lie detection. It determines users' emotional reactions and accuracy levels by analysing facial expressions. (https://truthify.com)

2.7.9. IDRND

Q3D offers a technology for emotion and lie detection based on voice analysis. It determines accuracy and emotional states by analysing changes in voice tone during speech. (https://www.idrnd.ai)

2.7.10. Pindrop

Pindrop is a technology that detects fraud using voice analysis and speech biometrics. This platform detects and prevents fraud attempts by analysing voice tone, speech patterns, and other biometric data. (https://www.pindrop.com)

2.7.11. NICE Actimize

NICE Actimize is a platform used for fighting financial crimes and detecting fraud. It detects abnormal behaviours and potential fraud attempts by using emotion analysis and behavioural analysis techniques. (https://www.niceactimize.com)

2.7.12. CallMiner

CallMiner analyses customer interactions and performs emotion analysis and speech analysis. It detects suspicious activities by analysing call centre conversations to identify fraud attempts. (https://callminer.com)

2.7.13. Feedzai

Behavioral biometrics technologies can detect fraud by analysing users' behaviour patterns. These technologies detect unusual behaviours of users and identify potential fraud attempts. (https://feedzai.com/blog/behavioral-biometrics-next-generation-fraud-prevention)

2.7.14. Verint Systems

Verint Systems analyses customer interactions and performs emotion analysis. It detects fraud attempts by performing speech analysis and emotion detection. (https://www.verint.com)

2.7.15. Behavioral Analysis

One of the key tools in AI-powered fraud detection systems is behavioral analysis. These systems can identify patterns in the language structure, word choice, and speaking style of scammers, providing valuable clues as to whether a conversation is generated by AI. This approach is particularly critical in environments like social media and email, where large-scale monitoring is necessary. As outlined in Table 4, behavioral analysis helps detect unusual user behaviors, which can serve as early indicators of fraudulent activity.

2.7.16. Feedback Mechanisms

Another essential feature in improving fraud detection systems is the integration of feedback mechanisms. These allow users to quickly report suspected fraud attempts, enabling AI systems to continuously refine and enhance their detection capabilities. Real-time user feedback offers critical data that helps AI algorithms adjust and respond more effectively to evolving fraud tactics. As seen in Table 4, feedback mechanisms are applicable across various digital platforms and play a vital role in combating online fraud (Al-Khazaali et al., 2023)

Developing strategies and safeguards to prevent the malicious use of AI in telephone scams will not only enhance the security of individuals and organizations but also promote the ethical and responsible use of AI technologies. These systems, designed to detect fraud attempts at an early stage, will protect users and strengthen trust in the digital world.

2.8. AI-ASSISTED APPLICATION PROPOSAL FOR FRAUD DETECTION ON SMARTPHONES

Purpose and Scope of the Application

The primary purpose of the AI-assisted application to be developed is to detect and prevent telephone scams. This application will help users detect fraud attempts instantly, protecting their personal and financial information. The application is specifically designed for elderly individuals and users with low digital literacy. (Financial Fraud Consortium, 2024)

Table 5. Features of the Proposed Application

Feature	Description	Usage Area
Sentiment Analysis	Detecting fraud intentions by analyzing call and message contents	All digital platforms
Voice Mimicry Detection	Determining whether the voices in calls are mimicked	Live calls
Real-Time Profile Analysis	Analyzing users' digital traces and social media activities	Social media, email
Security Protocols and Alerts	Filtering keywords and phrases and warning the user	All digital platforms

2.9. CORE FEATURES OF THE APPLICATION

The core features of the proposed application, as outlined in Table 5, focus on detecting and preventing fraud through advanced AI techniques. Each feature is designed to enhance user security and provide real-time alerts for potential threats.

2.9.1. Sentiment Analysis

The application uses sentiment analysis to detect fraudulent intentions by analyzing the content of incoming calls or messages. This feature performs both text-based and voice-based analyses, sending instant alerts to the user when suspicious patterns are identified. (Bhargavi et al., 2024)

2.9.2. Need for Application-Specific Corpus

To improve fraud detection, the application relies on a specialized corpus of fraud-related words and expressions. AI will be able to create and continuously update its own dictionary through machine learning techniques. This corpus will be essential for identifying new and evolving fraud tactics.

2.9.3. Voice Mimicry Detection

The application utilizes voice mimicry detection technology to identify AI-generated voices during calls. For example, it can instantly detect and alert the user if a fraudster attempts to mimic the voice of a close relative, a tactic often used in scams.

2.9.4. Real-Time Profile Analysis

Real-time profile analysis allows the application to monitor the user's digital traces and social media activities, identifying whether they are being targeted by fraud attempts. This helps in detecting personal information-based fraud attempts at an early stage.

2.9.5. Security Protocols and Automatic Alerts

The application includes built-in security protocols that automatically filter calls containing specific keywords or phrases, such as "urgent," "immediately," or "police." When such words are detected, the user is alerted to the possibility of a fraud attempt. (FightCybercrime.org, 2023)

2.9.6. Feedback and Reporting Mechanisms

A feedback mechanism allows users to quickly report suspected fraud attempts. This feedback helps the application to continuously improve its fraud detection capabilities by incorporating user experiences and data.

2.10. TECHNICAL INFRASTRUCTURE AND OPERATION

2.10.1 Machine Learning Models

The application detects fraud attempts using machine learning algorithms and continuously learns. These models are trained on large data sets and become more sensitive over time. (Liu J., 2021)

2.10.2. Cloud-Based Data Analysis

The application performs cloud-based data analysis, providing real-time updates and serving a wide user base. Thus, real-time information about fraud attempts is collected and analysed. (Liu J., 2021)

2.10.3. User Education and Awareness

The application provides educational materials to users to raise awareness about fraud attempts. These materials provide information about fraud techniques and measures that can be taken against them.

2.10.4. Sample Scenarios and Usage Cases

In real-world applications, the fraud detection system can be employed in a variety of situations. Below are some examples of how the system can respond to potential fraud attempts. Instead of presenting the scenarios as isolated cases, they are woven into the overall functionality of the application, highlighting how its features can detect and prevent fraud in various situations.

For instance, when a user receives a phone call containing the phrase "you need to take immediate action," which is commonly used in emergency fraud schemes, the application's sentiment analysis feature will detect the urgency of the language. Based on predefined keywords and patterns associated with fraud, the system will instantly flag this interaction as suspicious, alerting the user to proceed with caution. In addition to providing an alert, the application may also suggest additional steps to verify the caller’s identity or block the call entirely. This process demonstrates how real-time fraud detection works in emergency fraud scenarios, ensuring user protection at the earliest stage.

In another example, consider a situation where a user receives a call that mimics the voice of a family member. Using voice mimicry detection, the application can analyze the tone, cadence, and speech patterns in the call. If it detects that the voice does not match the genuine characteristics of the family member or is AI-generated, the system will immediately inform the user that the call may be fraudulent. This real-time detection prevents users from falling victim to impersonation scams that leverage emotional manipulation.

These examples illustrate the system's ability to protect users from a range of fraud attempts by utilizing advanced AI features. By continuously monitoring and analyzing speech patterns, language use, and caller behavior, the application provides a robust defense against common fraud tactics.

2.10.5. Future Development and Improvements

Future versions of the application can include more advanced AI algorithms and new features based on user feedback. This will make fraud detection more effective and comprehensive.

This section provides a comprehensive look at how an AI-assisted application to be developed against telephone fraud will work and what features it will have. The application aims to increase user security and prevent fraud attempts by developing measures against innovative fraud methods using AI.

2.11. METHODOLOGY OF THE STUDY

This section outlines the methodology used to design and develop the AI-assisted application for detecting and preventing telephone fraud. The study follows a multi-phase approach, integrating both qualitative and quantitative methods to ensure the system’s functionality, user-friendliness, and efficacy in real-world scenarios.

2.11.1. Problem Definition and Literature Review

The first phase involved identifying the key challenges and threats posed by telephone fraud, particularly those enhanced through the use of AI. A comprehensive literature review was conducted, focusing on previous studies related to fraud detection systems, sentiment analysis, voice mimicry technologies, and AI-based behavioral analysis (Bhargavi et al., 2024). This review helped in defining the features required for an effective fraud detection application and understanding the latest developments in fraud techniques.

2.11.2. Design of the Application Architecture

In this phase, the architecture of the proposed AI-assisted application was developed. This included designing the modules for sentiment analysis, voice mimicry detection, real-time profile analysis, and security protocols. The application architecture was designed to be modular and scalable, allowing for continuous updates as new fraud techniques emerge. Specific algorithms were chosen for each feature, with a focus on ensuring low latency in fraud detection and alerting users in real time.

2.11.3. Data Collection and Corpus Creation

To enhance the system’s accuracy, a large dataset was collected consisting of real-world examples of fraudulent calls and messages. This dataset was used to train the machine learning models that power the application’s fraud detection capabilities. Additionally, a specialized corpus of fraud-related words, phrases, and behaviors was developed, which forms the backbone of the application’s fraud detection algorithms.

2.11.4. Development and Integration of AI Models

AI models were trained using the collected dataset to perform sentiment analysis and voice mimicry detection. For sentiment analysis, the models were trained to detect emotional manipulation tactics commonly used in scams. For voice mimicry detection, deep learning

techniques were employed to differentiate between genuine voices and AI-generated imitations. Real-time profile analysis was integrated using machine learning models that analyze users' digital traces and flag suspicious activity.

2.11.5. Testing and Validation

The application underwent rigorous testing to ensure its effectiveness in detecting various types of telephone fraud. Test cases were created based on real-world fraud scenarios, and the system's accuracy in identifying fraudulent activities was measured. User feedback was also gathered to assess the application's usability and refine its interface for better user experience.

2.11.6. Continuous Improvement and Feedback Loop

Finally, a feedback mechanism was implemented within the application, allowing users to report potential fraud attempts. This real-time feedback is used to improve the machine learning models and update the fraud detection algorithms, ensuring the system remains effective against new and evolving fraud techniques.

By following this structured methodology, the AI-assisted application aims to significantly reduce the risk of telephone fraud and provide users with a reliable tool for detecting and preventing fraud attempts.

3. FINDINGS

The study reveals several critical insights into the role of artificial intelligence (AI) in facilitating and combating telephone scams. Based on the analysis of AI-based fraud techniques, the following key findings have been identified:

Sentiment Analysis and Victim Profiling: AI-driven sentiment analysis and victim profiling enable scammers to tailor their fraud attempts more effectively. Scammers can detect emotions like fear and anxiety in real-time and adjust their tactics to exploit these emotional states, increasing the likelihood of success.

Voice Mimicry Technology: The study highlights the increasing sophistication of voice mimicry technology, which allows fraudsters to imitate the voices of trusted individuals, such as family members or authority figures. This technology significantly enhances the credibility of fraud attempts, making it difficult for victims to detect the deception.

AI-Assisted Conversations: AI-powered conversation systems allow scammers to respond dynamically to victims' reactions during real-time calls. This enables fraudsters to create a convincing narrative, adapting their approach based on the victim's level of suspicion or trust, leading to higher success rates.

Countermeasures Effectiveness: The study demonstrates the potential of AI-based countermeasures, such as AI-driven fraud detection systems, to mitigate the risks posed by these advanced scams. Sentiment analysis and voice mimicry detection are particularly effective in identifying fraudulent activities, especially in real-time communications.

These findings underscore the importance of continuous technological advancements in both fraud prevention and detection. They highlight the need for real-time, AI-driven solutions to keep up with the evolving tactics used by scammers.

4. DISCUSSION

This study demonstrates the effectiveness of an AI-based telephone fraud detection and prevention system, but it raises some critical questions about the practical application of such technologies. Given that fraud techniques are constantly evolving, it is essential to consider the long-term sustainability of these systems. In this discussion, we analyze the strengths and weaknesses of the developed system, compare the findings with existing literature, and explore future possibilities for improvement.

4.1 Advantages and Opportunities of AI in Fraud Detection

One of the primary strengths of the developed system is its ability to detect fraud in real-time using AI technologies such as sentiment analysis and voice mimicry detection. These methods offer significant protection against fraudsters who rely on manipulative techniques to gain victims' trust. With the rapid advancement of deepfake and voice imitation technologies, having a system capable of detecting such threats provides a critical safeguard for users.

Additionally, the system's real-time profile analysis allows it to target individuals based on their digital traces, which prevents personalized fraud attempts. These findings are consistent with other studies in the literature, particularly those examining AI's role in enhancing fraud prevention (Cialdini, 2006; Blauth et al., 2022). However, the holistic integration of voice mimicry detection into fraud prevention presents a novel contribution, filling a gap in previous research.

4.2. Limitations and Challenges

Despite promising results, this study also faces certain limitations. Data quality and diversity pose a challenge to the system's effectiveness. While the system was tested on a variety of fraud cases, a more extensive dataset would improve its accuracy in identifying different types of fraud across broader scenarios. Additionally, international applicability is a concern, as fraud methods and cultural differences in communication may affect the system's performance. Expanding the system to be tested across different countries and fraud types would help address these concerns.

Another challenge lies in the real-time performance and user feedback integration. The efficiency of AI algorithms is highly dependent on the quality of the training data, and as fraud tactics evolve, the system's ability to adapt must keep pace. Without continuous updates, the accuracy of fraud detection may diminish over time.

4.3. Comparison with Literature

The findings align with previous research in the field, particularly with regard to social engineering and persuasive techniques used by fraudsters. Studies such as Cialdini's (2006) work on social influence highlight how fraudsters exploit human psychology. Similarly, 'Bhargavi et al., 2024' research emphasizes the role of AI in fraud detection. What sets this study apart, however, is the emphasis on voice mimicry detection and its practical application. While much of the literature focuses on social engineering or phishing, this study adds value by exploring the intersection of AI and voice technology in fraud prevention.

4.4. Suggestions for Improvement

Several areas for improvement emerge from this study. First, the system should be expanded to cover other types of fraud, such as email phishing, social media scams, and identity theft. Enhancing the dataset to include diverse fraud methods would make the system more robust. Moreover, the cultural and linguistic adaptability of the system must be tested to ensure its international application.

Another crucial factor is user education. No matter how advanced the AI system is, user awareness plays a significant role in the overall effectiveness of fraud prevention. Providing users with educational resources and training on how to recognize fraud attempts would complement the system's technological capabilities.

4.5. Future Research Directions

The findings of this study open new avenues for future research. One of the most promising areas is the development of real-time adaptive systems and automated feedback loops to enhance the system's ability to respond to evolving fraud techniques. Additionally, the integration of AI into a broader ecosystem of fraud prevention tools, including biometrics and multi-factor authentication, could strengthen security measures.

Lastly, the study underscores the importance of ethical considerations in the use of AI for fraud prevention. As AI systems become more powerful, ensuring the privacy and security of user data must remain a priority. Future research should explore how to balance the benefits of AI with the need for ethical standards in fraud detection.

5. CONCLUSION AND RECOMMENDATIONS

Although AI technologies have significantly increased the complexity and impact of telephone fraud, various measures can be implemented to mitigate their misuse. The role of AI in combating fraud should extend beyond mere detection of fraudulent activities. It is, therefore, essential to develop filters that prevent AI tools from being exploited for fraudulent purposes and to design applications capable of identifying whether a fraud attempt is AI-generated.

Fraud Prevention Strategies

AI systems can continuously monitor user behavior to detect abnormal or suspicious activities. Accounts involved in fraud often exhibit unusual behavioral patterns, such as the frequent use of specific keywords or irregular calling frequencies. Monitoring such behaviors allows the system to automatically trigger alarms and intervene in real-time (Alzahrani, 2023).

Robust security protocols must be incorporated into AI products to prevent their use in fraudulent activities. Content filters can be implemented to limit the use of specific keywords or phrases. For example, frequent occurrences of terms like "urgent" or "immediate" should be flagged and reviewed automatically (Bhargavi et al., 2024).

Tightening user identity verification processes can make it more difficult for scammers to create fake accounts. Multi-factor authentication (MFA) and biometric verification methods have proven effective in thwarting fraud attempts.

AI-driven applications that analyze voice and speech patterns can help prevent scammers from deceiving victims. By evaluating tone, speed, and other linguistic features, these applications can determine whether a voice is AI-generated or real, thus identifying fraud attempts early on (Bhargavi et al., 2024).

Incorporating feedback mechanisms that allow users to quickly report suspected fraud attempts can significantly improve AI systems' fraud detection capabilities. User reports should be analyzed in real-time, with necessary precautions taken immediately to protect others (Sangwang et al., 2023).

RECOMMENDADITONS

There is a pressing need to develop AI-assisted applications tailored specifically to detect and prevent telephone fraud. These applications should provide real-time detection and protection for users, especially the elderly and those with low digital literacy, safeguarding their personal and financial information.

Educational initiatives should be implemented to increase public awareness of fraud techniques and prevention strategies. Informed users are better equipped to identify and resist fraud attempts (Alzahrani, 2023).

Fraud detection systems should integrate AI with sentiment analysis techniques. These systems will be able to automatically detect fraudulent communications, alert the relevant parties, and take immediate action.

Developing a specialized corpus for fraud detection is critical. This corpus should contain frequently used fraud-related words and phrases, enabling AI systems to adapt to new tactics more effectively and efficiently (Sangwang et al., 2023).

Future iterations of fraud detection applications should incorporate more advanced AI algorithms, continuously improving based on user feedback. These innovations will make fraud detection more accurate and comprehensive (Bhargavi et al., 2024).

Promoting the ethical use of AI in combating fraud is essential. By developing methods to counter AI-driven fraud, we can support the responsible use of these technologies, thereby increasing trust in AI-based systems and protecting users.

The findings of this study offer practical applications for the development of various strategies and technologies aimed at preventing telephone fraud. Techniques such as AI-based sentiment analysis and voice mimicry detection can safeguard users by identifying fraud attempts at an early stage. Furthermore, real-time profile analysis and security protocols can protect users' personal and financial data. AI-assisted applications designed for vulnerable populations, particularly the elderly, will play a crucial role in reducing fraud risks.

In comparison to existing studies, which often focus on singular AI methods, this study presents a more comprehensive perspective by integrating multiple AI techniques such as sentiment analysis, voice mimicry detection, and behavior profiling. This holistic approach makes significant contributions to the existing body of literature by addressing gaps related to the integration of various AI technologies in fraud prevention (Alzahrani, 2023).

Future research should explore the effectiveness of AI-based fraud detection methods across different age groups and demographic characteristics. Additionally, studies examining the cultural and social adaptability of these techniques could make fraud prevention strategies more applicable on a global scale (Bhargavi et al., 2024).

The development of AI-driven methods to prevent the misuse of these technologies in telephone fraud will enhance security for both individuals and organizations. Promoting ethical AI use will contribute to building trust in digital systems and protecting users from emerging threats. As AI continues to evolve, so too will the techniques for both fraud attempts and their prevention. We hope that the insights provided in this study will inspire future research and guide developers in creating more effective fraud prevention tools.

REFERENCES

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.). https://doi.org/10.1037/0000165-000

Alzahrani, R. A., & Aljabri, M. (2023). AI-based techniques for ad click fraud detection and prevention: Review and research directions. *Journal of Sensor and Actuator Networks*, 12(1), 4. https://doi.org/10.3390/jsan12010004

Al-Khazaali, A., Shakir, M., & Abdallah, S. (2023). AI-based model for fraud detection in bank systems. ResearchGate. https://www.researchgate.net/publication/376388638_AI-based_model_for_fraud_detection_in_bank_systems

Babu, P. B., Aswini, T. N., Vishnu, M. H. S., Gopiprashanth, B., & Reddyjanapala, B. S. (2024). Detecting and classifying fraudulent SMS and email with a robust machine learning approach. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 15(1), 109-112. https://doi.org/10.61841/turcomat.v15i1.14549

Bhargavi, D. K., & Shivani, B. M. (2024). Detection of fraudulent phone calls detection in mobile applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 15(2), 1-5. https://doi.org/10.61841/turcomat.v15i2.14644

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. IEEE Access, https://ieeexplore.ieee.org/abstract/document/9831441

Chandran, D. R. (2022). Use of AI voice authentication technology instead of traditional keypads in security devices. *Journal of Computer and Communications*, 10(6), 11-21. https://doi.org/10.4236/jcc.2022.106002

Çalışkan, M. (2018). Yeni nesil siber saldırılar ve korunma yolları. Journal of Polytechnic, 21(3), 733-741. https://dergipark.org.tr/tr/download/article-file/747841

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. Annual Review of Psychology, 55, 591-621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Cialdini, R. B. (2006). Influence: The psychology of persuasion (Rev. ed.). Harper Business.

European Public Prosecutor's Office. (2021). Aggravated customs fraud in Germany, Austria and Slovakia: Damage of more than €1.1 million to the EU budget. Retrieved June 16, 2024, from https://www.eppo.europa.eu/en/media/news/aggravated-customs-fraud-germany-austria-and-slovakia-damage-more-eu11-million-to-eu

FightCybercrime.org. (2023). The rise of AI in phishing scams: How scammers use it and how we can fight back. FightCybercrime.org. Retrieved from https://www.fightcybercrime.org/blog/the-rise-of-ai-in-phishing-scams/ (Accessed by VPN and membership method)

Financial Fraud Consortium. (2024). Fraud prevention and mitigation resources. https://www.fraudconsortium.org/

Global Engagement. IRS scams. Texas A&M University. Retrieved June 16, 2024, from https://global.tamu.edu/isss/resources/taxes/irs-scams

Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. https://www.jstor.org/stable/2092623

IdentityIQ. (2023). The rise of AI social engineering scams. IdentityIQ. Retrieved from https://www.identityiq.com/blog/the-rise-of-ai-social-engineering-scams/

Insights2Techinfo. (2024). Unmasking scam calls: Analyzing and detecting scammers using AI. Insights2Techinfo. https://insights2techinfo.com

Liu, J. (2021). *Understanding and defending against telephone scams with large-scale data analytics and machine learning systems* (Doctoral dissertation, University of Georgia). ProQuest Dissertations & Theses. https://www.proquest.com/openview/35085b2b8c0c312c0da2a24b97b9de18/1?pq-origsite=gscholar&cbl=18750&diss=y

Milani, A., Petrocchi, M., Pietro, R. D., & Spognardi, A. (2024). Chatbot-based emotional intelligence: A systematic review and new directions. Computers, 13(1), 5. https://doi.org/10.3390/computers13010005

Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1841-1848. https://doi.org/10.1016/j.chb.2013.02.014

Sangwan, R. S., Badr, Y., & Srinivasan, S. M. (2023). Cybersecurity for AI systems: A survey. Journal of Cybersecurity and Privacy, 3(2), 166-190. https://doi.org/10.3390/jcp3020010

Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020). Cyber threat detection using machine learning techniques: A performance evaluation perspective. *2020 International Conference on Cyber Warfare and Security (ICCWS)*, 1-6. https://doi.org/10.1109/ICCWS48432.2020.9292388

Subex. (2024). Harnessing generative AI and AI agents to tackle modern telecom fraud challenges. https://www.subex.com/ai/