IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI device that can determine one's identity using a code language at radio frequency over unsecured phone call communication

Ishaq Azhar Mohammed[#1], Sikender Mohsienuddin Mohammad[*2]

[#1]*Sr. Data Scientist & Department of Information Technology*

[#2] *Vice President & Department of Information Technology*

[#1]*Dubai, UAE*

[#2]*California, USA*

Abstract- *The main purpose of this paper is to develop an AI device that can determine one's identity using a code language at radio frequency over unsecured phone call communication. Because of the widespread use of smartphones, calls made via the cellular network account for the vast majority of call volumes globally at present. Because there are no cables involved in making a mobile phone call, anybody in the proximity of the phone may potentially intercept the transmission. When a mobile phone is used to make a call, the phone's initial action is to check the closest signal from the ground station antenna of the operator and establish a radio connection with that base station antenna [1]. The concept is the same for receiving a call, with the exception that the ground station antenna is the one that must create the connection. In this scenario, the operators will need to identify the network connection of the receiver to route the call properly. As a result, even when not in use for phone conversations, mobile devices "report" to the network – or update their apps (in the case of smartphones) – at periodic intervals while they are turned on and even if they're not making calls [1].*

For instance, the encryption used by the earlier 2G standard was very simple to decrypt. The fact that these loopholes were addressed when protocols were upgraded doesn't mean that subsequent versions of encryption provide complete protection either. When mobile phone networks were first developed, they were not intended to employ technological methods to prevent subscribers' calls from being intercepted [2]. This meant that anyone with a radio receiver of the appropriate kind could eavesdrop on the conversations. Thus, this paper will propose a method for an AI device to use a radio receiver to identify vulnerabilities in a coding language used in an unsecured phone conversation to determine an individual's identity.

Keywords: *Artificial intelligence, IMSI Catcher. radio frequency, code language, Network, IoT*

I. INTRODUCTION

When it comes to information transmission, various routes of communication provide a varying level of protection for the information sent. Some, such as landlines, are by their very nature more secured. Others, like VoIP, can only guarantee optimum safety when providers and consumers comply with specific requirements. A radio set is composed mostly of two components: a transmitter and a receiver. An electrical power source, as well as an antenna for the transmission and receiving of radio waves, are other components that are required for proper functioning [3]. It incorporates an oscillator, which is responsible for the generation of radio frequency (RF) energy to produce an alternating current (AC). The radiofrequency (RF) is sent to the antenna via a communication line or cable. When an alternating current is applied, the antenna transforms it into electromagnetic radiation that is then broadcast into space. The communication is controlled via the use of a keying device [1]. Most of the time, in single-channel radio communications, the receiver receives electromagnetic energy by transmitting it that uses the same antennas as the transmitters. The antenna is responsible for converting the electromagnetic energy received into the radio frequency of the alternate current. The radio-frequency (RF) signal is sent to the receiver via a transmission line or cable. The radiofrequency (RF) signal is transformed to audio frequencies in the receiver. The audio frequencies are subsequently converted into sound waves through a headphone or loudspeakers.

Unsecured phone call communication identification is a critical job for successfully detecting and combating fraud [1]. With the ongoing flow of unprotected telephone calls into other countries and the extensive use of VoIP and software

for modifying contact information in recent years, fraudulent telephone number change and becomes more hidden. As a consequence of these modifications, the conventional crowdsourcing approach that relies on a blacklist seems to be no longer reliable. Nevertheless, the fraudulent telephone call activity continually improves and changes, and the opposability increase [2,3,4] to prevent inquiries. The unpredictability of the spoofed contact information and the opposability of its call behavior provides a significant challenge in this identification exercise.

A new study from the 360 Internet Security Center as well as other prior studies reveals that there are distinct variations involving fraudulent phone conversations and frequent voice calls in call frequency, call duration, long-distance call rate, as well as other behaviors [4]. Although the unpredictability and variety of a fraudulent telephone number also apply, the mobile phone number itself has some regularity, including a non-standard number, foreign telephone number, short number, or counterpart number [5]. Many conventional machine learning methods are suggested in the domain of fraudulent phone call identification that makes use of the characteristics listed above.

With the associated studies, the issue of fraudulent phone call detection is addressed as an issue of classification. This issue is addressed by first carefully synthesizing features of a fake phone conversation and then categorizing these aspects using state-of-the-art artificial intelligence systems [5,6]. The engineering of features is a critical stage in conventional artificial intelligence. Feature engineering is a painstaking, time-consuming process that is built on accumulated expertise and personal experience. Several proposed methods [8] have demonstrated that identifying distinguishing characteristics is critical for the accurate detection of a fraudulent phone conversation. Furthermore, the costs of doing these activities are high due to the dynamic nature of fake phone numbers and the associated call patterns [7]. It has not been established if it is possible to effectively automate the extraction of features phase before categorization at this point by the scientific world. As a result, the automated and accurate identification of fraudulent phone conversations has become a difficult thing to achieve, and this is the primary issue that will be addressed in this research.

Using artificial intelligence, I present a new method for identifying a person's identity via an unprotected phone call communication by using a code language transmitted at radio frequency and based on radio frequency transmission. Since this method may include automated feature learning, it is not limited to a certain set of features [8,9]. Since this AI-based technology is intended to be adaptable to any disruptions in the characteristics provided by unprotected phone call communication, this may be a game-changer in the battle towards identifying individuals based on their code language. In this study, we propose the first automated phone call identification method, which surpasses state-of-the-art approaches in terms of accuracy and speed.

II. PROBLEM STATEMENT

The main problem that this paper will solve is to develop an AI device that will be much needed in identifying and tracking one's identity using a code language at radio frequency over the unsecured phone call communication. The telecommunications sector has been waging a long-running campaign against modern fraudulent activities using phone calls. Communication networks are changing at a fast pace across a wide technical context that encompasses virtualization, the Internet of Things, and Industry 4.0, among other factors [9]. This is addressed with a cybersecurity environment that is both wide and degrading at the same time. In the digital age, the telecom sector offers a wide range of services to its clients in addition to phone calls. Because of these expanded capabilities, the telecom sector has transformed into a veritable treasure of information. As a result, it has grown very vulnerable to dangers and other kinds of fraud. When you combine the enormous amount of electronic phone calls with the notion that any contact information may be spoofed, identifying telephone fraud is a challenging task to do successfully. My proposed device analyzes phone conversations to detect malicious actions and to verify that genuine callers are making the call [9,10]. The gadget captures an audio call and deconstructs it into distinct call characteristics to generate an audio fingerprint of a telecommunications network. Although scammers often switch contact information, it is far more difficult for them to alter the audio features that m device utilizes to generate a unique identity for the call audio features [11]. Technology upgrades are released regularly, opening the door to a variety of threats and vulnerabilities. To combat deception in the telecommunication sector, fraud management systems must be adjusted to be as effective as possible and to do so in real-time. Trends and patterns may be seen in all types of fraud [11]. In the past, conventional rule-based telecom fraud detection programs focusing on the capacity of humans to recognize trends and patterns to be effective.

III. LITERATURE REVIEW

A. Automated Identity Verification

The identity Verification procedure can now be simplified thanks to advancements in artificial intelligence technologies. A reliable artificial intelligence system may do this time-consuming procedure in a matter of minutes rather than hours. To solve this issue, we'll examine how an AI-based identification and authentication solution may assist [11,12]. On the one hand, artificial intelligence allows computers to make choices that are similar to those made by humans while also automating a certain function. It enables commonplace technology such as search engines, self-driving vehicles, and face recognition applications to function more effectively. When utilized with proper understanding, artificial intelligence can not only prevent online frauds and scams, but it can also play a key role in shaping financial irregularities a difference to the world. Clients' identities can be verified and correctly processed at a large-scale using machine learning techniques, according to another site's machine learning and deep learning capabilities [12,13].

B. Voice Recognition

This is the process of identifying a person by utilizing a collection of quantifiable qualities found in the human voice to create a complex algorithm that uniquely defines their voice. Artificial intelligence (AI) may be used to redact sensitive material from call records, such as personally identifiable information. Call records containing sensitive information may be erased or replaced with white noise if recognition algorithms for codes and keywords are used to identify the recordings [13]. When compared to speech recognition, speaker or voice recognition varies in that the former detect and identify the voice of the speaker using biometric features, while the latter evaluates the content of what is being spoken. Biometric authentication incorporates physical features, such as vocal tract architecture, which is essential for articulating and regulating voice output, as well as behavioral features such as pitch, cadence, and tone, etc. Voice biometric technologies use a technique known as voice fingerprinting to take each phrase and break it down into segments containing certain frequencies or formants [13]. These segments then become a unique voiceprint known as a voiceprint that can be matched to specific people. Such a voiceprint is for identifying and authenticating the speaker.

C. Case scenario

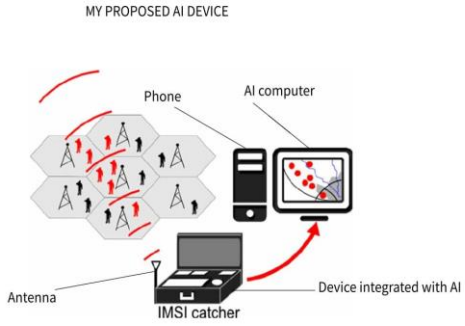
With the latest release of Apple's mobile operating system, its system will learn what human voice sounds like,

and Siri will be able to recognize people, disregarding other voices that attempt to interfere. Siri, Apple's sophisticated personal assistant, isn't the only one that recognizes the voice. Increasingly sophisticated voice-identification algorithms have begun to dominate daily life, from phones to government facilities to bank call centers, as learning software advances. More are almost certainly on the way. Research teams at Google released a study at the end of September in which they described a machine learning algorithm that could authenticate the identification of a person who said "OK Google" with an error margin of less than 2%. Vocalization is defined as a "physiological phenomena" that is influenced by the physical features as well as the languages people speak [13]. A voice is distinct from an individual's voice, which is distinct from another person's voice, which is distinct from the voice of everyone else on the other end of the continent, and so on. The most up-to-date machine-learning methods are capable of distinguishing even the smallest variations. Human voices can be recognized by computers, but interpreting what they are communicating is another matter. Large collections of voice data have been used to drive the development of a massive simulation of how individuals talk, which has been used to drive speech recognition [14]. This helps to identify whether someone's voice is theirs by allowing assessments of how much an individual's voice varies from the majority of the people. Variations in a person's voice as a result of illness or tension may cause the program to malfunction.

D. Proposed ai device

My proposed system will integrate an IMSI Catcher in its systems to intercept phone calls in unsecured phone communication. These phone calls will be relayed to an AI-programmed computer that will process code messages utilizing the matches that have been collected from the past communication of the user. My proposed device analyzes phone calls to identify malicious behavior and verify legitimate callers. It analyzes an audio call and divides it into distinct calling characteristics to generate a telephony network audio identity. Scammers keep changing contact information, but the changes in audio features are much more difficult to make a unique identity for the caller audio features. An RF signal decreases its intensity at a very fast pace when the antenna is disconnected. The RF signals of different frequencies are jammed within the radio frequency range. Consequently, the required signal should be selected and amplified by radiofrequency techniques. This is done using an RF amplifier. This is inserted in the receiver to improve selectivity and also to increase sensitivity (the capacity to pick a single frequency among several. Typically, the RF amplifiers utilize tunable circuitry to choose the frequency. By utilizing clusters on the similarity matrix across records analysts get transcript chunks and thus voice recording clusters. My proposed AI system aggregates call from several sources like phone numbers, allowing analysts to achieve the goal that most mobile device lines only connect once or twice via a network. The idea behind this is as shown below: if many calls from a certain telephone network are made, their voice features like the code language in the audio recordings will be analyzed and traced to a specific serial number of the caller who bought the phone. Criminal perpetrators prefer to utilize several different telephone numbers for unsecured telephone calls.

E. Design



F. How it works

This device works by picking up signals of phone communication by tricking and intercepting phone calls utilizing an IMSI Catcher. Once the phone is tricked into disclosing its IMSI, the IMSI catcher can establish the approximate position of the phone by monitoring the phone's network performance. Monitoring the signal strength from various places enables an ever-more-accurate estimate of the phone's position. IMSI Catchers are electronic devices that can "intercept" texts, phone conversations, and Internet data. This implies that others can read or listen to any private conversations. IMSI Catchers are capable of rerouting and editing conversations and data transmitted to and from the mobile phone, among other things. In addition, IMSI Catchers may restrict service to stop using a phone for making or receiving calls and text messages - even in emergency calls.

G. What is an IMSI Catcher?

An IMSI Catcher is an intrusive technology that may be used in a defined region for finding and tracking all mobile phones that have been switched on [15]. The IMSI Catcher does this by posing as a cell phone towers and tricking the phone into connected to it, at which point your personal information is revealed without anyone's knowledge. It is possible to monitor who organizes a political protest or a public event such as a sporting event using IMSI Catchers, which are unintentionally indiscriminate surveillance tools. They may also be used to monitor your phone conversations and alter your messages when you aren't even aware of what is going on around them [16,17]. They are devices that mimic cell towers to fool a target's smartphone into connecting to them, which subsequently relays the message to a real cell tower operated by the network provider. The IMSI Catcher intercepts all connections from the target, including phone conversations, text messages, internet traffic, and other forms of communication. The IMSI Catcher may read messages, listen to phone calls, and perform other functions. At the same time, the phone owner will be completely unaware of what is taking on since everything will seem to be functioning normally. In the area of information security, this is referred to as a Man-in-the-Middle attack.

This is conceivable as a result of a weakness in the GSM communication protocol. Mobile devices are always on the lookout for the telecom tower with the strongest signal to offer the most reliable commuting experience [16,17]. This is typically the one that is closest to you. A phone connects to a cellphone tower at the same time as it authenticates itself to

the tower by using an IMSI number. The tower, on the other hand, is not required to authenticate back. That's why, whenever anyone installs a device that serves as a cell tower close to the phone, their phone will connect to it and transmit its IMSI [17]. The SIM card's IMSI has a unique identification number. It is this unique number that is revealed when the phone has been tricked into connecting to an IMSI catcher. When the IMSI number is identified, it will be easy to identify someone's identity.

IV. FUTURE OF THE DEVICE IN THE U.S

With the increase in cybersecurity and cases of fraud, this technology will become more important for the United States in detecting those who engage in criminal activity. Their conversations will be readily intercepted, and their code language will be studied to understand the hidden message. This is a single crime solution that will aid numerous security agencies in the detection of phone fraud without impacting the experiences of low-risk callers [18,19]. Many situations can be dealt with properly to minimize the number of false positives. In addition, this solution offers an interactive user interface, which the engineering team can be used to analyze call data, monitor potentially fraudulent calls in real-time, and make decisions such as incident escalation. Many of the most important incident or case management systems are compatible with REST integration.

V. ECONOMIC BENEFITS

AI isn't a far-fetched concept; it's already here, and it's being integrated and implemented across a wide range of industries. Banking, national security, health care, crime prevention, infrastructure, and smart cities are just a few examples of the many areas covered. Innumerable instances exist where artificial intelligence is already having an effect on the world and enhancing human skills in important ways [17]. My proposed artificial intelligence technology is economically advantageous to the United States since it helps to reduce instances of identity theft, which cause significant losses to numerous businesses and the overall economy of the country. The amount of money invested in financial artificial intelligence in the United States more than quadrupled between 2013 and 2014, reaching a total of $12.2 billion [18].

Fraud detection is one example of how artificial intelligence may be beneficial in financial systems. In big companies, it may be difficult to distinguish between legitimate and fraudulent operations; nevertheless, artificial intelligence can detect anomalies, outliers, and deviant instances that need a further examination of conversations [18]. Because of this, managers can identify issues early in the cycle, before they escalate to critical levels. These advancements are intended to remove emotion from the investment process and allow investors to make decisions based on analytical factors in a matter of minutes rather than hours or days.

VI. CONCLUSION

This paper discussed the development of an artificial intelligence device that can determine a person's identity by transmitting a code language at radio frequency via an unsecured phone call communication channel utilizing code language. It is possible to locate and track all mobile phones that are turned on in a certain region using the device I designed, which makes use of the IMSI Catcher. This is a device that mimics cell towers to track a target's phone into connecting to them, which subsequently relays the message to a real cell tower operated by the network provider. The IMSI Catcher intercepts all communications from the target, including phone conversations, text messages, web traffic, and other forms of communication. The IMSI Catcher may read messages, monitor phone calls, and perform other functions. This technology will be useful in determining the identity of an individual based on the code language they use. The device's artificial intelligence capabilities enable it to evaluate code signals utilizing AI algorithms that have been trained to match previously collected data or to identify important features of the code language and anticipate what the primary message will be, among other things.

REFERENCES

[1] J. Scotland, "Using Texts Which Address Local Issues to Create a Discursive Space within an Undergraduate Writing Course", Journal of Language, Identity & Education, vol. 19, no. 4, pp. 260-274, 2019.

[2] R. Yager, "Using fuzzy measures for modeling human perception of uncertainty in artificial intelligence", Engineering Applications of Artificial Intelligence, vol. 87, p. 103228, 2020.

[3] R. Booth and J. Chandler, "From iterated revision to iterated contraction: Extending the Harper Identity", Artificial Intelligence, vol. 277, p. 103171, 2019.

[4] J. Jasrina, S. Yusof and M. Izhar, "Intelligent Selective Spectrum Access in Cognitive RadioNetworks", Journal of Artificial Intelligence, vol. 9, no. 4, pp. 65-71, 2016.

[5] A. Kazemy and H. Moodi, "Finite-frequency H∞ control design for T–S fuzzy systems with state/input delay and physical constraints", Engineering Applications of Artificial Intelligence, vol. 85, pp. 607-618, 2019.

[6] J. Cruz-Benito, S. Vishwakarma, F. Martin-Fernandez, and I. Faro, "Automated Source Code Generation and Auto-Completion Using Deep Learning: Comparing and Discussing Current Language Model-Related Approaches", AI, vol. 2, no. 1, pp. 1-16, 2021.

[7] H. Vu, "Only When I Am Not Ashamed of Myself Can I Teach Others": Preservice English-Language Teachers in Vietnam and Code-Switching Practices", Journal of Language, Identity & Education, vol. 16, no. 5, pp. 285-298, 2017.

[8] S. Sinha and C. George, "Artificial intelligence for all using R programming language", AI Matters, vol. 5, no. 4, pp. 10-13, 2020.

[9] K. Yamada and K. Ohuchi, "Error Estimation Scheme Using AMI Code for Detect-and-Forward Multi-hop Communications", Journal of Advances in Computer Networks, vol. 3, no. 2, pp. 127-133, 2015.

[10] L. Venema, "Code of conduct for using AI in healthcare", Nature Machine Intelligence, vol. 1, no. 6, pp. 265-266, 2019.

[11] J. Qadir, "Artificial intelligence-based cognitive routing for cognitive radio networks", Artificial Intelligence Review, vol. 45, no. 1, pp. 25-96, 2015.

[12] N. Soltanieh, Y. Norouzi, Y. Yang and N. Karmakar, "A Review of Radio Frequency Fingerprinting Techniques", IEEE Journal of Radio Frequency Identification, vol. 4, no. 3, pp. 222-233, 2020.

[13] A. Lilly, "IMSI catchers: hacking mobile communications", Network Security, vol. 2017, no. 2, pp. 5-7, 2017.

[14] J. Bar-Magen and Z. Zalevsky, "Remote objects detection and mapping using Radio Frequency with a Nexus 5X Smartphone", Scientific Phone Apps and Mobile Devices, 2019.

[15] I. Gabay, M. Danino and Z. Zalevsky, "Radiofrequency Echo mapping with cellular devices", Scientific Phone Apps and Mobile Devices, vol. 4, no. 1, 2018.

[16] P. Ney, I. Smith, G. Cadamuro and T. Kohno, "SeaGlass: Enabling City-Wide IMSI-Catcher Detection", Proceedings on Privacy Enhancing Technologies, vol. 2017, no. 3, pp. 39-56, 2017.

[17] J. Wallace, L. Diamantides, K. Ki and M. Butler, "Switched-Antenna Low-Frequency (LF) Radio-Frequency Identification (RFID) for Ornithology", IEEE Journal of Radio Frequency Identification, vol. 4, no. 2, pp. 137-145, 2020.

[18] P. Ziayi, S. Farmanbar, and M. Rezvani, "YAICD: Yet Another IMSI Catcher Detector in GSM", Security and Communication Networks, vol. 2021, pp. 1-13, 2021.

[19] A. Yurtman and B. Barshan, "Human Activity Recognition Using Tag-Based Radio Frequency Localization", Applied Artificial Intelligence, vol. 30, no. 2, pp. 153-179, 2016.