A Method for identifying cyberattacks based on the use of social engineering over the phone

Sergii Lysenko[1,†,*], Oleksandr Bokhonko[1,†], Volodymyr Vorobiyov[1,†], and Piotr Gaj[2,†]

[1] *Khmelnitsky National University, Khmelnitsky, Instytutska street 11, 29016, Ukraine*
[2] *Silesian University of Technology, ul. Akademicka 2A, 44-100 Gliwice, Poland*

Abstract
Identifying and mitigating cyberattacks involving social engineering over the phone is crucial for protecting individuals and organizations from potential threats. The paper presents the new for the identifying cyberattacks based on the use of social engineering over the phone. The core of the method is the usage of the so-called unique linguistic word identifier. Furthermore, the proposes approach deals with the language processing of the potential attackers' conversation and transforming it into the set of unique linguistic wording identifiers. As the mean of object classification, the KNN algorithm was involved. The obtained results demonstrated high efficiency of the attacks identification.

Keywords
cyberattack, social engineering, cybersecurity, cybercriminals, attack identification

1. Introduction

1.1. Motivation

In our interconnected digital age, the prevalence of cyberattacks continues to escalate, posing significant threats to individuals, businesses, and even nations. Among the myriad tactics employed by malicious actors, social engineering remains a pervasive and insidious method for gaining unauthorized access to sensitive information [1-2] This paper focuses on a specific facet of social engineering – its application over the phone – and proposes a novel method for identifying and mitigating cyberattacks perpetrated through this channel.

Social engineering over the phone involves manipulating individuals into divulging confidential information, such as passwords, personal details, or sensitive corporate data [3-5]. As technology advances, so do the tactics employed by cybercriminals, making it imperative for cybersecurity professionals to develop innovative strategies to combat these evolving threats [6-8].

IntelITSIS'2024: 5th International Workshop on Intelligent Information Technologies and Systems of Information Security, March 28, 2024, Khmelnytskyi, Ukraine
* Corresponding author.
† These authors contributed equally.
sirogyk@ukr.net (S. Lysenko); booweb24@gmail.com (O. Bokhonko); wworobyov@gmail.com (V. Vorobiov); piotr.gaj@polsl.pl (P. Gaj)
0000-0001-7243-8747 (S. Lysenko); 0000-0002-7228-9195 (O. Bokhonko); 0000-0002-2291-7341 (P. Gaj); 0000-0001-7738-1444 (V. Vorobiov)

Social engineering over the phone is a deceptive and manipulative technique employed by cybercriminals to exploit human psychology and extract sensitive information. In this method, attackers use various psychological tactics to convince individuals to divulge confidential data, such as passwords, personal details, or financial information, over a phone call. This form of social engineering leverages the natural inclination of individuals to trust and cooperate with seemingly legitimate authorities or entities [9-11].

Common tactics used in phone-based social engineering include impersonation of trusted entities, such as IT support personnel, bank representatives, or government officials. Attackers may employ sophisticated techniques to manipulate emotions, instill a sense of urgency, or create a false crisis to coerce individuals into providing sensitive information or performing actions that compromise their security.

Several techniques fall under the umbrella of phone-based social engineering, including: impersonation, pretexting, phishing calls, vishing (voice phishing).

Using the impersonation attackers may pose as someone the target knows and trusts, such as a colleague, manager, or IT support personnel, to gain access to sensitive information [!!!]. While pretexting attack attackers involve creating a fabricated scenario or pretext to obtain information. For example, an attacker might pretend to be conducting a survey, needing verification for an account, or seeking assistance with a supposed technical issue.

When attackers execute the phishing calls they may use deceptive tactics to trick individuals into revealing information by pretending to be from a legitimate organization, such as a bank, government agency, or a reputable service provider.

Vishing involves using voice communication to trick individuals into providing confidential information. This could include leaving voicemails with urgent messages, directing individuals to call back a fraudulent number, or manipulating call display information to appear trustworthy.

The success of phone-based social engineering often relies on exploiting human trust, creating a sense of urgency, and using psychological manipulation techniques. As technology evolves, attackers continuously adapt their tactics, making it essential for individuals and organizations to stay vigilant, implement security awareness training, and adopt countermeasures to detect and prevent such attacks. Combining technology, such as voice recognition and call verification, with education and awareness campaigns can enhance defenses against social engineering over the phone.

Let's consider an example of an attack in the form of a phone call from a fictitious international organization.

Hacker: Good afternoon, I am Oleksandr Petrenko, a representative of an international organization that provides assistance to Ukrainians affected by military operations.

Victim: Good afternoon. What questions do you have for me?

Hacker: We are informing you that our international organization intends to make a payment of non-refundable financial assistance to your bank payment card in the amount of 6500 UAH. You urgently need to contact your bank to open a payment card.

Victim: I already have an open payment card at the bank to which I receive my salary.

Hacker: Great. Then, in order to receive financial assistance, please give me your full bank payment card number and the short 3-digit number on the back of the card. We will credit you immediately.

In this situation there is a strong need to proceed the conversation and create the tool to identify the social engineering attack.

1.2. Objective of the research

The objective of this research is to introduce a comprehensive method for detecting and thwarting cyberattacks orchestrated through social engineering over the phone. By combining technological solutions with behavioral analysis and awareness campaigns, our proposed approach aims to enhance the resilience of individuals and organizations against these deceptive tactics.

This paper begins by providing an overview of the current landscape of cyber threats, emphasizing the increasing prevalence of social engineering attacks. Subsequently, it delves into the specific challenges posed by phone-based social engineering, exploring the psychological and technical aspects that make it a potent tool for cybercriminals.

The core of our proposed method involves a multi-layered defense mechanism that incorporates the k-nearest neighbors algorithm - a non-parametric, supervised learning classifier. It relies on proximity to categorize or forecast the grouping of a specific data point. Although it has applicability to both regression and classification tasks, it is predominantly employed as a classification algorithm based on the premise that points with similarities tend to be in close proximity to each other.

We argue that a holistic approach is necessary to address the multifaceted nature of social engineering attacks, which often exploit both technological vulnerabilities and human psychology.

Furthermore, this paper discusses real-world case studies and scenarios to illustrate the effectiveness of our method in identifying and mitigating phone-based social engineering attacks. By presenting empirical evidence and practical applications, we aim to underscore the feasibility and significance of our proposed approach in the realm of cybersecurity.

This research seeks to contribute to the ongoing discourse on cybersecurity by offering a robust method for identifying and combating cyberattacks facilitated through social engineering over the phone. As the digital landscape continues to evolve, it is crucial to develop proactive strategies that empower individuals and organizations to safeguard their information assets against the ever-present threat of social engineering attacks.

2. Related works

Article [12] discusses a method of detecting telephone fraud called CallMine. This method has the ability to process about 35 million records in about one hour on a regular computer, it is fully automatic and does not require user input. In the real world, on a large-scale dataset of millions of records, CallMine was able to detect fraudsters 7000 times faster than a human expert who took more than 10 months to do so.

Paper [13] presents a method that focuses on detecting telephone fraud based on the content of conversations. The developers collected descriptions of phone fraud from the media and social networks and used deep data mining techniques to select high quality descriptions of phone fraud to create relevant datasets. The authors use natural language processing to extract features from textual data.

For improved fraud detection in the telecommunications environment of the cloud, the authors establish criteria for identifying identical content within a single phone call and present an "Alert Algorithm" that can be installed on a customer's smartphone. This is an Android software that is downloaded once to the client's smartphone and automatically analyzes the call content to detect fraud when intrusion is detected.

In [14], in order to detect telephone fraud, the authors proposed "ScamBlk" - a machine learning approach based on voice recognition and natural language processing. "ScamBlk uses real conversation content obtained from audio recordings of calls, which is transcribed into text form, pre-processed, and fed to a machine learning model. The machine learning model uses an ensemble approach, including sequence collection (short-term and long-term memory network) and a linear model (support vector machine), to classify fraudulent phrases (sentences) in telephone conversations. Training of the machine learning model involves the use of an individual dataset that includes fraudulent phrases (sentences) obtained from various sources on the Internet. The ensemble model proves to be more efficient than other machine learning approaches, reaching an accuracy of 97.08%.

Article [15] provides an overview of artificial intelligence-based techniques for detecting and analyzing fraudulent phone calls. The researchers proposed a new approach to detecting fraudulent calls, which demonstrated high accuracy and precision. The effectiveness of the proposed method is the result of the researchers' use of a dataset containing real cases of fraudulent calls.

In [16], the researchers created a dataset of voice phone calls from YouTube videos, conducted experiments on voice classification using machine learning and MFCC features. A telephone fraud detection system was built that classifies speakers by their voice and uses them as identifiers. The support vector machine is the most accurate among the four machine learning classifiers compared in the study (94.46% accuracy using 68 MFCC features).

In [17], the authors propose a method for detecting telephone fraud based on the content of a spoken utterance. The researchers collected descriptions of telephone fraud from open sources. To generate datasets, this method uses machine learning techniques to analyze data and select high-quality descriptions from previously collected knowledge. Natural language processing is used to extract characteristics from textual data. For additional detection of phone fraud, criteria for identifying identical material within a single phone call are formed. The researchers proposed an Android application that can be installed on a user's smartphone; this software analyzes the content of an incoming call to detect potential fraud.

In [18], researchers used machine learning techniques as an effective method for detecting fraudsters in mobile communications. The fraud datasets are taken from the real environment of a telecommunications operator. The authors conducted various experiments with several popular machine learning classification algorithms to evaluate the effectiveness of this model.

In [19], the authors developed a methodology for semi-automated analysis of fraudulent calls and the extraction of information about fraudsters. The researchers used the community of "fraud catchers" on YouTube (people who deliberately interact with telephone fraudsters and publish their conversations). Of course, these conversations cannot be considered real fraudulent calls, but they provide a valuable opportunity to study fraudsters' scenarios and techniques, as fraudsters do not realize that they are not communicating with a potential victim of fraud. The researchers modeled the topics and time series along with identifying emotions to the fraudsters' statements, and identified social engineering techniques associated with the

identified stages of the scenario, including the visible use of emotions as a social engineering tool. This work is an important step towards understanding telephone fraud techniques, which forms the basis for more effective mechanisms for detecting and preventing telephone fraud.

In article [20], the authors present a method for detecting telephone fraud using a large language model (LLM). This is a type of artificial intelligence model that is trained on huge amounts of text data to understand and generate human-like text. These models are designed to process and generate natural language texts, so they are capable of performing tasks such as text generation, text classification, language translation, answering questions, and more. Large speech models are versatile and can be adapted to perform various natural language processing tasks with a minimum amount of task-specific training data.

In article [21], researchers proposed a solution that uses machine and deep learning methods to identify fake voices, based on artificial intelligence technology - Google Audio LM. This software can accurately reproduce intonation, accents, and other unique features by imitating the human voice. At the stage of feature extraction, the software uses the Mel Frequency Cepstral Coefficients (MFCC). These features are then classified using models based on machine and deep learning, and according to the results obtained, it is determined whether the voice is real or fake.

Paper [22] describes a method of using artificial intelligence to detect fraudulent phone calls based on a speech artificial intelligence model. With the user's permission, when the user receives a call from an unknown number, the call content is automatically transcribed and analyzed in real time to determine the likelihood of the call being suspicious. When such a call is found to be fraudulent, the user is notified accordingly. If the user grants permission, artificial intelligence based on a speech AI model can answer the call and have a conversation with the caller without user intervention. Speech AI can be trained to adapt to new strategies used by fraudsters.

Study [23] presents an approach to detecting fraudulent calls based on natural language processing (NLP). The aim of the study is to discover and explore new methods of combating social engineering attacks, as well as new methods of detecting and mitigating these attacks.

While there are existing methods for identifying cyberattacks based on the use of social engineering over the phone, these methods have certain drawbacks that highlight the need and motivation for creating new, more effective approaches. Existing methods may struggle to adapt to rapidly evolving social engineering tactics. Cyber attackers frequently modify their strategies, making it challenging for static identification methods to keep up with emerging threats. Another problem is the rate of false positives and false negatives. Some methods produce false positives, incorrectly identifying legitimate calls as potential threats, or false negatives, failing to detect actual social engineering attacks. These inaccuracies can lead to inefficient use of resources or missed opportunities to prevent cyber threats.

Social engineering attacks often involve voice spoofing, where attackers mimic trusted individuals or organizations. Existing methods may not effectively differentiate between genuine and spoofed voices, making it difficult to identify such attacks.

Traditional methods may lack context awareness, meaning they might not consider the broader context of a conversation or the relationship between individuals. This limitation can lead to misinterpretation of communication dynamics and hinder accurate threat detection.

Some current methods do not leverage advanced technologies, such as natural language processing, machine learning, or voice biometrics, which can enhance the accuracy and efficiency of social engineering attack identification.

Social engineering attacks exploit human psychology, and existing methods may not sufficiently incorporate behavioral analysis to detect subtle cues indicative of manipulation. Understanding and analyzing human behavior in the context of phone conversations is crucial for effective identification.

Some methods rely heavily on known patterns of social engineering attacks, which may not cover the full spectrum of tactics used by attackers. A new method should be designed to recognize both familiar and novel techniques employed by cybercriminals.

While threat intelligence is crucial for identifying emerging threats, existing methods may not fully integrate with comprehensive threat intelligence platforms. This can hinder the ability to detect and respond to the latest social engineering attack trends.

Thus, a new method for identifying cyberattacks based on the use of social engineering over the phone are to be developed to provide a more robust, accurate, and adaptive solution to enhance overall cybersecurity resilience.

3. A Method for identifying cyberattacks based on the use of social engineering over the phone

3.1. The Basis of the Method

In order to increase the efficiency of the identifying cyberattacks based on the use of social engineering over the phone a new method was produced.

This paper proposes a method that makes it possible to detect attacks over the phone based on the use of a unique linguistic word identifier. This identifier is similar to the signature method of detecting computer viruses.

The method is based on the use of language processing by breaking down sentences and words and forming a unique linguistic wording identifier.

The proposed approach operates with methods of natural language processing, in particular, the representation of textual information in the form of an n-dimensional vector.

One of the important aspects of the method for identifying cyberattacks based on the use of social engineering over the phone is the identification of a set of words used in the relevant attack. The specified set of words is characterized by a certain set of features and properties, which, when placed in vectors with their semantic proximity, are located next to each other.

Similarly, it is possible to build a set of sentences (phrases) used in the implementation of attacks, and with the help of which it is possible to identify the attack.

Method operates with the notion of the *unique linguistic wording identifier* – a specific verbal statement made by an attacker that not only conveys information but also encourages a certain action.

For example, the statement "I would like to have some tea, can you make some tea?" is a speech statement, as it instructs the listener to make tea.

We characterize the unique linguistic wording identifier (ULVI) as a set of verbal utterances that perform speech statement that are directly relate to the social engineering attacks over the phone. Just as a unique universal identifier for viruses identifies a specific type of virus, a fraud's ULVI clearly defines a class of social engineering attacks.

Let us denote the unique linguistic wording identifiers set as $I_1 = \{i_j\}_{j=1}^{N}$ – a set of ULVI the describe the attackers' conversation, where N is the number of unique linguistic wording identifier.

The examples of samples for the ULVI construction can be as follows:

I_1 = "National Bank Security Service, we would like to inform you that your payment card will be blocked";

I_2 = "You have been credited with non-refundable financial assistance from an international fund";

I_3 = "Tell us the full number of your payment card, PIN code, CVV code indicated on the back of the card";

I_4 = "You need to go to the nearest ATM to enter a special combination of numbers";

…

I_j = "Now you will receive a secret SMS code to your number, which you need to tell only to us".

3.2. K-Nearest neighbors as the unique linguistic wording identifier classification

K-Nearest Neighbors (K-NN) was applied to unique linguistic wording identifier classification tasks, where the goal is to categorize ULVI into different classes based on set of certain features. K-Nearest Neighbors is a viable approach for ULVI classification, particularly when dealing with datasets where the decision boundaries are complex and not easily captured by traditional models [24]. It is fine-tuning parameters and thoughtful feature selection are essential for achieving optimal results.

In order to implement the approach, the steps are to be executed: Data representation; Execute the training phase; Execute classification phase (attack identification).

Data representation includes the feature extraction and the feature vector construction procedures.

In order to build the unique linguistic wording identifier a set of relevant features are to be extracted. These features include aspects like stroke patterns, curvature, size, aspect ratio, and other characteristics that are distinctive for ULVI analysis.

The next step is the feature vector construction. Each ULVI's set of extracted features are to be presented as the feature vector. Each ULVI's feature vector represents its position in a multidimensional feature space.

Execution of the training phase includes the obtaining of the labeled dataset and feature scaling.

The next step is to prepare the labeled dataset where each unique linguistic wording identifier is associated with its corresponding class – malicious or benign phone call.

After that we are to perform the feature scaling procedure. This process consists of normalization of the feature values to ensure that all features contribute equally to the distance calculation.

Classification Phase includes the distance calculation, the neighbor selection, and the majority voting procedures.

During the classification phase it is important to evaluate the distance, that is when we are classifying a new ULVI, we have to calculate the distances between its feature vector and the

feature vectors of all ULVIs in the training set. To do this in the research the distance metric, Euclidean distance was involved:

$$d(x,y) = \sqrt{\sum_{i=1}^{n}(y_i - x_i)^2}. \quad (1)$$

After the distance evaluation the neighbor selection procedure is to be performed, where we are to select the K-nearest neighbors based on the calculated distances.

Ent the last step is to apply a majority voting scheme to determine the class of the new ULVI. The class that occurs most frequently among the K-nearest neighbors is assigned to the specified ULVI.

The pseudocode of the K-Nearest Neighbor is presented in Figure 1.

Algorithm 1 The K-Nearest Neighbor

```
Perform the loading of the training data
Prepare the training data: perform the scaling, treat the missing values, perform the dimensionality reduction
Perform the search for the optimal value K:
for i to n do
    Define the class values for new data
    Evaluate the distance(X, Xi), where X is the new data point, Xi is the training data, distance is the distance metric
    Perform the sorting of obtained distances in ascending order with corresponding train data
    Perform the selection of the top 'K' rows based on the sorted list.
    Perform the finding of the predicted class via defining the most frequent class from the chosen 'K' rows
end for
```

Figure 1: Algorithm 1 The K-Nearest Neighbor.

4. Experimental results

4.1. Basic Settings

In order to conduct experiments with the developed method for identifying cyberattacks based on the use of social engineering over the phone, the adapted dataset based on the CallHome, which is the part of the TalkBank project [26, 27]. It is a specific dataset or collection of data related to telephone conversations. The TalkBank project is a research initiative that focuses on collecting, analyzing, and sharing spoken language data for the purpose of studying various aspects of human communication and language development [27].

CallHome datasets typically involve recordings of telephone conversations in different languages and from various cultural contexts. These datasets are valuable resources for researchers in linguistics, communication studies, and related fields to investigate topics such as conversation analysis, sociolinguistics, and the development of language in naturalistic settings [26]. Another source cyberattacks based on the use of social engineering over the phone

was the bank security service of the biggest bank of Ukraine. Modified dataset included 1300 unique linguistic wording identifiers. For system test the 30 conversations were generated that included properties of the cyberattacks based on the use of social engineering over the phone.

4.2. Results

To assess the efficiency of the method for identifying cyberattacks based on the use of social engineering over the phone the metrics were involved: TPR – True Positive Rate, FPR – False Positive Rate, Precision, Recall, F1-score, and MCC were involved [25]:

$$FPR = \frac{TP}{TP + FN} * 100\,, \tag{2}$$

$$FPR = \frac{FP}{TN + FP} * 100, \tag{3}$$

$$S_P = \frac{TN}{TP + FN} * 100, \tag{4}$$

$$Precision = \frac{TP}{TP + FP'} \tag{5}$$

$$Recall = \frac{TP}{TP + FN'} \tag{6}$$

$$F1 = \frac{2 * Recall * Precision}{Recall + Precision}, \tag{7}$$

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}, \tag{8}$$

where MCC - Matthews Correlation Coefficient is a metric used to assess the quality of binary classification models, particularly when dealing with imbalanced datasets. It takes into account true positive, true negative, false positive, and false negative predictions, providing a balanced measure that considers all four outcomes. The MCC value ranges from -1 to +1, with +1 indicating perfect prediction, 0 indicating no better than random, and -1 suggesting total disagreement between predictions and actual outcomes. The results of the binary classification of the malicious and benign phone conversation for 30 experiments are presented in Table 1.

5. Discussion

The results of the proposed approach are highly promising but it has to be mentioned that the developed system is sensitive to the settings of the KNN algorithm parameters. Experiment with different values of K to find the optimal one for your dataset.

Cross-validation can help in this process. Select a distance metric that aligns with the characteristics of the signature features. Consider experimenting with different distance metrics to find the most suitable one. Properly preprocess the data, handle outliers, and select relevant features for signature classification.

Table 1
The results of the binary classification of the malicious and benign phone conversation for 30 experiments

Number of Attack	**Accuracy**	**Precision**	**Recall**	**F-score**
1	0,939	0,971	0,949	0,931
2	0,954	0,944	0,963	0,933
3	0,934	0,962	0,946	0,966
4	0,935	0,972	0,973	0,962
5	0,942	0,935	0,974	0,943
6	0,967	0,937	0,943	0,965
7	0,974	0,936	0,936	0,941
8	0,963	0,931	0,938	0,949
9	0,953	0,938	0,951	0,964
10	0,962	0,945	0,941	0,953
11	0,952	0,943	0,968	0,973
12	0,96	0,941	0,955	0,951
13	0,973	0,959	0,937	0,972
14	0,97	0,939	0,933	0,954
15	0,966	0,966	0,95	0,961
16	0,961	0,954	0,959	0,952
17	0,941	0,949	0,956	0,955
18	0,968	0,946	0,964	0,937
19	0,931	0,974	0,935	0,959
20	0,955	0,957	0,947	0,939
21	0,958	0,933	0,967	0,946
22	0,972	0,948	0,934	0,95
23	0,933	0,95	0,944	0,957
24	0,937	0,975	0,931	0,971
25	0,938	0,967	0,945	0,942
26	0,946	0,951	0,942	0,938
27	0,959	0,934	0,965	0,969
28	0,943	0,953	0,953	0,944
29	0,965	0,973	0,969	0,934
30	0,969	0,942	0,957	0,975

6. Conclusion and future work

Identifying and mitigating cyberattacks involving social engineering over the phone is crucial for protecting individuals and organizations from potential threats.

The paper presents the new for the identifying cyberattacks based on the use of social engineering over the phone. The core of the method is the usage of the so-called unique linguistic word identifier. Furthermore, the proposes approach deals with the language processing of the potential attackers' conversation and transforming it into the set of unique

linguistic wording identifiers. As the mean of object classification, the KNN algorithm was involved. The results demonstrated high efficiency of the attacks identification up to 97%.
Nevertheless, the future work has to implementing another machine learning models to improve the detection efficiency in order to analyze voice patterns, sentiment, or speech characteristics during phone conversations. The future method might involve training models to distinguish between normal and suspicious communication based on learned features.

References

[1] R. Alazaidah, A. Al-Shaikh, M. R. AL-Mousa, H. Khafajah, G. Samara, M. Alzyoud, S. Almatarneh. Website phishing detection using machine learning techniques. Journal of Statistics Applications & Probability, , 13(1), (2024) 119-129.

[2] G. Markowsky, O. Savenko, S. Lysenko, A. Nicheporuk, The technique for metamorphic viruses' detection based on its obfuscation features analysis, CEUR-WS. 2104 (2018) 680–687.

[3] K. Bobrovnikova, S. Lysenko, B. Savenko, P. Gaj, O. Savenko, Technique for IoT malware detection based on control flow graph analysis, Radioelectronic and Computer Systems. (2022) 141–153.

[4] S. Lysenko, O. Savenko, K. Bobrovnikova, DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy c-Means Clustering, CEUR-WS. 2104 (2018) 688-695.

[5] O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchuk, Multi-Agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic Communications, Computer and Information Science. 370 (2013) 243-254.

[6] K. Chetioui, B. Bah, A. Alami, A. Bahnasse, Overview of social engineering attacks on social networks, Procedia Computer Science. 198 (2022) 656-661.

[7] Z. Wang, H. Zhu, L. Sun, Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods, IEEE Access. 9 (2021) 11895–11910.

[8] S. Albladi, Weir, G.R.S. Predicting individuals' vulnerability to social engineering in social networks. Cybersecurity. 3 (2020) 7.

[9] K. Hughes-Larteya, M. Li, F. Botchey, Z. Qin, Human factor, a critical weak point in the information security of an organization's Internet of things, Heliyon. 7 (2021) 6522–6535.

[10] M. Govindankutty, Is human error paving way to cyber security? Int. Res. J. Eng. Technol. 8 (2021) 4174–4178.

[11] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, A. Ginther, A. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73 (2018) 345–358.

[12] Cazzolato, Mirela, CallMine: Fraud Detection and Visualization of Million-Scale Call Graphs, in: Proceedings of the 32nd ACM International Conference on Information and Knowledge Management, 2023, pp. 4509-4515. doi: 10.1145/3583780.3614662.

[13] E. Ogala , R. Ogala, M. U. Agbane , E. R. Adeiza, B. Tenuche, S. Sunday, Detecting Telecoms Fraud in a Cloud-Base Environment by Analyzing the Content of a Phone Conversation, Asian Journal of Research in Computer Science. 4(3) (2022) 115-131.

[14] M. Nandakumar, R. Nachiappan, Sunil, A.K., Neves, J.C., Proença, H.P., M. Sathiyanarayanan, ScamBlk: A Voice Recognition-Based Natural Language Processing Approach for the Detection of Telecommunication Fraud, in: Bashir, A.K., Fortino, G., Khanna, A., Gupta, D. (eds) Proceedings of International Conference on Computing and

Communication Networks, Lecture Notes in Networks and Systems, volume 394, Springer, Singapore, 2022, doi.org/10.1007/978-981-19-0604-6_47.
[15] S. Malhotra, G. Arora, R. Bathla, Detection and Analysis of Fraud Phone Calls using Artificial Intelligence, in: 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON), 01-03 May, 2023, IEEE Xplore ISBN:978-1-6654-9382-6, doi:10.1109/REEDCON57544.2023.10150631.
[16] Y.M. Rahman; Y. Bandung, Phone Call Speaker Classification using Machine Learning on MFCC Features for Scam Detection, in: 2022 6th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2023, doi:10.1109/ICITISEE57756.2022.10057625.
[17] D. Naidu, Voice analysis system for detection of vishing using deep learning, International Journal of Health Sciences. 6 (2022), 10457-10466.
[18] Krasić, S. Čelar, Telecom Fraud Detection with Machine Learning on Imbalanced Dataset, in:2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2022, pp. 1-6, doi: 10.23919/SoftCOM55329.2022.9911518.
[19] I. Wood, M. Kepkowski, L. Zinatullin, T. Darnley, M. A. Kaafar, An analysis of scam baiting calls: Identifying and extracting scam stages and scripts. (2023) Subjects:Cryptography and Security. arXiv preprint arXiv:2307.01965.
[20] J. Liming, Detecting Scams Using Large Language Models. arXiv preprint arXiv:2402.03147, 2024.
[21] H. H. Kilinc, F. Kaledibi, Audio Deepfake Detection by using Machine and Deep Learning, 2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM), Istanbul, Turkiye, 2023, pp. 1-5, doi: 10.1109/WINCOM59760.2023.10323004.
[22] Rao, K. Mallikarjuna, P. Bhavikkumar, Suspicious Call Detection and Mitigation Using Conversational AI, Technical Disclosure Commons. 04 (2023).
[23] C. J. Shalke, R. Achary, Social Engineering Attack and Scam Detection using Advanced Natural Langugae Processing Algorithm, in: 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 1749-1754, doi: 10.1109/ICOEI53556.2022.9776697.
[24] N. Hasan, N. Ahmed, S. M. Ali, Improving sporadic demand forecasting using a modified k-nearest neighbor framework. Engineering Applications of Artificial Intelligence. 2024. Vol. 129, 107633.
[25] D. Chicco, G. Jurman, The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. BioData Mining. 2023. Vol. 16 (1). Pp.1-23.
[26] B. Macwhinney, D. Fromm, Language Sample Analysis With TalkBank: An Update and Review, Frontiers in Communication. (2022) 7: 865498.
[27] Linguistic Data Consortium. University of Pennsylvania. CALLHOME American English Speech. URL: https://catalog.ldc.upenn.edu/LDC97S42.
[28] K.Bobrovnikova, M. Kapustian, D.Denysiuk, Research of machine learning based methods for cyberattacks detection in the internet of things infrastructure. Computer Systems and Information Technologies,. 3 (2022), pp.110–115. https://doi.org/10.31891/CSIT-2021-5-15.