

Phishing Attack Detection Using Convolutional Neural Networks

Siva Satya Sreedhar P

Department of Information
Technology Seshadri Rao
Gudlavalleru Engineering College,
Andhra Pradesh, India.
sivasatyasreedhar@gmail.com

Sravani Velpula

Department of Information
Technology Seshadri Rao
Gudlavalleru Engineering College,
Andhra Pradesh, India.
velpulasravani888@gmail.com

Rishwitha Parise

Department of Information Technology
Seshadri Rao Gudlavalleru Engineering
College, Andhra Pradesh, India.
rishwithaparise@gmail.com

Naidu Krishna vamsi

Department of Information
Technology Seshadri Rao
Gudlavalleru Engineering College,
Andhra Pradesh, India
krishnavamsinaidu999@gmail.com

Sakhamuri Krishna Chaitanya

Department of Information Technology
Seshadri Rao Gudlavalleru Engineering
College, Andhra Pradesh,
India
sakhamurikrishnachaitanya@gmail.com

Abstract—Phishing attacks are a prevalent form of social engineering that target individuals through emails to obtain confidential and sensitive information. These attacks can lead to larger security breaches in both corporate and government networks. There have been several attempts to counter phishing assaults, but so far none have proven successful. For this reason, improved strategies for identifying phishing attempts are desperately needed. The proposed fix is a deep learning-based strategy for identifying malicious phishing attempts. By analyzing more than 5,000 phishing emails sent at the University of Malaysia's Department of Computer Science and Information Technology, the authors hoped to create a model that reliably detects phishing assaults to achieve this, they selected relevant features through feature engineering and used the Random Forest models to extract feature importance at different levels. Finally, the model was trained using Convolutional Neural Networks (CNN), leading to improved detection and accuracy.

Keywords—Convolutional Neural Network; Phishing Attack; Deep Learning; Python – keras, Tensor flow; Accuracy.

I. INTRODUCTION

The dramatic rise in the frequency of phishing assaults in recent years has made this form of online fraud a serious problem in the modern Internet. Cybercriminals resort to fraudulent means, such as posing as a trustworthy third party, in order to get personal information from their victims [1]. The attackers create fake websites that mimic legitimate ones, such as Facebook, Amazon, and eBay, making it difficult for the average person to distinguish between the two [2]. The user is lured into accessing the fake website, which results in the attacker gaining access to sensitive information. Phishing scams and other forms of cybercrime have proliferated alongside the expansion of online shopping. These assaults are often executed by email, malicious websites, and malware [3 - 4].

Anti-Phishing Working Group (APWG), in 2020, an average of 225,759 phishing assaults occurred per month, a 220% increase from 2016. China is affected by 47.9 percent by phishing sites of infected machines. Phishing has become one of the most dangerous cyber threats, leading to economic losses of up to \$3.5 billion in 2019, according to

the FBI Internet Crime Center. However, these losses are likely under-reported.

A number of methods for identifying and preventing phishing scams have been developed in response to this growing threat. Methods using whitelists and blacklists, deep learning, machine learning, and heuristics are only a few examples of the different sorts of strategies that may be broken down by a review conducted by Mohammad et al [5].

The blacklist and whitelist approaches are quick, but their detection rate is poor and highly dependent on the number of sites included in the lists [6], [7]. Heuristic detection technology uses features extracted from multiple web pages and third-party services, such as website ranking and network traffic, to improve upon the blacklist techniques. As a result of the challenges involved in extracting characteristics from third-party services, this method is time-consuming and has a poor accuracy rate [8].

Although machine learning (ML) may be used to spot telltale signs of a phishing website's Uniform Resource Locator (URL), this method isn't without its limitations, such as the requirement for regular tweaks to the URL features, in addition to expert operation and expensive maintenance costs [9].

The increasing frequency and severity of phishing assaults has made them a major problem with far-reaching consequences. There are a number of methods for identifying phishing sites, each with its own set of benefits and drawbacks. To stay protected, it is important to stay vigilant and always verify the authenticity of websites before entering personal information [10], [11].

II. LITERATURE REVIEW

Fatima Salahdine et al [12] proposed that this method is using a machine learning-based method for detecting phishing attacks, they compiled and examined over 4,000 such messages that had been sent to email system. Modelling these assaults by picking 10 important characteristics and constructing a sizable dataset. Many machine learning methods were trained, validated, and

tested using this dataset. A total of four metrics detection probability, false alarm probability, false detection probability, and false detection probability had been utilized to assess the effectiveness of the system.

Abdul Basit et al [13] proposed that it permits researchers to recognize. There are a number of methods, challenges, and new developments that have been created to detect phishing assaults. The field of information security has recognized that blocking phishing attacks is challenging. Successful phishing attack detection requires a system with low false positive rates. In this research, they explore the use of deep learning algorithms, heuristics, machine learning, and data mining as preventative strategies. There is a larger cost per false positive when using heuristic and information mining approaches, but they are more successful at differentiating phishing attacks. The outcomes achieved by ML approaches are superior than those attained by other methods. Since malicious URLs are created on a regular basis and attackers utilize strategies to fool users and alter the URLs in order to attack, ML techniques provide superior results when compared to one-of-a-kind approaches.

Baoying Huang et al [14] stated that an effective solution for phishing detection is urgently needed to ensure a secure environment for investors. In this study, they propose a 3-stage framework for mining Ethereum transaction data to discover phishing frauds on Ethereum. They started by getting two legitimate websites to provide them labelled phishing accounts and the associated transaction data. They build an Ethereum transaction network using the collected data. For the following phishing categorization, they employ a community embedding technique called node2vec, which is able to extract the latent capacities of banknotes. Last but not least, the account is classified as a phishing account or not using a one-class support vector machine (SVM). Our model is supported by experiments that indicate our phishing detection system has an F-rating of 0.846%, an improvement above previous methods

Athulya. A A et al [15] explained the term "phishing" is used to describe the process of creating a fake yet convincing website in order to steal personal information from consumers.. Phishing scams are among the most common forms of online fraud. One of the threats that has been around for a while, but which continues to be a problem today is phishing. Different forms of phishing assaults, modern methods of evading phishing, and countermeasures against phishing. It educates users on the various phishing tactics and methods and shows them how to use anti-phishing browser extensions and other security software to protect their data. If you really want to put a stop to phishing, one of the things you can do is make sure your anti-phishing software is up to date.

Zunera Jalil et al [16] during COVID-19 it was put up that phishing assaults are currently one of the most severe risks faced by internet users, businesses, and service providers, particularly while working remotely. The goal of a phishing assault is to acquire sensitive information, such as a user's login credentials or credit card number, by means of email or website that appear legitimate but are actually fraudulent. The ground has been fertilized for the

introduction of cutting-edge phishing assaults by cybercriminals, hacktivists, and state-sponsored espionage organizations. Effectively detecting phishing attacks prior to user damage is possible with the use of machine learning techniques. Phishing attacks on a website can be uncovered by using this novel ensemble version. The K-Nearest Neighbors (KNN) classifier, the Decision Tree (DC) classifier, and the Random Forest Classifier are three machine learning classifiers you may use in an ensemble method (RFC). This ensemble method outperforms previous research at identifying phishing attacks on websites. Evidence from experiments shows that a combination of KNN and RFC is effective in identifying phishing attacks.

III. TRAINING SET

Preprocessing records is a not unusual place first step withinside the deep studying workflow to put together uncooked records in a layout and making it appropriate for a deep studying version. Feature significance is used to pick out the maximum relevant functions to teach the version. It additionally enables in detecting inappropriate functions, which reduces overfitting and development in performance. Thus, teach the CNN version via way of means of the usage of pinnacle 15 functions. Fig. 1 describes the working of the proposed block diagram. Finally, it detects the given URL is phishing or legitimate.

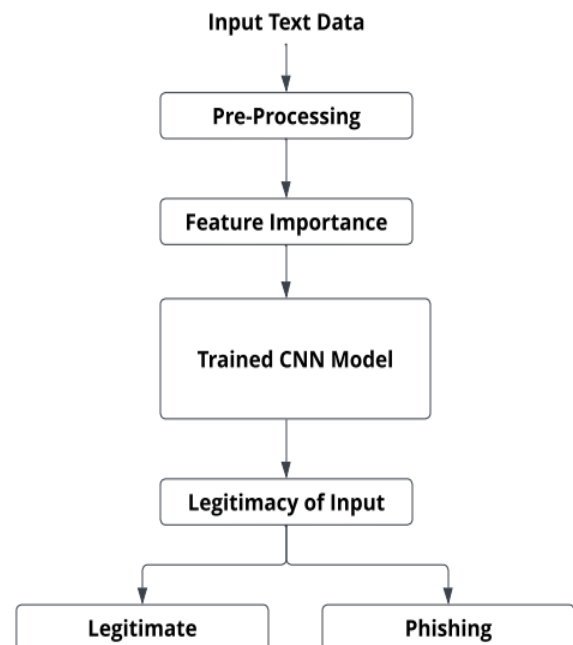


Fig. 1. Block Diagram of proposed work

The input data for training is taken from dataset Phishing Legitimate includes 48 extracted features. The input text data can be any URL of piece of text that the user wanted to test the legitimacy. In this case, here taken into account a variety of phished and authentic URLs for use in training and testing the system. Data preprocessing is a way to show the uncooked facts amassed from numerous re-assets into purifier data it is greater appropriate for work. In different words, it is an initial step that takes all the to be had data to prepare it, type it, and merge it. Pre-processing module is a

totally vital first step for all people coping with facts sets. That's as it ends in higher facts sets, which are purifier and are greater manageable, an ought to for any enterprise seeking to get precious data from the facts it gathers. Feature Importance module is vital to reap the maximum everyday functions or the gadgets that reason phishing. It is achieved earlier than version education, the most effective give attention to education the device with pinnacle 18 applicable functions. For acting characteristic significance, don't forget Random woodland class for similarly improving the performance.

To verify the veracity of user input text, this Deep Learning model is put into action. The most significant feature is selected from the feature significance module and used to train and evaluate the CNN model.

IV. PROPOSED WORK

A. System Design

The design of a system entails specifying its architecture, modules, components, their respective interfaces, and the information that flows through it. To put it simply, it's tailored to fit the demands of a certain business.

Analyzing the inner workings of a system by dissecting it into its component elements is called system analysis. It's a method for fixing issues and making ensuring everything in the system serves its intended function as well as possible.

Unified Modeling Language (UML) is a general-purpose modelling language that is widely adopted in the field of object-oriented software development. The Object Management Group is responsible for the development of this trend. The goal is to make UML the de facto language for representing software architectures in the realm of object-oriented computing. Currently, UML is made up of two main parts: the Meta-version and the notation. Some new forms of technique or procedure linked to UML will be introduced in the future.

The UML is a cutting-edge language used not just for software modelling, but also for enterprise modelling and other non-software systems. It is used for describing, visualizing, building, and documenting software system artefacts.

The UML is a collection of best engineering practices that have been proven effective in the modelling of large and complex systems.

The UML plays a crucial role in the creation of object-oriented software and the management of the software development process. The UML is a visual language for representing software projects' architectures.

The number one dreams withinside the layout of the UML are as follows:

In order to create and trade major models, you need provide consumers a Visual Modeling Language that is both expressive and easy to use.

Improve the fundamentals by incorporating methods for extension and specialization.

- Don't cling to any one programming language or method of development.

The modelling language needs a solid basis, so make sure you provide it one.

You should push for the OO gear industry to grow.

- Promote advanced improvement concepts including teamwork, structure, design patterns, and individual parts. Put together the best practices.

B. Activity Diagram

Like the flow chart in Fig. 2, an activity diagram depicts the progression of control from one activity to the next. To represent the dynamic nature of the system, employ an activity diagram here. This often entails simulating a computing process's individual phases in sequential order. Activity diagrams are also useful for modelling the transition of an item between states in a control flow. Control flow may be described with activity diagrams, but activity diagrams can also be used independently to visualize, specify, develop, and document the dynamics of a society of objects.

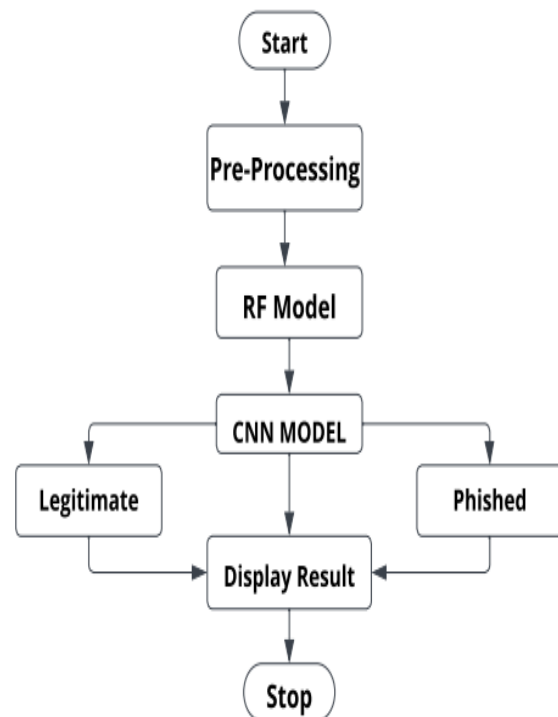


Fig. 2. Activity Diagram

C. State Chart Diagram

The flow of power from one kingdom to another is depicted on a state chart graphic. The existence of an object and the changes made to it throughout the course of a few events are referred to as a state. To model the whole existence of a product, from inception to decommissioning, is state chart diagram's primary function. Here is a description of the state diagram shown in Fig. 3.

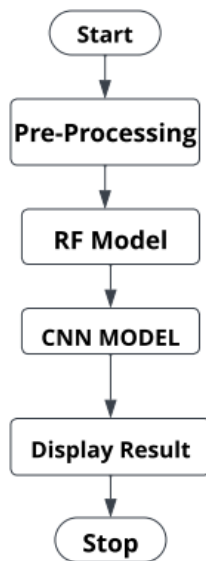


Fig. 3. State Chart Diagram

D. Data Flow Diagram

Fig. 4 explains that the input data that is pre-processed to remove discrepancy and then the clean data after pre-processing is used to build and RF module to obtain the feature importance. After obtaining the features the most relevant features obtained are used as train and test data to build CNN module. After CNN module is build it can use the system to detect phishing by passing manual input in required formats to determine the input to be legitimate or phishing.

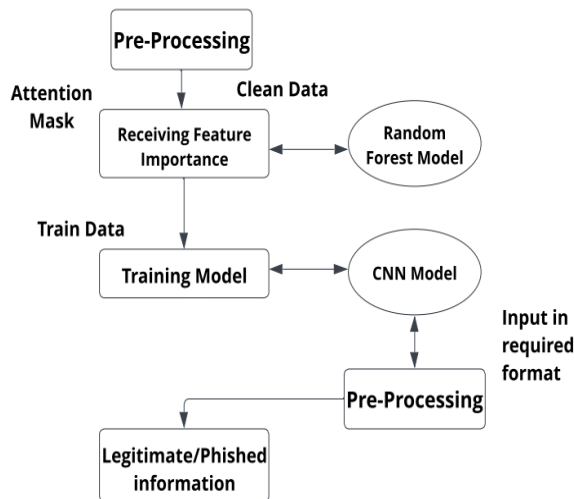


Fig. 4. Data Flow Diagram

E. Random Forest Model

Random Forest is widely used in ML for both classification and regression problems. Ensemble learning, the process of merging several classifiers to solve a difficult issue and improve the model's accuracy, is fundamental to its success.

The first step of Random Forest is to generate a randomly forested region by mixing N selected trees, and the second step is to make predictions for each tree generated in the first step. Here see the algorithm for the Random Forest Model in Fig. 5 below.

The working technique may be defined within the under steps and diagram:

Step-1: Select random K records factors from the education set.

Step-2: Build the selection bushes related to the chosen records factors (Subsets).

Step-3: Choose the range N for selection bushes which you need to build.

Step-4: Repeat Step 1 & 2.

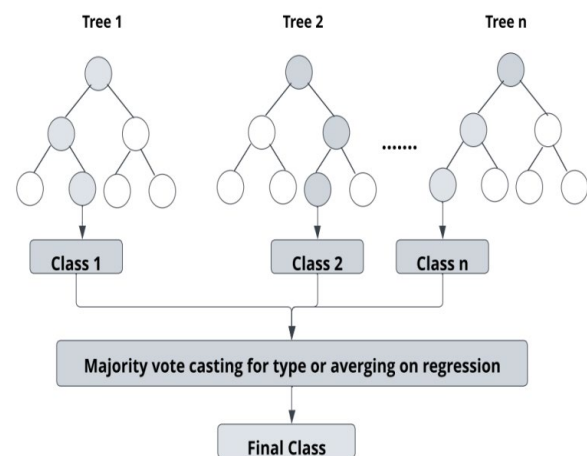


Fig. 5. Random Forest Model

V. RESULTS

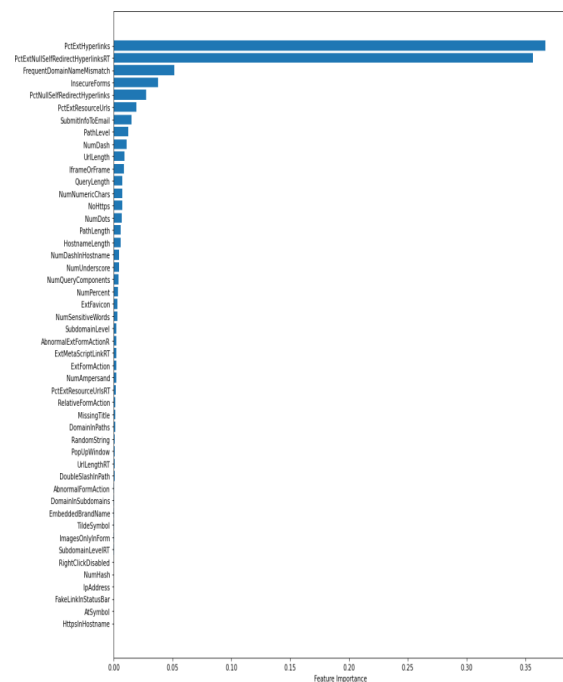
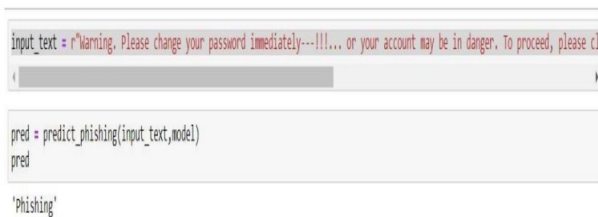


Fig. 6. Obtaining Feature Importance

Fig.6 describes the pre-processed dataset consists of Phishing Legitimate URLs with 48 extracted features. The dataset is balanced, it consists of precisely 50% phishing and 50% valid URLs. The bar graph representation of the feature importance, these features are further utilized to train the CNN module for detecting Phishing URL's. The model is trained with the obtained features with 90% train data and 10% test data. The model is trained with test and train data obtained from feature importance i.e., RFM module with splitting of data into 85% train data and 15% test data and executed through 10 epochs. Above the manual input text is provided i.e., URL and the output is determined to be Phishing as the URL is determined to be having feature of the phished website by the trained CNN model as shown below in the Fig. 7, Fig. 8.

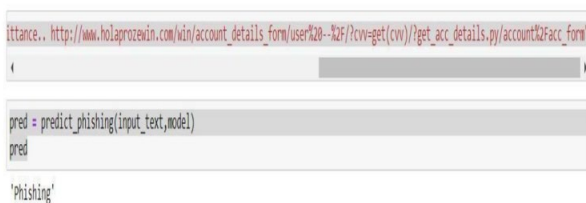


```
input_text = r"Warning, Please change your password immediately---!!!... or your account may be in danger. To proceed, please click here."

pred = predict_phishing(input_text,model)
pred
```

'Phishing'

Fig. 7. Testing of output 1



```
input_text = "http://www.holaprozwin.com/win/account_details_form/userk20--k2f/cvve-get(cvv)/get_acc_details.py/account2facc_form"

pred = predict_phishing(input_text,model)
pred
```

'Phishing'

Fig. 8. Testing of output 2

The most important cause of cell software useful checking out is to make sure the quality, assembly the required expectations, lowering the hazard or mistakes and client satisfaction. The software is useful examined and located that each one the required fields are working. The gadget is examined for overall performance and diagnosed to have highest quality reaction time with required responses. The software is examined for usability and it's far located to be steady easy and may be without difficulty operated via way of means of goal user.

TABLE 1. COMPARISON BETWEEN EXISTING METHODS AND OUR METHOD

	Accuracy
Proposed Method (CNN with RF)	98.68%
Basit A et al [13]	94%
M. Zafar et al [16]	97.33%

Comparing our method with the existing methods, our proposed method has an accuracy of 98.68% which is efficient and provides better accuracy than the existing methods as shown in the above Table 1

VI. CONCLUSION

The foremost purpose isn't always handiest figuring out phishing internet sites, however additionally to offer with

the viable centered domain. The level procedure wherein the primary level is primarily based totally on RDF version of the internet pages and the second one level is primarily based totally on CNN version. Both ranges paintings hand in hand to lessen the range of fake positives and to enhance the machine's accuracy. The CNN version labored with the accuracy of 98.68%. As a higher key-word extraction algorithm, our machine has very less, nearly 0 fake negatives. In future, the hybrid model of CNN with ML algorithms are to be proposed to achieve good accuracy.

REFERENCES

- [1] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based associative classification data mining," *Expert Systems with Applications*, vol. 41, no. 13, pp. 5948–5959, 2014.
- [2] Sen, G. Namata, M. Bilgic, L. Getoor, B. Galligher, and T. Eliassi-Rad, "Collective classification in network data," *AI magazine*, vol. 29, no. 3, pp. 93–93, 2008.
- [3] Ramesh, Gowtham and Ilango Krishnamurthi. "A comprehensive and efficacious architecture for detecting phishing webpages." *Comput. Secur.* 40 (2014): 23-37.
- [4] Ramesh, Gowtham et al. "Intelligent explanation generation system for phishing webpages by employing an inference system." *Behaviour & Information Technology*, 36 (2017): 1244 - 1260.
- [5] R. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, vol. 25, no. 2, pp. 443–458, 2014.
- [6] M. Mohammad, F. Thabtah, and L. McCluskey, "Intelligent rulebased phishing websites classification," *IET Information Security*, vol. 8, no. 3, pp. 153–160, 2014.
- [7] A. Joshi, P. Pattanshetti, and R. Tanuja, "Phishing attack detection using feature selection techniques," in *Nutan College of Engineering & Research, International Conference on Communication and Information Processing (ICCIP)*, 2019.
- [8] A. Subasi, E. Molah, F. Almkallawi, and T. J. Chaudhery, "Intelligent phishing website detection using random forest classifier," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. IEEE, 2017, pp. 1–5.
- [9] Salahdine, Fatima and Naima Kaabouch. "Social Engineering Attacks: A Survey." *Future Internet* 11 (2019): 89.
- [10] S. Navaneethan, P. Siva Satya Sreedhar, S. Padmakala and C. Senthilkumar, "The human eye pupil detection system using bat optimized deep learning architecture," *Computer Systems Science and Engineering*, vol. 46, no.1, pp. 125–135, 2023.
- [11] Salahdine, Fatima and Naima Kaabouch. "Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey." *Phys. Commun.* 39 (2020): 101001.
- [12] F. Salahdine, Z. El Mrabet and N. Kaabouch, "Phishing Attacks Detection A Machine Learning-Based Approach," *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2021, pp. 0250-0255.
- [13] Basit A, Zafar M, Liu X, Javed AR, Jalil Z, Kifayat K. A comprehensivesurvey of AI-enabled phishing attacks detection techniques. *Telecommun Syst.* 2021;76(1):139-154. doi: 10.1007/s11235-020-00733-2. Epub 2020 Oct 23.
- [14] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang and X. Zhang, "Detecting Phishing Scams on Ethereum Based on Transaction Records," *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, Seville, Spain, 2020, pp. 1-5.
- [15] A. A.A. and P. K., "Towards the Detection of Phishing Attacks," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)*(48184), Tirunelveli, India, 2020, pp. 337-343.
- [16] M. Zafar, A. R. Javed and Z. Jalil, "A Novel Ensemble Machine Learning Method to Detect Phishing Attack," *2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 2020, pp. 1-5, doi: 10.1109/INMIC50486.2020.9318210.