DS Journal of Cyber Security
Volume 1 Issue 1, 39-45, Jul - Sep 2023
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V1I1P104

Original Article

Phishing Attacks Detection Using Convolutional Dense Neural Network

R. Surendiran

School of Information Science, Annai College of Arts and Science, Tamilnadu, India.

surendiranmca@gmail.com

Received: 29 May 2023; Revised: 10 June 2023; Accepted: 23 June 2023; Published: 6 July 2023;

Abstract - The term "cyber security" covers all aspects of safeguarding an existing performance, customers, and activities from internet threats. The advancing digital transformation has led to an increase in cybersecurity risks on a global scale. The possibilities for cybercriminals are made deeper by technology. Cyberattacks sometimes begin as phishing efforts to get secret user passwords. Attackers frequently employ phishing to deceive individuals into giving them access to networks and digital assets inside an organisation. Cybercriminals use security flaws to conduct attacks, gain unauthorised access, disable systems, and even charge a fee for access to be restored. The phishers use strategies to get beyond anti-phishing software and tools. Cybersecurity is still the best method for preventing phishing efforts, even though threat intelligence and perception solutions aid enterprises in identifying unusual traffic patterns. In light of this, the suggested Phishing Attack Detection (PAD) research project has developed an approach that uses Convolutional Dense Neural Networks (CDNNs) to identify phishing threats. Initially, the data are pre-processed using a data mining technique to remove the noise from the data. Based on pre-processed data, CDNN is utilised to categorise the attacks. Finally, a maximum accuracy of suggested (PAD) of 97% was accomplished using existing random approaches.

Keywords - Cyber security, Artificial Intelligence, Deep Learning, Convolutional Dense Neural Networks, Phishing attack detection.

1. Introduction

Phishing emails, which appear to be from a reputable source, actually arrive from cybercriminals who seek to trick you into giving them your personal information. In these emails, cybercriminals typically use intimidation tactics, threatening to terminate those accounts or have you arrested if you do not give the information they normally keep secret.

Users should be aware of phishing assaults. The privacy and financial security of internet users are gravely compromised. A type of scammer build fake websites [1, 2] to appear and feel authentic and trick visitors. They create false emails in order to steal the identities of real people. Credit card numbers, passwords, account details, and the user's sensitive information are all collected during the transaction. They constantly change their methods of attack. One of the key methods used is social engineering [3]. This method allows them to obtain personal information from a reliable source. Phishers make fake websites and spoof emails [4], often making them look nearly identical to the websites of legitimate companies. In hopes of pressuring people into updating their systems, attackers have been known to assume the identity of trustworthy sources.

However, they endanger suspending the client's account and demand a release. Here, another technique used for phishing deception is network message spoofing. Consumers are frequently scammed into disclosing sensitive data like credit card numbers and passwords. Thus, the principal intent is to steal sensitive information, including bank accounts, passwords, and credit card numbers. Due to the increasing growth of this form of fraud, consumers and business people are beginning to lose faith in online trade. Due to their lack of faith in online transactions, customers started to have a negative image of internet companies. Attacks are still a threat even if machines are outfitted with encryption software [5] to protect the data they save. The detection in this paper was carried out using DL.

The remaining section of this work is structured as follows. The literature review is covered in section 2. It stands in for the proposed technique in section 3. The results and discussions are reported in section 4. The conclusion is covered in section 5.

2. Literature Survey

Phishing attacks can take many different kinds and are intended to deceive users. Various phishing detection techniques and technologies are also available to prevent phishing efforts. One of the methods used to identify website phishing is classification. Here are descriptions of typical phishing attack types and classification strategies.

[6] Combining a knowledge base system and a Simulated Expert (SE), Sajid Anwar, F. et al. offer a unique way 2019 to identify malicious Uniform Resource Locators (URLs) , providing a defence against freshly produced harmful URLs. The experimental results clearly demonstrate that NB is effective in the proposed model since it outperforms the other algorithms in terms of average minimum execution time (i.e., 3 s) and can successfully identify 107 586 URLs with a 0.2% error rate and 99.8% accuracy rate.

[7] Tong Anh Tuan H. et al., experimental examination of machine learning techniques for botnet DDoS attack detection was proposed in 2019. The UNBS-NB 15 and KDD 99 publicity datasets for Botnet DDoS attack identification are used in the evaluation. Support Vector Machines (SVM) are extensively employed in machine learning. When compared to the UNBS-NB 15 dataset, the results were better. In the disciplines of computer security and other related areas, this validation is important.

[8] Ammara Zamir, T. et al. want to provide a framework in 2020 that uses a stacking model to identify phishing websites. The attackers access users' sensitive and private information for financial gain. The suggested and remaining features are submitted to principal component analysis utilising a range of Deep Learning approaches, including Neural Network (NN), Random Forest (RF), Support Vector Machine, Bagging, k-Nearest Neighbour, and Naive Bayes. The outcomes demonstrate that RFE is crucial in removing the least significant feature from the data set.

[9] In 2020, Gunikhan Sonowal, S. et al. introduced PhiDMA a multilayer model called Phishing Detection using Multi-filter Approach used to spot phishing. The PhiDMA model consists of five layers: an auto-update whitelist layer, a layer for URL attributes, a layer for lexical signatures, a layer for string matching, and a layer for comparing accessibility scores. The outcome demonstrates that with a 92.72% accuracy rate, the algorithm was able to recognise phishing websites.

[10] In 2020, Nureni Ayofe Azeez, B. and others, several anti-phishing models have been put forth to protect internet users against phishing attacks. Finding the forensic features of a phishing assault can help both allow defence against it and find the attack's perpetrators. The proposed phish detect approach may be implemented with an accuracy of 99.1%, proving its efficacy in identifying different types of phishing assaults.

[11] Edwin Donald Frauenstein, S. and colleagues presented a theoretical strategy to overcome the phishing risk on SNSs in 2020. Using data gathered from 215 respondents, the study examined the mediating role of information processing with regard to user susceptibility to social network phishing. According to the findings of the Structural Equation Modelling (SEM) inquiry, people are often less susceptible to phishing on SNSs because it has been established that they have a negative impact on predictive processing.

[12] Ahmet Selman Bozkir, M. et al. provide a complementary methodology to identify and categorise the target brand logos present in page screenshots in 2020 "zero hour" phishing websites using only computer vision algorithms in an object detection manner. Many research has been conducted to combat this security concern using various information sources, including URLs, text content, etc. As a result, in terms of detection precision and run-time effectiveness, LogoSENSE offers encouraging results.

To secure web users, phishing attempts can be fought using various strategies. Due to the fact that criminals frequently change their strategies, online fraud and URL phishing efforts are among the most challenging to identify and stop. It was advised to block malicious emails and fake links to stop this kind of phishing.

3. Proposed Methodology

This section covers the suggested framework as well as how to identify phishing attacks using Deep Learning (DL). DL techniques were employed in the experiment. There are two ways to apply DL methods. Unsupervised learning is the second option after supervised learning. The choice of features is essential for DL algorithms. It lessens the redundant data in the data sets that are superfluous or unnecessary. Convolutional Dense Neural Network (CDNN), a different statistical technique, has been applied to categorise the datasets and identify the elements of the variables.

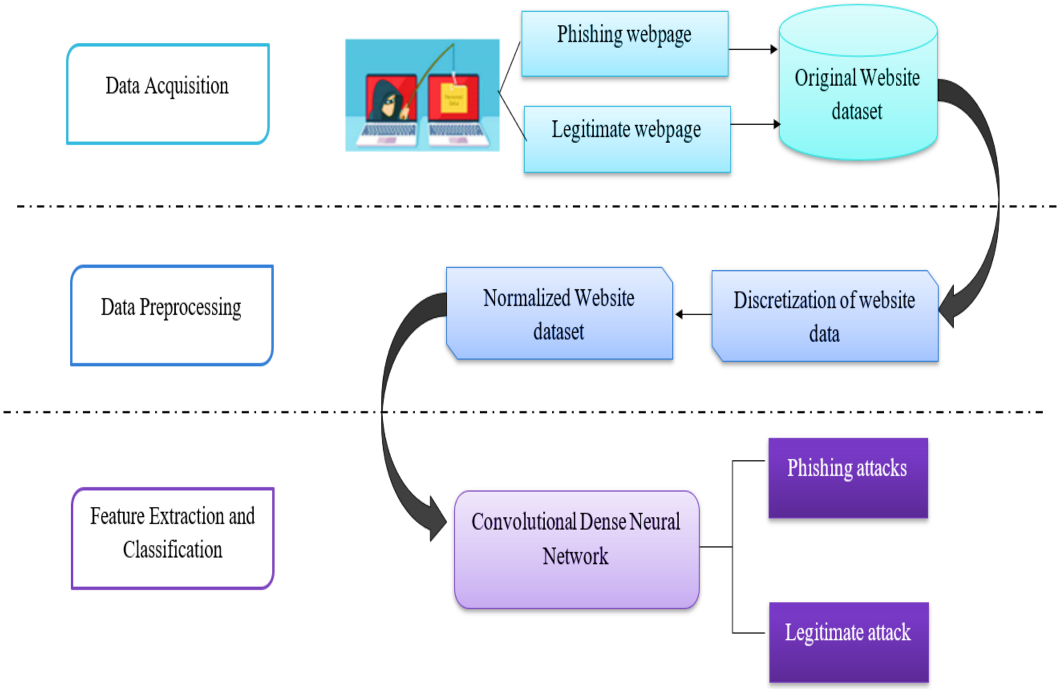
Data Acquisition
Phishing webpage
Legitimate webpage
Original Website dataset
Data Preprocessing
Normalized Website dataset
Discretization of website data
Feature Extraction and Classification
Convolutional Dense Neural Network
Phishing attacks
Legitimate attack

Fig. 1 Schematic representation of the proposed model

Figure 1 shows how the suggested model was displayed. First, the dataset was chosen in order to test the phishing website. A feature selection method was used to analyse the properties. For feature selection in the suggested model, the REF algorithm was employed. The feature is further divided into the weakest and the strongest. CDNN was then used for analysis.

3.1. Data Gathering

We used datasets from kaggle.com since they are essential for data analysis in our study.

Table 1. The phishing dataset

Feature	Description
IP Address	If IP address exists in URL-> phishy else->legit
URL's having @symbol	If URLhas ;'@'-> phishy else-> phishy
Adding prefix or suffix	If domain part has '-'-> phishy else->phishy
Abnormal URL	No hostname in URL-> phishy else->legit
DNS record	No DNS record-> phishy else->legit

3.2. Data Pre-Processing

In the DL application, pre-processing data is a critical step. It was produced utilising data mining to format raw, unformatted data. The dataset analysis required a clear and noise-free dataset. Most of the dataset had missing and partial data values, which were filled up and finished for DL processing.

3.2.1. Feature Description

The selection of features is a crucial step in analysing the dataset. Features were present in our dataset. Whether they were suspicious or malicious can be assumed based on the information on the features. Table 2 provides explanations of the features.

Table 2. Feature description

Feature Name	Feature Explanation
Index	Indexing could be used for the web page to display in the search engine
Age of Domain	Duration of the domain that has existed
Google Index	Add web pages in google search
Links Pointing to Page	Used to rank the web pages
Class	Contains attributes and behave

3.3. Modeling Using Deep Learning and Classifier

In order to identify the classification and find cyberattacks, supervised learning techniques are used. This strategy uses data that has already been processed to estimate new data. This study employs two well-known Deep Learning algorithms to identify phishing attempts.

3.3.1. Convolutional Dense Neural Network

The DL can learn patterns from the data and anticipate solutions for situations that are similar in the future. The human brain's neural network served as inspiration for Neural Networks (NN). The area of Artificial Intelligence known as computer vision focuses on graphics issues. Combining CNN with computer vision enables it to carry out difficult tasks like classifying images and resolving scientific issues.

The layers of the Deep Learning model can be thought of as its architecture. The models can make use of a variety of layers. Every one of their several layers offers a unique significance based on their characteristics. The dense layer also referred to as a completely linked layer, is used in the last phases of the neural network. This layer serves to change the dimensionality of the output over the previous layer to make it easier for the model to determine the interactions among the values for the data it is working with.

A CDNN-based model that makes use of CDNN's capacity to distinguish between authentic and phishing websites. The model assessed a dataset of websites that included 4898 phishing sites and 6157 authentic sites, respectively. This model is used to identify phishing network web that is not visible. Also, the model's Phishing detection rate and F1 score increased by 0.978 and 98.2%, respectively.

4. Result and Discussion

In this study, data analysis on the chosen dataset was done to detect phishing attacks using feature analysis. The multiple regression displays the accuracy performance table in relation to the dataset's actual classifications.

4.1. Performance Evaluation

Based on the confusion matrix, it was conducted using accuracy, precision, recall, and F1 score (Figures 2 and 3)—multiple regression estimated performance with a given database table.

4.1.1. Accuracy

The accuracy of all correctly predicted categories to the dataset's actual classifications represents the prediction algorithm's accuracy. Equation (1) determines the model's accuracy. Each prediction model typically yields four distinct outputs: True Negative (TN), True Positive (TP), False Negative (FN) and False Positive (FP).

$$Accuracy = \frac{TP+TN}{TP+TN+FN+FP} \tag{1}$$

4.1.2. Precision

The percentage of phishing websites successfully identified as real phishing websites represents the prediction algorithm's accuracy. Equation (2) calculates the precision of the model.

$$Precision = \frac{TP}{TP+FP} = \frac{True\ position}{Total\ predicted\ position} \tag{2}$$

4.1.3. Recall

The amount of accurate phishing URL predictions made over all URLs in the dataset is known as the prediction algorithm's recall. Equation (3) determines the model's recall.

$$Recall = \frac{TP}{TP+FN} = \frac{True\ position}{Total\ prediction\ position} \tag{3}$$

4.1.4. F1 Score

The method for calculating the harmonic mean of a classifier's precision and recall. It is possible to turn it into a single metric. Equation (4) determines the model's F1 score.

$$F1\ score = \frac{2\times(precision\times recall)}{(precision+recall)} \tag{4}$$

4.2. Performance Metrics

Figure 2 shows the accuracy and F1 score of comparative analysis with existing and proposed methods. The existing RFE, PDM, and SEM are compared with the proposed PAD method. Precision, recall, and accuracy metrics were used to analyse the prediction results.

4.2.1. Accuracy and F1 Score

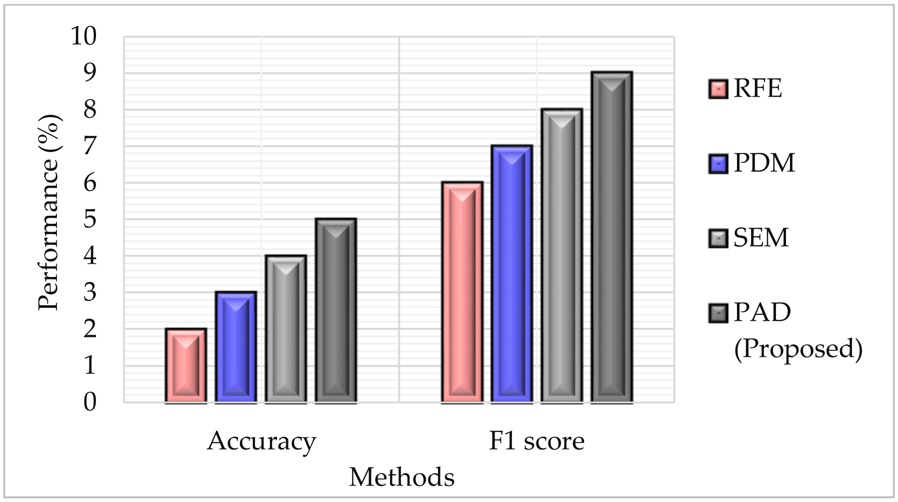

Fig. 2 Comparative analysis with existing and proposed method

The proposed PAD is high in comparison to other existing approaches. The size of the F1 is 0<100 in size, shown in Figure 2.

4.2.2. Recall and Precision

Figure 3 shows the Recall and precision of comparative analysis with existing and proposed methods. The existing RFE, PDM, and SEM are compared with the proposed PAD method. Precision, recall, and accuracy metrics were used to analyse the prediction results.

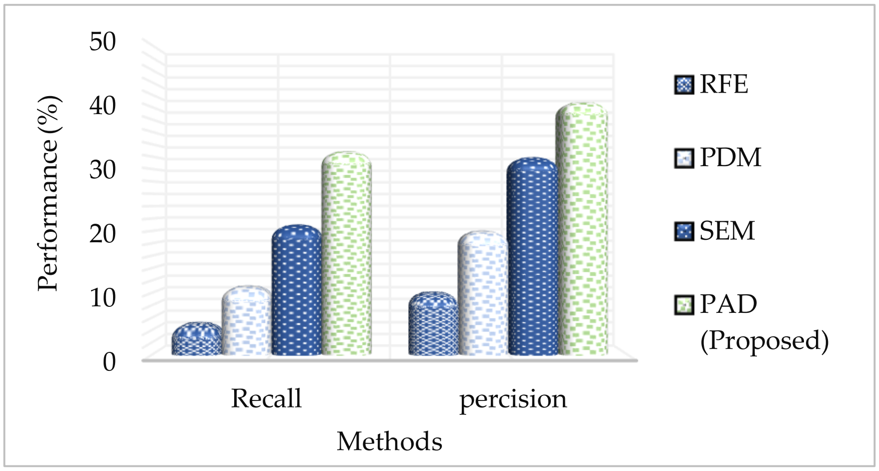

Fig. 3 Comparative analysis with the existing and proposed method

The proposed PAD is high in comparison to other existing approaches. The size of the F1 is 0<100 in size, shown in Figure 3.

- True Positive (TP) : The actual phishing URLs and correctly predicted phishing URLs were both found.
- False Negative (FN) : Safe URLs were used to identify the true phishing sites.
- False Positive (FP) : The real URLs itself were identified as phishing URLs and labelled as false values.
- True Negative (TN) : Both the real and expected classes were similar.

5. Conclusion

In the suggested research, Convolutional Dense Neural Networks (CDNNs) were used to create a model to identify phishing assaults. Initially, the data are pre-processed using a data mining technique to remove the noise from the data. CDNN is used to classify the attacks based on pre-processed data. DL techniques were employed in the experiment. There are two ways to apply DL methods. Unsupervised learning is the second option after supervised learning. Feature extraction is essential for DL algorithms. The majority dataset had missing and partial values, which were filled up and finished for DL processing. The selection of features is a crucial step in the analysis of the dataset. A CDNN-based model that makes use of CDNN's capacity to distinguish between authentic and malicious websites. The model evaluated a dataset of websites that included 4898 phishing websites and 6157 authentic websites, respectively. The model is used to identify phishing websites that are not visible. Also, the model's phishing detection rate and F1 score increased by 0.978 and 98.2%, respectively. Data analysis on the chosen dataset was performed in this study in order to detect phishing assaults using feature analysis. The confusion matrix compares the accuracy performance table to the actual classifications in the dataset. While evaluating performance, accuracy, precision, recall, and F1 score which were determined using the prediction model used. Finally, a maximum accuracy of the proposed (PAD) with 97% was achieved through the random existing methods.

References

[1] Samaneh Mahdavifar, and Ali A. Ghorbani, "Dennes: Deep Embedded Neural Network Expert System for Detecting Cyber Attacks," *Neural Computing & Applications*, pp. 14753–14780, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Sandhya Mishra, and Devpriya Soni, "Smishing Detector: A Security Model to Detect Smishing through SMS Content Analysis and URL Behavior Analysis," *Future Generation Computer Systems*, vol. 108, pp. 803-815, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Kayode Sakariyah Adewole et al., "Twitter Spam Account Detection Based on Clustering and Classification Methods," *Journal of Supercomputing*, vol. 76, no. 7, pp. 4802-4837, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Hang Hu, and Gang Wang, "End-to-End Measurements of Email Spoofing Attacks," *USENIX Security Symposium*, pp. 1095-1112, 2018. [Google Scholar] [Publisher Link]

[5] Mirkhon Nurullaev, and Aloev Rakhmatillo Djuraevich, "Software, Algorithms and Methods of Data Encryption Based on National Standards," *IIUM Engineering Journal*, vol. 21, no. 1, pp. 142-166, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[6] Sajid Anwar et al., "Countering Malicious URLS in Internet of Things Using a Knowledge-Based Approach and a Simulated Expert," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4497-4504, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Tong Anh Tuan et al., "Performance Evaluation of Botnet DDoS Attack Detection Using Machine Learning," *Evolutionary Intelligence*, vol. 13, no. 2, pp. 283-294, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ammara Zamir et al., "Phishing Web Site Detection Using Diverse Machine Learning Algorithms," *Electronic Library*, vol. 38, no. 1, pp. 65-80, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Gunikhan Sonowal, and K.S. Kuppusamy, "Phidma - A Phishing Detection Model with Multi-Filter Approach," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 1, pp. 99-112, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Nureni Ayofe Azeez et al., "Identifying Phishing Attacks in Communication Networks Using URL Consistency Features," *International Journal of Electronic Security and Digital Forensics*, vol. 12, no. 2, pp. 200-213, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Edwin Donald Frauenstein, and Stephen Flowerday, "Susceptibility to Phishing on Social Network Sites: A Personality Information Processing Model," *Computers & Security*, vol. 94, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Ahmet Selman Bozkir, and Murat Aydos, "Logosense: A Companion HOG Based Logo Detection Scheme for Phishing Web Page and Email Brand Recognition," *Computers & Security*, vol. 95, 2020. [CrossRef] [Google Scholar] [Publisher Link]