IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023

DOI: 10.17148/IJARCCE.2023.12747

Phishing Websites Prediction based on Artificial Neural Network Technique

Tony Chhipne[1], Prof. Sushma Kushwaha[2]

M.Tech Scholar, Department of Computer Science and Engineering, Swami Vivekanand College of Science and Technology, Bhopal, India[1]

Assistant Professor, Department of Computer Science and Engineering, Swami Vivekanand College of Science and Technology, Bhopal, India[2]

Abstract- Phishing attacks have emerged as a significant threat to online security, targeting unsuspecting users to divulge sensitive information through fraudulent websites. To counter this threat, a proactive approach involving predictive techniques is crucial. This study presents a novel approach for predicting phishing websites using an Artificial Neural Network (ANN) technique. The proposed model leverages the inherent pattern recognition capabilities of ANNs to analyze a comprehensive set of features extracted from website URLs, content, and meta-information. A dataset comprising legitimate and phishing websites is used for training and evaluation. This paper presents phishing websites prediction based on artificial neural network technique.

Index Terms- ANN, AI, Phishing Websites, Deep Learning.

I. INTRODUCTION

In today's digitally connected world, the internet serves as a vital platform for communication, information sharing, and various online transactions. However, alongside its numerous advantages, the internet also presents an alarming challenge in the form of phishing attacks. Phishing attacks are malicious endeavors where cybercriminals deceitfully attempt to acquire sensitive user information, such as login credentials, credit card details, or personal identification, by impersonating trustworthy entities. These attacks often involve the creation of fraudulent websites that closely resemble legitimate ones, tricking users into disclosing confidential data.

The rapid evolution of phishing techniques, coupled with their potentially devastating consequences, underscores the pressing need for robust and proactive cybersecurity measures. Traditional rule-based and signature-based approaches to detecting phishing websites have shown limitations in their ability to adapt to the ever-changing tactics employed by cybercriminals. As a result, there is a growing emphasis on leveraging advanced technological solutions to predict and prevent phishing attacks before they can compromise users' sensitive information.

This research focuses on harnessing the capabilities of Artificial Neural Networks (ANNs) to predict phishing websites. ANNs are a class of machine learning algorithms inspired by the complex interconnected structure of biological neural networks. ANNs have demonstrated remarkable success in pattern recognition tasks and are well-suited for analyzing intricate and non-linear relationships within data.

The primary objective of this study is to develop an effective and accurate prediction model for identifying phishing websites using ANN-based techniques. By leveraging a diverse set of features extracted from website URLs, content, and meta-information, the proposed model aims to learn and generalize the underlying patterns that differentiate legitimate websites from phishing ones. Through comprehensive experimentation and evaluation, we intend to showcase the potential of ANN-based prediction models in enhancing cybersecurity efforts against phishing attacks.

This paper is organized as follows: Section 2 provides an overview of related work in the field of phishing detection and prediction. Section 3 outlines the methodology, detailing the dataset, feature extraction process, and the architecture of the ANN model. In Section 4, present the experimental setup and analyze the results obtained. Finally, Section 5 concludes the study, discussing the implications of the findings and highlighting the significance of ANN-based phishing prediction in the broader context of online security.

DOI: 10.17148/IJARCCE.2023.12747

II. PROPOSED METHODOLOGY

The proposed methodology is explained using following flow chart-

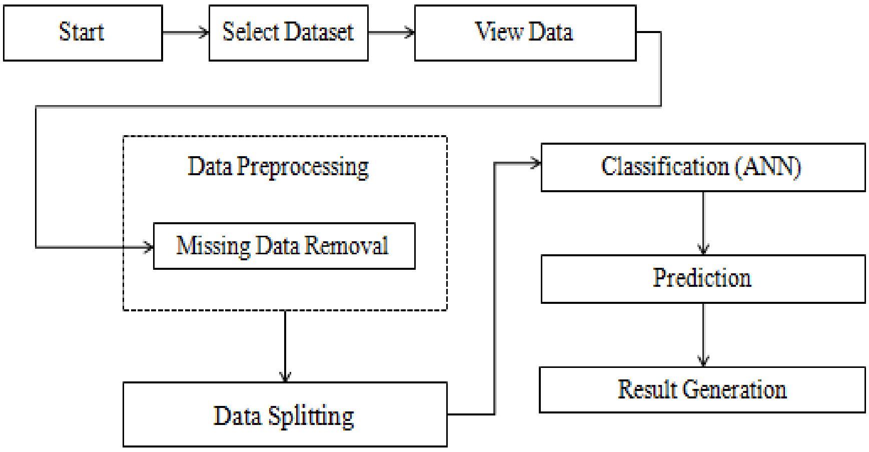


Figure 1: Flow Chart

This section outlines the methodology employed in developing the phishing website prediction model based on Artificial Neural Network (ANN) techniques. The methodology encompasses data collection and preprocessing, feature extraction, model architecture design, training and validation, and performance evaluation.

- **Data Collection and Preprocessing**: A diverse and representative dataset is essential for training and evaluating the prediction model. This dataset comprises both legitimate and phishing websites. Legitimate websites are sourced from well-established domains, while phishing websites are obtained from reputable threat intelligence sources. The collected URLs are subjected to preprocessing, which involves removing duplicate entries, resolving redirects, and ensuring uniform formatting.

- **Feature Extraction**: Effective feature extraction is critical for capturing relevant characteristics that distinguish between legitimate and phishing websites. Features are extracted from various aspects of the URLs, website content, and meta-information. Examples of features include URL length, domain age, presence of HTTPS, HTML content analysis, and keyword frequency. These features provide the model with comprehensive information to discern patterns indicative of phishing behavior.

- **Model Architecture Design**: The neural network architecture is designed to accommodate the complexity of the data and task. A feedforward neural network architecture, consisting of input, hidden, and output layers, is chosen. The number of neurons in the hidden layers and the choice of activation functions are determined through experimentation. Dropout layers may be incorporated to prevent overfitting.

- **Training and Validation**: The dataset is divided into training, validation, and testing subsets. The training set is used to optimize the model's parameters through backpropagation and gradient descent. The validation set aids in tuning hyperparameters and preventing overfitting. The model's performance on the validation set guides the training process, ensuring convergence to an optimal configuration.

- **Model Training**: The chosen ANN model is trained using the training dataset. During training, the model learns to identify patterns associated with phishing websites by minimizing a suitable loss function. Regularization techniques such as L1/L2 regularization may be applied to prevent overfitting. The training process continues until convergence is achieved.

- **Performance Evaluation**: The trained ANN model's performance is evaluated using the testing dataset, which it has not encountered during training. Standard metrics such as accuracy, precision, recall, F1-score, and area under the Receiver Operating Characteristic (ROC-AUC) curve are calculated to assess the model's predictive capabilities. Comparative analysis with existing phishing detection methods may be conducted to highlight the model's effectiveness.

DOI: 10.17148/IJARCCE.2023.12747

- The entire methodology is implemented using suitable programming languages and frameworks for neural network development, such as TensorFlow or PyTorch. Rigorous experimentation with different network architectures, hyperparameters, and feature combinations contributes to refining the prediction model's accuracy and generalization to unseen phishing instances.

Algorithm

Input: Phishing Websites Dataset.

Take the initial data features like id having IP Address URL Length Shortening Service having Symbol double slash redirecting, Prefix Suffix having Sub Domain, SSL etc.

Filtering the null value

Classify the dataset based on the selected features

Output: Optimal Precision, Recall, F-Measure, Accuracy and Error rate

```
Step:  1. Split train and test dataset Y_train, Y_test, X_train and X_test
       2. Feature extractions, features = {} for phishing count: features [phishing count] = True
       3. Model selection and split
              Y train counts
              Y test count
4. Apply the artificial neural network classifier.
5. Generate confusion matrix and show value of TP, FP, TN and FN
6. Calculate Accuracy, error rate, precision, recall and f-measure
7.     Plot the ROC Curve
```

Evaluation

The confusion metrics used to evaluate a classification model are accuracy, precision, and recall.

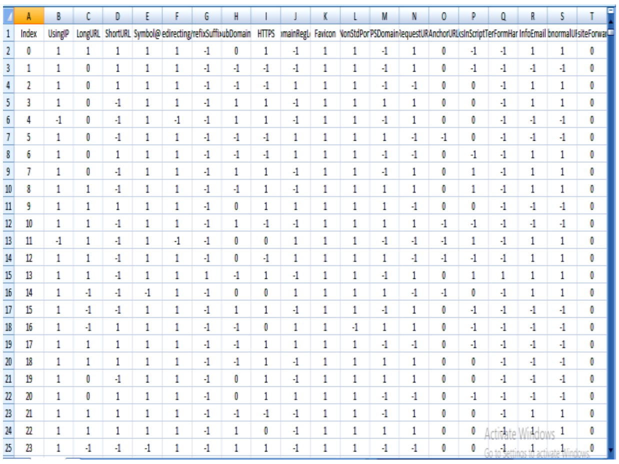
- Precision = True Positive/(True Positive + False Positive)
- Recall = True Positive/(True Positive + False Negative)
- F1-Score = 2x (Precision x Recall)/(Precision + Recall)
- Accuracy = [TP +TN] / [TP+TN+FP+FN]
- Classification Error = 100- Accuracy

Result Generation

The final result will get generated based on the overall classification and prediction. The performance of this proposed approach is evaluated using some measures like accuracy, error rate etc.

III. SIMULATION AND RESULTS

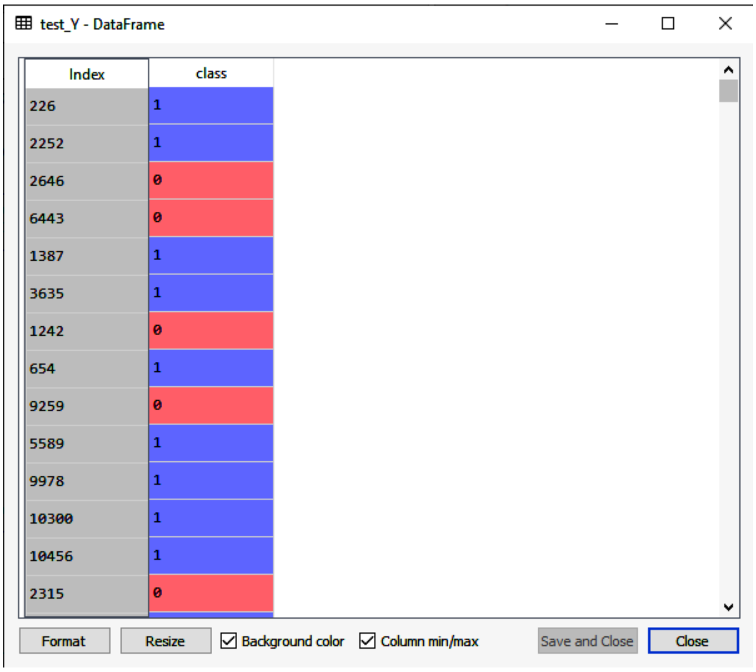
The simulation is performed using the Python Spyder IDE 3.7 software.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Index	UsingIP	LongURL	ShortURL	Symbol@	edirecting/	refixSuffi	ubDomain	HTTPS	mainRegL	Favicon	NonStdPor	PSDomain	equestUR	AnchorURL	ksInScript	TerFormHar	InfoEmail	bnormalU	siteForwar
2	0	1	1	1	1	1	-1	0	1	-1	1	1	-1	1	0	-1	-1	1	1	0
3	1	1	0	1	1	1	-1	-1	-1	-1	1	1	-1	1	0	-1	-1	-1	-1	0
4	2	1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	0	-1	1	1	0
5	3	1	0	-1	1	1	-1	1	1	-1	1	1	1	1	0	0	-1	1	1	0
6	4	-1	0	-1	1	-1	-1	1	1	-1	1	1	-1	1	0	0	-1	-1	-1	0
7	5	1	0	-1	1	1	-1	-1	-1	1	1	1	1	-1	-1	0	-1	-1	-1	0
8	6	1	0	1	1	1	-1	-1	-1	1	1	1	-1	-1	0	-1	-1	1	1	0
9	7	1	0	-1	1	1	-1	1	1	-1	1	1	-1	1	0	1	-1	1	1	0
10	8	1	1	-1	1	1	-1	-1	1	-1	1	1	1	1	0	1	-1	1	1	0
11	9	1	1	1	1	1	-1	0	1	1	1	1	1	-1	0	0	-1	-1	-1	0
12	10	1	1	-1	1	1	-1	1	-1	-1	1	1	1	1	-1	-1	-1	-1	-1	0
13	11	-1	1	-1	1	-1	-1	0	0	1	1	1	-1	-1	-1	1	-1	1	1	0
14	12	1	1	-1	1	1	-1	0	-1	1	1	1	1	-1	-1	-1	-1	1	1	0
15	13	1	1	-1	1	1	1	-1	1	-1	1	1	-1	1	0	1	1	1	1	0
16	14	1	-1	-1	-1	1	-1	0	0	1	1	1	1	-1	-1	0	-1	1	1	0
17	15	1	-1	-1	1	1	-1	1	1	-1	1	1	-1	1	0	-1	-1	-1	-1	0
18	16	1	-1	1	1	1	-1	-1	0	1	1	-1	1	1	0	-1	-1	-1	-1	0
19	17	1	1	1	1	1	-1	-1	1	1	1	1	-1	-1	0	-1	-1	-1	-1	0
20	18	1	1	1	1	1	-1	-1	1	-1	1	1	1	1	0	0	-1	-1	-1	0
21	19	1	0	-1	1	1	-1	0	1	-1	1	1	1	1	0	0	-1	-1	-1	0
22	20	1	0	1	1	1	-1	0	1	1	1	1	-1	-1	0	-1	-1	-1	-1	0
23	21	1	1	1	1	1	-1	-1	-1	-1	1	1	-1	1	0	0	-1	1	1	0
24	22	1	1	1	1	1	-1	1	0	-1	1	1	1	1	0	0	-1	1	1	0
25	23	1	-1	-1	-1	1	-1	1	1	-1	1	1	-1	-1	0	0	-1	1	1	0

Figure 3: Dataset

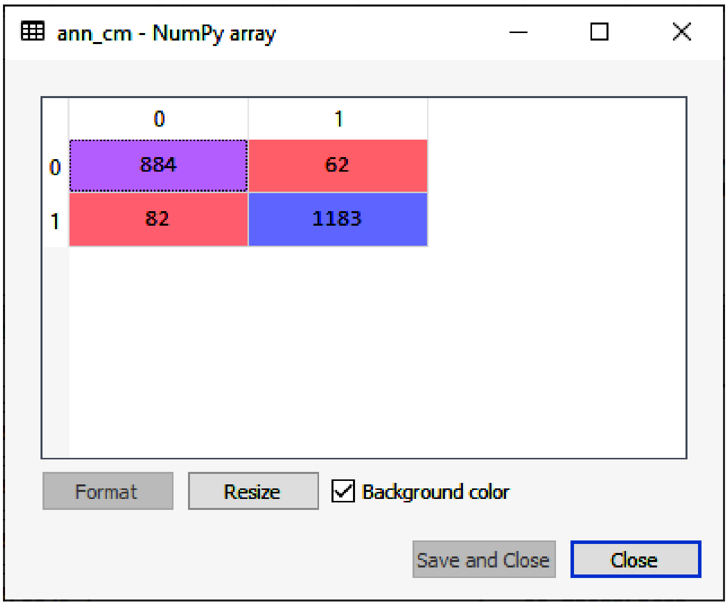
Figure 3 is showing the dataset in the python environment. The dataset have various numbers of rows and column. The features name is mention in each column.



Index	class
226	1
2252	1
2646	0
6443	0
1387	1
3635	1
1242	0
654	1
9259	0
5589	1
9978	1
10300	1
10456	1
2315	0

Figure 4: Y test

Figure 4 is showing the y test of the given dataset. The given dataset is divided into the 20-30% part into the train dataset.



	0	1
0	884	62
1	82	1183

Figure 5: Confusion matrix heat map

Figure 5 is showing the heat map confusion matrix of the ANN classification technique. It is an N x N matrix used for evaluating the performance of a classification model.

DOI: 10.17148/IJARCCE.2023.12747

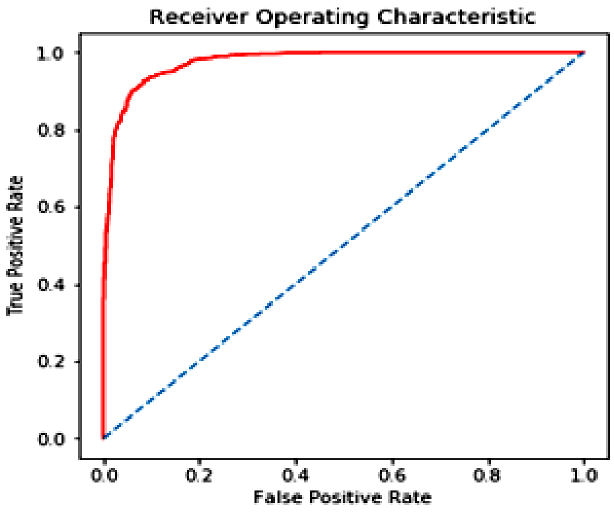


Figure 6: ROC

Figure 6 is presenting the receiver operating characteristic curve. The ROC curve shows the trade-off between sensitivity (or TPR) and specificity (1 – FPR). Classifiers that give curves closer to the top-left corner indicate a better performance.

Table 1: Result Comparison

Sr. No.	Techniques	Accuracy (%)
1	Decision Tree	91.51%
2	K-Nearest Neighbor	97.69%
3	Random Forest	94.44%
4	SVM	98.23%
5	ANN (Proposed)	98.54%

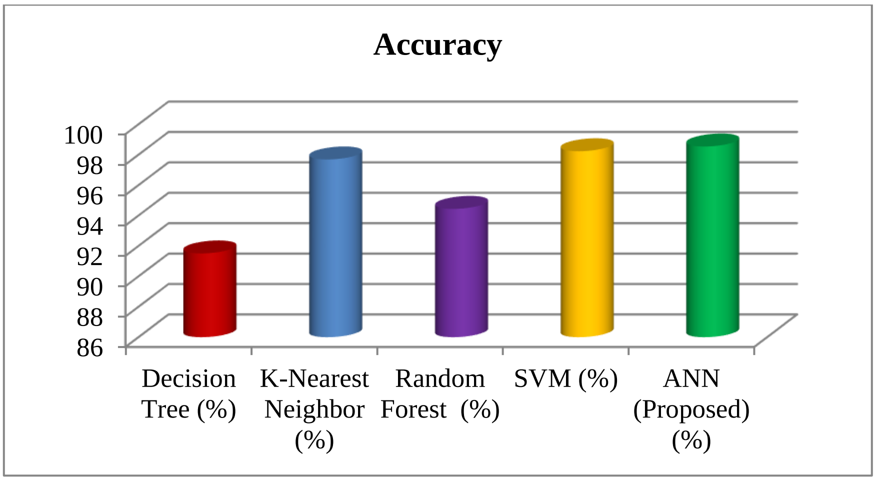


Figure 6: Accuracy Result graph

Figure 6 is presenting the graphical representation of the accuracy. The proposed work achieved better accuracy then existing work.

DOI: 10.17148/IJARCCE.2023.12747

IV. CONCLUSION

ANN-based phishing website prediction model presents a formidable tool in the ongoing battle against phishing attacks. By capitalizing on the strengths of machine learning and neural networks, we contribute to the advancement of cybersecurity and the protection of users' online experiences. As the digital landscape continues to evolve, our approach serves as a testament to the potential of AI-driven solutions in safeguarding the integrity of online interactions. The ANN achieved 98.54% accuracy while existing SVM achieve 98.23% accuracy.

REFERENCES

[1]. S. Jain and C. Gupta, "A Support Vector Machine Learning Technique for Detection of Phishing Websites," 2023 6th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-6, doi: 10.1109/ISCON57294.2023.10111968.

[2]. F. Yahya et al., "Detection of Phising Websites using Machine Learning Approaches," 2021 International Conference on Data Science and Its Applications (ICoDSA), 2022, pp. 40-47, doi: 10.1109/ICoDSA53588.2021.9617482.

[3]. S. M. Istiaque, M. T. Tahmid, A. I. Khan, Z. A. Hassan and S. Waheed, "Artificial Intelligence Based Cybersecurity: Two-Step Suitability Test," 2021 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2021, pp. 1-6, doi: 10.1109/SOLI54607.2021.9672437.

[4]. R. Yaqoob, Sanaa, M. Haris, Samadyar and M. A. Shah, "The Price Scraping Bot Threat on E-commerce Store Using Custom XPATH Technique," 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 1-6, doi: 10.23919/ICAC50006.2021.9594223.

[5]. M. Min, J. J. Lee, H. Park and K. Lee, "Honeypot System for Automatic Reporting of Illegal Online Gambling Sites Utilizing SMS Spam," 2021 World Automation Congress (WAC), 2021, pp. 180-185, doi: 10.23919/WAC50355.2021.9559478.

[6]. H. Dao, J. Mazel and K. Fukuda, "CNAME Cloaking-Based Tracking on the Web: Characterization, Detection, and Protection," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3873-3888, Sept. 2021, doi: 10.1109/TNSM.2021.3072874.

[7]. R. Nanjundappa et al., "AWAF: AI Enabled Web Contents Authoring Framework," 2020 IEEE 17th India Council International Conference (INDICON), 2020, pp. 1-5, doi: 10.1109/INDICON49873.2020.9342385.

[8]. K. E. Aydın and S. Baday, "Machine Learning for Web Content Classification," 2020 Innovations in Intelligent Systems and Applications Conference (ASYU), 2020, pp. 1-7, doi: 10.1109/ASYU50717.2020.9259833.

[9]. U. Iqbal, P. Snyder, S. Zhu, B. Livshits, Z. Qian and Z. Shafiq, "AdGraph: A Graph-Based Approach to Ad and Tracker Blocking," 2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 763-776, doi: 10.1109/SP40000.2020.00005.

[10]. N. Megha, K. R. Remesh Babu and E. Sherly, "An Intelligent System for Phishing Attack Detection and Prevention," 2019 International Conference on Communication and Electronics Systems (ICCES), 2019, pp. 1577-1582, doi: 10.1109/ICCES45898.2019.9002204.

[11]. S. S. Hashmi, M. Ikram and M. A. Kaafar, "A Longitudinal Analysis of Online Ad-Blocking Blacklists," 2019 IEEE 44th LCN Symposium on Emerging Topics in Networking (LCN Symposium), 2019, pp. 158-165, doi: 10.1109/LCNSymposium47956.2019.9000671.

[12]. T. Vo and C. Jaiswal, "ADREMOVER: THE IMPROVED MACHINE LEARNING APPROACH FOR BLOCKING ADS," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019, pp. 1-4, doi: 10.1109/UEMCON47517.2019.8993052.

[13]. https://www.kaggle.com/datasets/isatish/phishing-dataset-uci-ml-csv?select=uci-ml-phishing-dataset.csv.