IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

A Filter-Based Feature Selection for Robust Phishing Attack Detection using XGBoost

Isaac Dawandakpoye Ohwosoro
Post Graduate Student, Department of Computer Science
Faculty of Science, Delta State University, Abraka, Nigeria
ohwozik@gmail.com

Abstract: *Phishing attacks are a pervasive cyber threat that has grown in sophistication and scale, presenting significant challenges to cybersecurity professionals. To effectively combat phishing, robust detection mechanisms are crucial, and machine learning has emerged as a powerful tool for this purpose. This study addresses the challenge of creating a fast and reliable framework to counter phishing attacks. We introduce a novel approach that integrates filter-based feature selection methods with the XGBoost algorithm. XGBoost is chosen for its high computational efficiency, outperforming other gradient boosting techniques by a factor of ten, while mutual information gain is used for rapid initial feature selection. Our proposed framework achieves outstanding performance, with an accuracy of 97.0%, precision of 96.3%, recall of 96.5%, F1-score of 96.6%, and ROC AUC score of 99.6%. These results demonstrate the framework's capability to effectively detect and mitigate phishing attacks, providing a timely and powerful tool for enhancing cybersecurity defenses.*

Keywords: XGBoost, Machine learning, filter method Phishing attacks and mutual information gain.

I. INTRODUCTION

Phishing attacks, a prevalent form of cybercrime, exploit deception to manipulate individuals or organizations into divulging sensitive information. During the first quarter of 2024, social media was the most targeted sector, with around 37.6% percent of phishing attacks worldwide directed towards these platforms. Following closely behind were web-based software services and webmail, comprising approximately 21% percent of attacks, with financial institutions facing a notable risk of 9.8%. These deceptive tactics, such as crafting authentic-looking emails or messages to trick victims into divulging valuable data like credit card details or login credentials, have severe consequences such as financial losses, identity theft, and compromised data security. With millions of deceptive emails sent daily across the globe, phishing attacks remain a significant threat, consistently identified as a leading cause of data breaches according to industry reports, underscoring the pervasive danger they pose in the cybersecurity landscape.

Traditional phishing detection methods, such as blacklists and heuristic rules, have long been used to identify and combat phishing attempts. Blacklists involve maintaining databases of known malicious URLs or email addresses, while heuristic rules analyze various attributes of emails or websites to detect suspicious patterns. However, these methods face challenges in keeping pace with evolving phishing tactics. Attackers constantly adapt, making it difficult for blacklists to cover all new malicious URLs or for heuristic rules to accurately distinguish between legitimate and malicious content. Additionally, these methods can generate false positives and struggle to detect zero-day attacks or encrypted phishing attempts. To address these limitations, organizations must augment traditional methods with advanced technologies like machine learning and behavioral analysis to enhance detection accuracy and combat sophisticated phishing threats effectively.

Machine learning can be a powerful tool in detecting phishing websites. By training machine learning algorithms on a large dataset of both legitimate and fraudulent websites, the algorithms can learn to distinguish between both. This can lead to the development of effective phishing detection systems that can automatically identify and warn users about potentially dangerous websites. There are several types of machine learning algorithms that can be used for phishing detection, including supervised learning and deep learning. Supervised learning trains models on labeled data, such as decision trees, support vector machines (SVM), and neural networks, classify emails or websites based on extracted

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

features. Unsupervised learning identifies anomalies in unlabeled data, utilizing clustering algorithms or anomaly detection techniques. Deep learning employs neural networks with multiple layers, such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs), to analyze complex patterns in email content or website structure. By leveraging machine learning, organizations bolster their cybersecurity defenses, swiftly identifying and mitigating phishing threats with improved precision and efficiency as compared to traditional methods.

In this study, it presented the utilization of machine learning, notably XGBoost with mutual information gain, which showed considerable promise in the realm of phishing detection. Its benefits, including improved accuracy, efficiency, and adaptability, highlighted its capacity to effectively counter evolving cyber threats. Despite hurdles related to data quality, computational resources, and the ever-changing landscape of phishing techniques, recent advancements in machine learning algorithms and automation techniques offered promising avenues for bolstering cybersecurity measures. Our study aimed to delve deeper into the effectiveness of such approaches, providing valuable contributions to the ongoing discussions surrounding cyber defense strategies

This article presents a novel approach to email anomaly detection. Unlike previous methods that analyze email body and subject content, this research focuses solely on email header information. Their findings demonstrate that analyzing email headers is sufficient to reliably detect spam and phishing emails with high accuracy (97% for phishing, 99% for spam) using supervised learning algorithms like Random Forest and Support Vector Machines (SVM). Additionally, they show promising results (87% and 89% accuracy) using a one-class classification approach. This approach offers advantages in terms of resource utilization and efficiency for real-world email filtering applications and a novel approach for detecting web phishing pages based on anomalies in web structure and HTTP transactions. This method is independent of specific phishing implementations and offers low miss and false-positive rates, making it a promising tool for combating phishing attacks. It proposes a PHISH-SAFE, a system to combat phishing attacks. PHISH-SAFE utilizes machine learning to analyze website URLs and identify potential phishing attempts. Importantly, PHISH-SAFE achieved an accuracy of over 90% in detecting phishing websites using a Support Vector Machine (SVM) classifier.The proposed system combats phishing by combining Naive Bayes and Random Forest algorithms. This hybrid approach improves the accuracy of detecting fraudulent attempts to obtain sensitive information through deceptive websites. They emphasize the importance of robust system administration and firewall settings in preventing such attacks.Based on research conducted by, the results underscore the essential role of machine learning in addressing phishing threats. The study emphasizes the increasing danger posed by phishing to internet users, governmental bodies, and commercial entities. Through the creation of a detection model and examination of various datasets, the study yields promising outcomes. Particularly notable is the boosted decision tree algorithm, which exhibits high accuracy levels across a range of datasets, with values reaching 88%, 100%, and 97%. By combining CNN and LSTM algorithms, the Intelligent Phishing Detection System (IPDS) achieved an accuracy rate of 93.28% with an average detection time of 25 seconds. This hybrid approach enhances classifier prediction performance and reduces training time, making it a novel contribution to phishing detection.[14] Highlights the severity of phishing attacks and proposes a hybrid detection model using deep learning techniques. This model, employing the CNN-Attention-LSTM architecture, achieves 97% accuracy by combining local URL feature identification with semantic dependency learning. An attention mechanism enhances performance by focusing on key features.

Phishing attacks are a critical cybersecurity threat, prompting this propose novel detection method. The approach combines BERT feature extraction and deep learning to identify phishing URLs. Achieving 96.66% accuracy on a dataset of over 549,000 entries, the proposed model proves efficient and valid comparison to other existing literature.It introduces a novel phishing detection method using CNN and RF. This approach accurately predicts URL legitimacy without accessing web content or relying on third-party services. By converting URLs into fixed-size matrices, extracting features with CNN, and classifying with RF, the method achieves exceptional accuracy rates of 99.35% on the dataset and 99.26% on benchmark data, surpassing existing models.[17] presents a novel phishing detection method using VisionGNN, a Graph Neural Network approach, to analyze website images. Using the VisualPhish dataset, the model achieves 97% accuracy, demonstrating its effectiveness in identifying phishing sites. This study highlights the potential of GNN-based methods in enhancing cybersecurity and paves the way for future research.[18] proposes an advanced method for detecting malicious web links using a nature-inspired ensemble model. Tested on two datasets, the model achieved 97.05% accuracy on the first and 91.12% on the second. The ensemble, using a weighted voting

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

mechanism optimized by Particle Swarm Optimization, combines 12 machine learning models, including Logistic Regression, SVM, Random Forest, and others. A two-stage ensemble learning model for detecting malicious URLs using cyber threat intelligence features from web searches and analyst reports was adopted by [19] . The model combines random forest (RF) for preclassification and multilayer perceptron (MLP) for final decision making. This approach improves detection accuracy by 7.8% and reduces false positives by 6.7% compared to traditional URL-based models. Similarly, [20] employs machine learning techniques to detect malicious URLs, capitalizing on trends in technology and security. The study discusses the increasing online threat landscape and the significant growth in mobile device usage, which amplifies vulnerabilities. By utilizing Support Vector Machine with a polynomial kernel and logistic regression, achieves a high accuracy rate of 98% in identifying malicious URLs.

II. METHODOLOGY

In this study, it presented the utilization of machine learning, notably XGBoost with mutual information, which showed considerable promise in the realm of phishing detection. The methodology adopted a hybrid model that combined both XGBoost and mutual information score feature selection, to enhance the system's performance and accuracy. Specifically, the hybrid model consisted of mutual information score feature selection and a boosting algorithm which is XGBoost: to start, the analysis of the existing systems was utilized as a foundational component of the hybrid model.

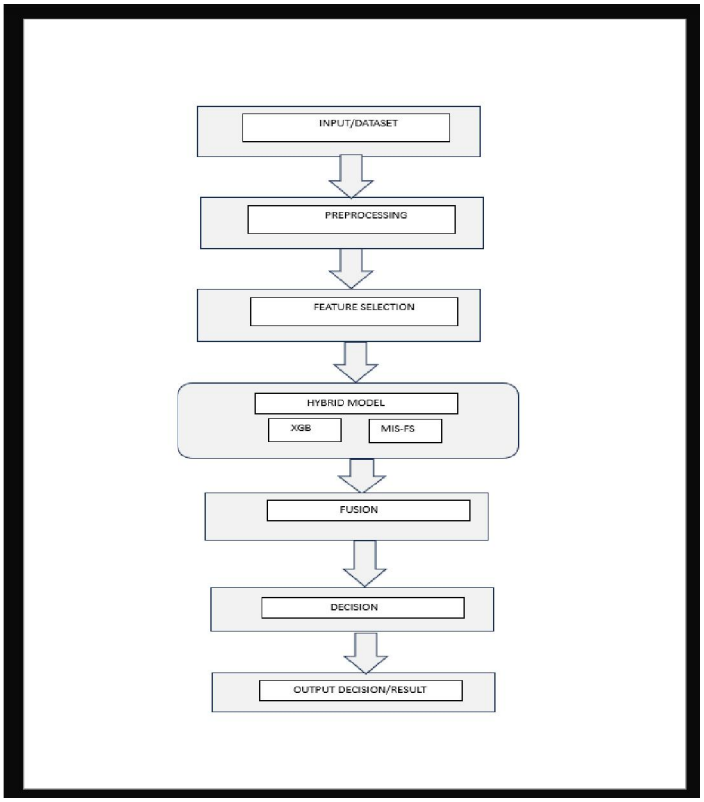

Fig 2: High Level Model of the Proposed System architecture.

2.1 Data Collection

The dataset for this study was obtained from Kaggle and contains an equal distribution of instances. The dataset contains a total of 11,430 records, with5,715 legitimate instances and 5,715 phishing instances, and includes 89 features.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

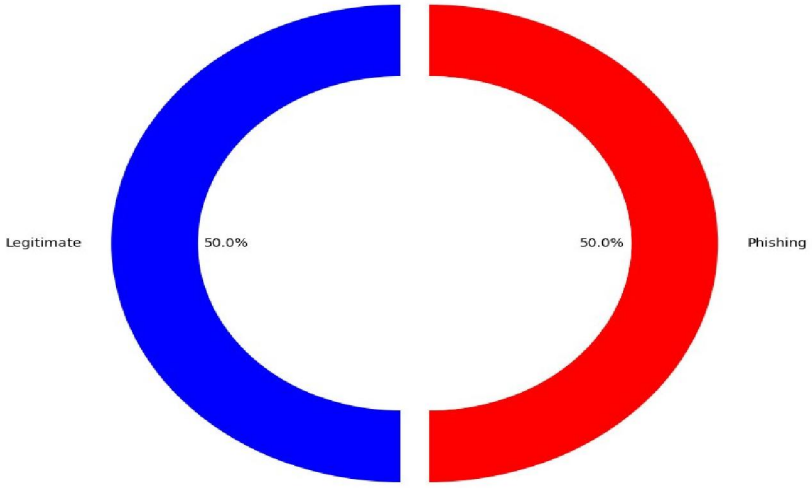

Fig 3: Doughnut Plot of Data Instances

Table 1: Attributes of Variables

	url	length_url	length_hostname	ip	nb_dots	nb_hyphens	nb_at	nb_qm	nb_and	nb_or	...	domain_in_title	domain_with_copyright	whois_registered
	onwood.com/router.php	37	19	0	3	0	0	0	0	0	...	0	1	
	y.com/V4/validation/a...	77	23	1	1	0	0	0	0	0	...	1	0	
	m.secureupdate.duila...	126	50	1	4	1	0	1	2	0	...	1	0	
	http://rgipt.ac.in	18	11	0	2	0	0	0	0	0	...	1	0	
	ig.com/tracks/gateway-motorspo...	55	15	0	2	2	0	0	0	0	...	0	1	
	leid.apple.com-app.es/	32	24	0	3	1	0	0	0	0	...	1	1	
	http://www.mutuo.it	19	12	0	2	0	0	0	0	0	...	0	1	
	ology.com/V4/validati...	81	27	1	2	0	0	0	0	0	...	1	0	
	nedicina.blogspot.com/	42	34	0	2	0	0	0	0	0	...	1	1	
	/425836/joshwigler/the-amazi...	104	10	0	1	10	0	0	0	0	...	1	0	

2.2 Preprocessing

The target variable was encoded into binary, where legitimate instances are mapped to 0 and phishing instances are mapped to 1. This step ensures that the model can easily differentiate between the two classes during training.

2.3 Feature selection.

There are different feature selection methods which include: mutual information, URL-based, black list-based method, Chi-square test methods, e.t.c. In this study, mutual information was used to select the most relevant features for the machine learning task. In phishing detection, it can be used to identify features that are most informative in distinguishing between legitimate and phishing websites. This metric measures the dependency between each feature and the target variable, identifying features with the highest predictive power. The figure below shows the mutual information scores for each feature, with higher bars indicating more informative features. By focusing on these top-scoring features, the study enhances model performance and reduces dimensionality.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

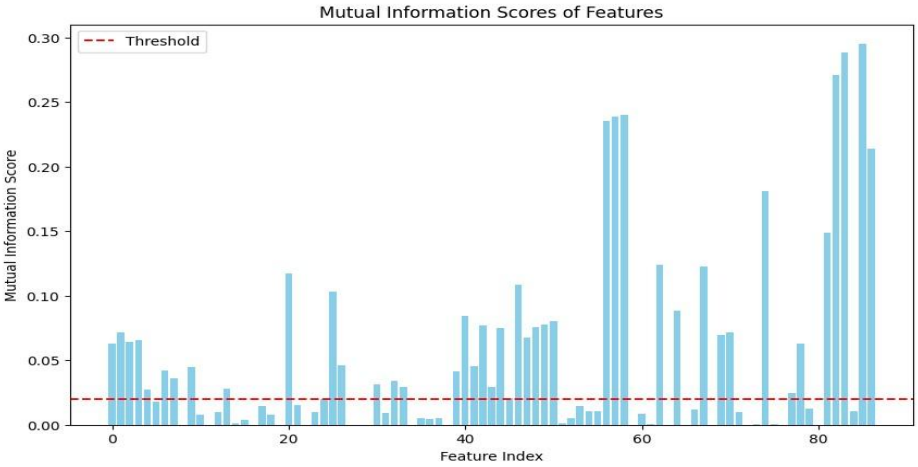

Fig 4: Mutual information score of features

2.4 XGBoost

XGBoost is a high-performance algorithm, excels at handling complex datasets and has proven its ability to classify phishing attacks with high accuracy. It is a machine learning algorithm that falls under the ensemble learning category, specifically within the gradient boosting framework. It uses decision trees as its base learners and incorporates regularization techniques to improve model generalization.

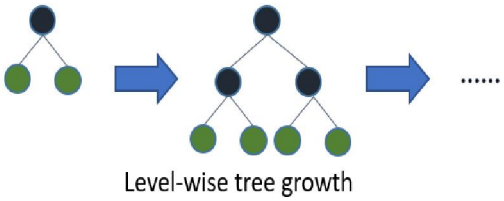

Fig 5: Shows Xgboost algorithm block diagram

Algorithm 1:

1. Initialize model with a constant value:

$$\hat{f}^{(0)}(x) = \arg\min_{\theta} \sum_{i=1}^{N} L(y_i, \theta).$$

2. For $m = 1$ to M

   1. Compute the 'gradients' and 'hessians'

$$\hat{g}^{m}(x_i) = \left[\frac{\partial L(y_i, f(x_i))}{\partial f(x_i)}\right]_{f(x)=\hat{f}^{(m-1)}(x)},$$

$$\hat{h}^{m}(x_i) = \left[\frac{\partial^2 L(y_i, f(x_i))}{\partial f(x_i)^2}\right]_{f(x)=\hat{f}^{(m-1)}(x)}.$$

   2. Fit the base learner using the training (70%) set by solving the optimization below:

$$\hat{\phi}^{m} = \arg\min_{\phi\in\Phi} \sum_{i=1}^{N} \frac{1}{2}\hat{h}^{m}(x_i)\left[\phi(x_i) - \frac{\hat{g}^{m}(x_i)}{\hat{h}^{m}(x_i)}\right]^2.$$

$$\hat{f}^{m}(x) = \alpha\hat{\phi}^{m}(x).$$

   3. Update model

$$\hat{f}^{(m)}(x) = \hat{f}^{(m-1)}(x) + \hat{f}^{m}(x).$$

3. Output the result:

$$\hat{f}(x) = \hat{f}^{(M)}(x) = \sum_{m=0}^{M} \hat{f}^{m}(x).$$

Fig 6: XGBoost Algorithm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Development Process

Designing a project for phishing detection involves the use of technologies like computer vision, machine learning, deep learning with sensor data to identify and respond to any suspected phishing attack. Here is an overview of how the proposed system's objective: which was to develop a system that can detect suspected phishing attacks and alert the authorities or information security personnel for action was implemented:

- **Data Collection**: A dataset of an equal distribution of instances were collected. This dataset should contain examples of both legitimate and phishing instances.
- **Data Pre-processing**: Pre-process the data by extracting relevant features for analysis.
- **Phishing Detection Model:** Train a machine learning model using techniques like object detection, action recognition, to identify suspected phishing attacks.
- **Real-time Detection**: Implement the model to perform real-time suspected phishing attacks.
- **Alert System**: An alert system was developed to triggers notifications to the information security personnel or authorities when suspected phishing attack is detected.
- **Integration with Security Systems**: The phishing detection system will be iintegrated with existing security systems to automate responses like denial of access login, sounding alarms, e.t.c.
- **Testing and Evaluation**: Test the system with different scenarios and evaluate its performance in terms of detection accuracy, false positives and false negatives.
- **Deployment and Monitoring:** The proposed model deployed will be continuously updated with new data to improve its accuracy and its performance
- **Technologies to Consider:** Computer Vision: OpenCV, TensorFlow, PyTorch; Machine Learning/Deep Learning models and Alert System such as: Email, SMS alert and an alarm notification.

2.5 Programming Language Used.

Python was used for the creation of this model because to its adaptability and superior usefulness when handling mathematical, statistical, and scientific processes. The Jupyter Notebook IDE was used to write our Python source code. The Jupiter notebook can be accessed using a web browser and which canbe hosted on a remote server or personal owned computer system

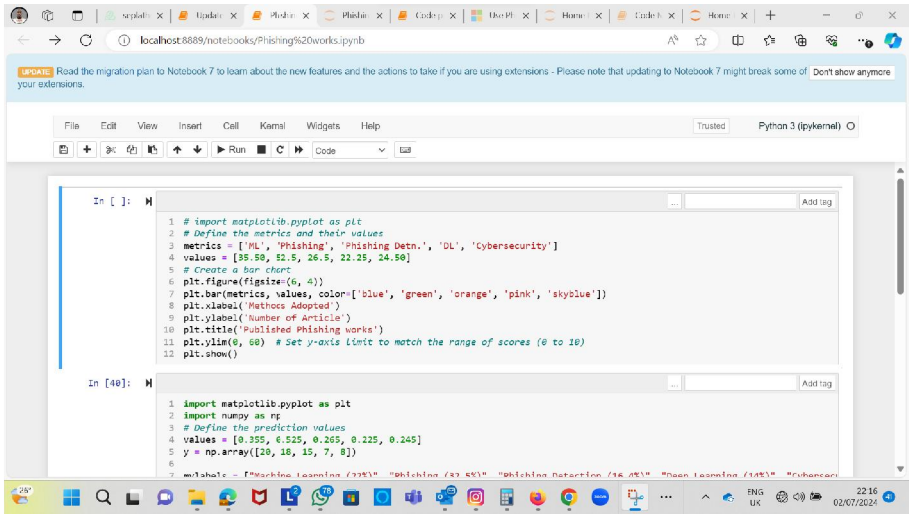

Fig 7: An overview of programming environment

2.6 Model Performance Evaluation/Metrics

The following evaluation metrics were employed in assessing the model performance, this include: accuracy, precision, recall, and ROC score (Receiver Operating Characteristic score). These metrics provide a comprehensive view of how well the models are performing and how they handle different aspects of classification.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

1. **Accuracy:** This measures the proportion of correctly predicted instances out of the total instances. It gives an overall assessment of how well the model predicts both positive and negative cases.

$$Accuracy = \frac{TPR + TNR}{TPR + TNR + FPR + FNR}$$

2. **Precision**: Precision is the ratio of true positive predictions to the total predicted positive instances. It assesses the accuracy of positive predictions, indicating how well the model avoids false positives.

$$Precision = \frac{TP}{TP + FP}$$

3. **Recall (Sensitivity or True Positive Rate):**This is the ratio of true positive predictions to the total actual positive instances. It measures the model's ability to correctly identify positive cases and avoid false negatives.

$$Recall = \frac{TP}{TP + FN}$$

4. **ROC (Receiver Operating Characteristic) core, or ROC AUC (Area Under the Curve) Score:** It is a performance measurement for classification models at various threshold settings. It plots the true positive rate (sensitivity) against the false positive rate (1-specificity). The AUC represents the likelihood that the model will correctly distinguish between a positive and a negative instance. An AUC score of 1.0 indicates perfect classification, while an AUC score of 0.5 suggests no discriminative ability, akin to random guessing. In this study, an ROC AUC score of 99.6% signifies an exceptionally high capability of the model to correctly identify phishing attacks with minimal false positives and negatives.

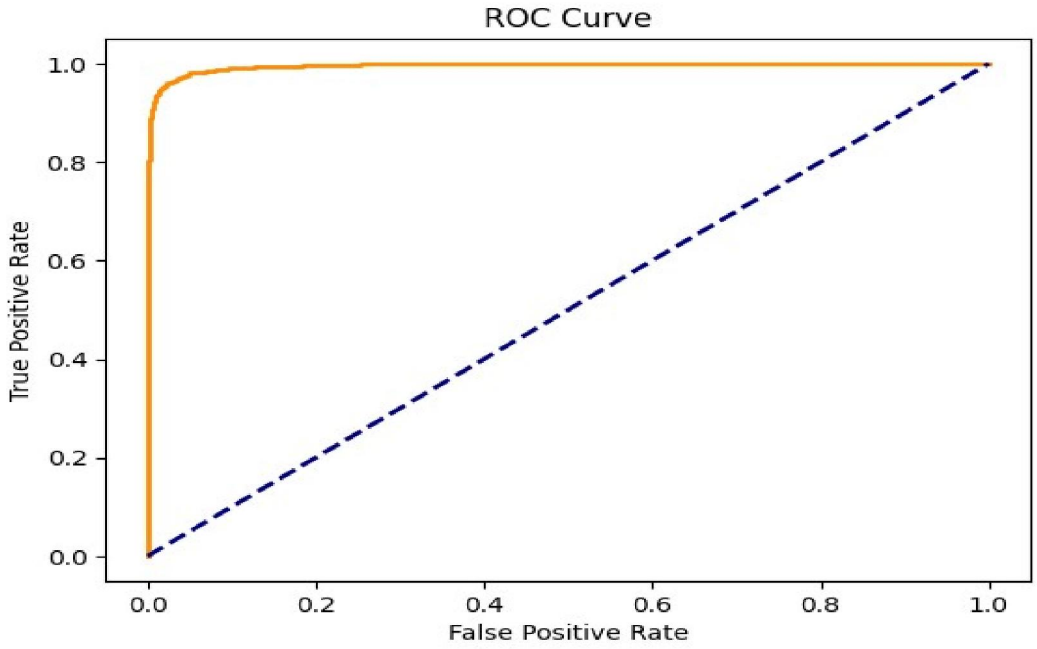

Fig 8: ROC curve for XGBoost

5**. The F1-Score:** is the harmonic mean of precision and recall. It provides a balanced assessment of the model's precision and recall, which is especially useful when classes are imbalanced.

$$F1 - Score(F) = \frac{2PR}{P + R}$$

6. Confusion Matrix Table: It is a table that presents the system's performance by summarizing the predictions against the actual labels. It consists of four elements: true positives (TP), true negatives (TN), false positives (FP), and false

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

negatives (FN). The confusion matrix provides an overall view of the system's performance and allows for the calculation of various metrics, including Precision, Recall, and F1-Score.

Table 2: Confusion Matrix table

Description	True Positive	True Negative
Predicted Positive	TP	FP
Predicted Negative	FN	TN

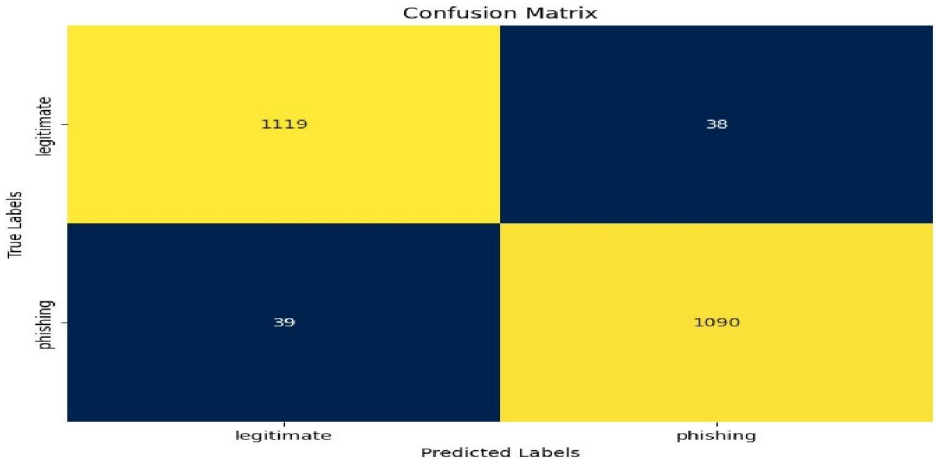

Fig 9: Confusion matrix for XGBoost.

In the figure above, the confusion matrix presents a comprehensive overview of our model's classification performance, detailing true positives, true negatives, false positives, and false negatives

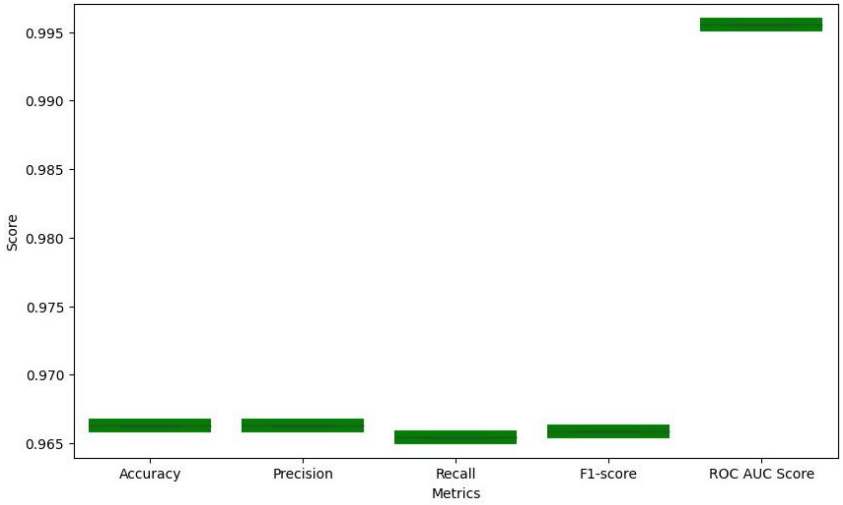

Fig 10: Box Plot of Model Performance Metrics

In the figure above, the model's accuracy across different metrics is demonstrated using box plots, providing a visual representation of its performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

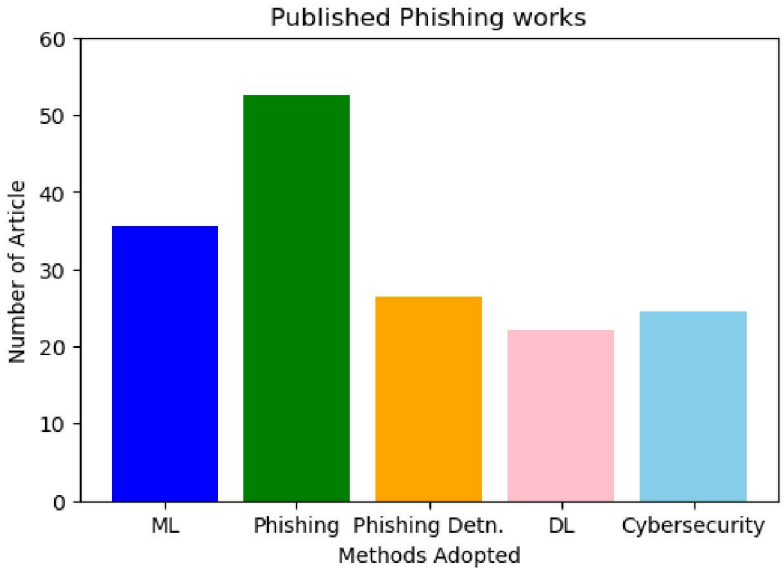

Fig 11: Numbers of articles published phishing works

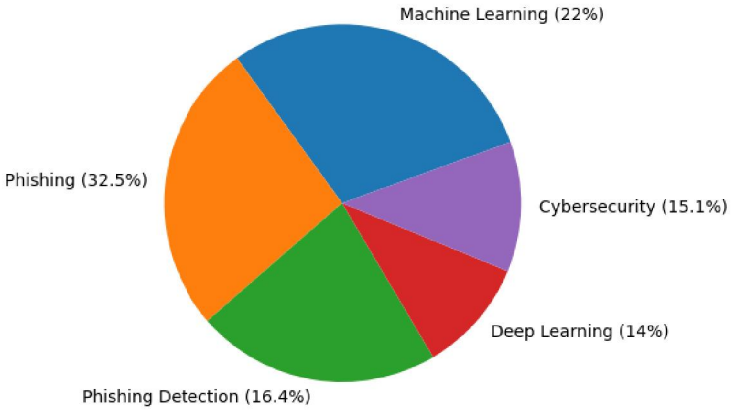

Fig 12: Percentage of articles using phishing works

III. LITERATURE REVIEW

Qabajeh et al. (Qabajeh et al., 2018) recently worked on conventional vs automated phishing detection techniques. The conventional anti-phishing methods include raising awareness, educating users, conducting periodic training or workshop, and using a legal perspective. The Computerized or automated anti-phishing approaches talks about list-based and Machine Learning Based techniques. More importantly, the paper compares these approaches' similarities, positive and negative elements from the user and performance perspectives. According to this study, Machine Learning and rule induction are suitable for combating phishing attacks. The limitations of this work are: the review is based on 67 research items, and the study does not include Deep Learning techniques for phishing website detection.

Zuraiq&Alkasassbeh (Zuraiq and Alkasassbeh, 2019) carried out a comprehensive review of current phishing detection methods. The study discusses anti-phishing techniques such as Heuristic, Content Based, and Fuzzy rule-based approaches. The study indicated that there are better methods for identifying phishing websites. The background of the work is based on research conducted between 2013 and 2018. The drawbacks of this work are that it analyzed only 18 studies and did not include Machine Learning, List Based and Deep Learning approaches for phishing website detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Kunju et al. (Kunju et al., 2019) used a survey method to detect phishing attacks. The research provides several phishing attack detection solutions and methodologies. According to the research, many of the proposed solutions were found to be insufficient in providing solutions to phishing attacks.

Kathrine et al. (Kathrine et al., 2019) presented a framework to detect and prevent different types of phishing attacks. According to this study, Machine Learning based algorithms effectively detect true positive results. The limitations of this study are: the literature in this work discussed only 11 studies, and the research does not include Deep Learning techniques for mitigating phishing websites.

Benavides et al. (Benavides et al., 2020) conducted a systematic review to analyze different approaches of other researchers for detecting phishing attacks by applying Deep Learning algorithms. In conclusion, there is still a significant gap in the area of Deep Learning algorithms for phishing attack detection.

Basit et al. (Basit et al., 2020) reported a survey on artificial intelligence-based phishing detection techniques. The authors used statistical phishing reports to examine the harm and trends of phishing attempts. In the paper, Antiphishing evaluations are classified into four categories: Machine Learning, Hybrid Learning, Scenario-based and Deep Learning. The research shows that Machine Learning procedures produce the best results compared to other approaches. The work is based on literature published in the last ten years and analyzed only 21 research items.

Arshad et al. (Arshad et al., 2021) presented different types of phishing and anti-phishing techniques in their study. The SLR evaluated that phone phishing, Email Spoofing, spear phishing, and Email Manipulation are the frequently used phishing techniques. According to this study, the highest Accuracy was achieved through Machine Learning approaches. The research is limited by the fact that it is based on only 20 studies.

Catal et al. (Catal et al., 2022) worked on a systematic literature review, which answered nine research questions. The study's main aim is to identify, assess, and synthesize the results of Deep Learning approaches for phishing detection. According to this study, Supervised ML algorithms were applied in 42 studies out of 43. The most used algorithm was DNN, and the best performance was given by DNN and Hybrid DL algorithms. The work only discusses Deep Learning related studies for phishing detection.

IV. RESULT AND DISCUSSION

In line of the evolving nature of phishing attacks, there is a critical need for a robust and efficient framework to counter them swiftly. The motivation for this study is to develop a framework that incorporates filter-based methods coupled with XGBoost. XGBoost is a boosting technique was chosen based on its remarkable speed, which is ten times faster than other gradient boosting techniques. Filter-based methods, such as mutual information gain, are also known for their speed, making them ideal for initial feature selection. While other techniques, such as wrapper methods, show promising results, they are computationally expensive. Therefore, by adopting a combination of filter methods (mutual information gain) and XGBoost, we can achieve both speed and high performance, providing a timely and effective solution in detecting and counteract phishing attacks.

Table 3: Existing results and their accuracies.

Authors/Year	**Method adopted**	**Used Algorithm**	**Data set used**	**Findings**	**Limitations/Challenges**	
Babagoli et al., 2019	Heuristic & Machine Learning	Support Vector Machine Harmony search	UCI Machine Learning Repository 11,055 web pages 30 features	The study claims that Harmony search has a greater accuracy rate of 94.13% for training and 92.80% for testing operations.	The approach was tested on a limited number of data sets, and the data set used in this work contained only 11,055 instances. The work experimented with only two algorithms.	76

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Liu and Fu, 2020	Visual Similarity & Heuristic	The unsupervised feature learning algorithm	PhishTank and OpenPhish (0.5 million malicious URLs), Alexa and DMOZ (1 million legitimate URLs)	The work achieved precision (over 95%).	Approach achieved precision (over 95%), recall (around 84%) As compared to other literary works, the performance achieved is less.	5
Jain et al., 2020	Visual Similarity	Term Frequency -inverse Document Frequency (TF-IDF)	PhishTank Open Phish Alexa 200 instances	The Accuracy value for this approach is 89.0%.	The study has used a minimal number of features(tags), i.e., only five within the body tag of a web page. The approach was tested on a limited dataset, i.e., 100 legitimate sites and 100 phishing sites. The study itself claims a small size of the corpus.	8
Suleman and Awan, 2019	Machine Learning & Heuristic	Naive Bayes Iterative Dichotomiser-3 K-Nearest Neighbor Decision tree Random Forest Genetic Algorithms	UCI machine learning repository	The research found that using ID3 along with Yet Another Generating Genetic Algorithm (YAGGA) gives the best Accuracy, 94.99%.	UCI dataset is open source and has normalized features. It does not include the Original URL.	
Jain et al., 2018	Machine Learning & Heuristic	Support Vector Machine Naive Bayes	PhishTank 33,000 instances 14 features	Experimental results showed 91.28% accuracy in detecting phishing websites using the Support Vector Machine classifier.	The study has achieved comparatively low results for Accuracy as compared to other studies with the same dataset and classifier.	

Table 3 above shows the summarized accuracies of some previous works done by various authors in phishing detection, in which the proposed system outperformed.

The findings of the study shows that the proposed framework, which combines XGBoost and filter-based methods like mutual information gain, achieves a high level of accuracy, precision, recall, and F1-score in detecting and countering phishing attacks. Analytically, the framework demonstrated an accuracy of 97%, precision of 96.6% ,recall of 96.5%,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

F1-score of 96.6% and a ROC AUC score of 99.6%. further affirming its effectiveness in identifying and mitigating phishing attacks. These results highlight the potential of the combined approach in providing a timely and efficient solution to address the evolving threat of phishing attacks in the cybersecurity domain.

The table below summarizes these metrics, demonstrating the model's high accuracy, precision, recall, F1-score, and ROC AUC score.

Table 4: Result of the proposed

Metrics	Value (%)
Accuracy	97.0
Precision	96.3
Recall	96.5
F1-score	96.6
ROC AUC Score	99.6

From the results of the proposed hybrid model, which are higher and impressive. An accuracy of 97%, precision of 96.3%, recall of 96.5%, F1 score of 96.6% and ROC score of 99.6% were achieved against this same performance metrics of all related works on face detection research of this work. This further demonstrated the effectiveness and robustness of the developed system in accurately predicting, effectively detecting and mitigate phishing attacks, with a timely and powerful tool for enhancing cybersecurity defenses.

V. CONCLUSION

The study successfully demonstrates that integrating filter-based feature selection methods with the XGBoost algorithm provides a highly effective framework for detecting and mitigating phishing attacks. The findings highlight the potential of combining mutual information gain for feature selection with the computational efficiency of XGBoost, presenting a robust and timely solution for enhancing cybersecurity defenses against the evolving threat of phishing attacks. The proposed system achieved exceptional performance metrics, including an accuracy of 97.0%, precision of 96.3%, recall of 96.5%, F1-score of 96.6%, and ROC AUC score of 99.6%. These results indicate that the framework not only offers rapid and reliable detection capabilities but also maintains high levels of accuracy and precision.

Recommendations: The suggested framework is hereby recommended for deployment in government and private organizations, to enhance adequate security of employees and organizational information and provide early detection in potentialsituations.

.

Author's contributions

Each author contributed to conceptualizing the study, in the designing the methodology, collecting data, developing algorithms, analyzing data, writing the manuscript, providing critical revisions, granting final approval and supervising the process.

Conflicts of Interest: The authors declare no conflicts of interest related to the research presented in this paper.

ACKNOWLEDGEMENT

This article received an immense support from my co-author who supported in the detailed review of literatures on similar research works by other authors in the same field in a bid to actualize this dream.

REFERENCES

[1]. Arshad, A.U. Rehman, S. Javaid, T.M. Ali, J.A. Sheikh and M. Azeem (2021). A Systematic Literature Review on Phishing and Anti-Phishing Techniques.

[2]. Basit, M. Zafar, A.R. Javed and Z. Jalil (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. In: Proceedings - 2020 23rd IEEE International Multi-Topic Conference INMIC 2020.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

[3]. K. Jain and B. Gupta (2018). PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning. Computer Science.

[4]. Mughaid, S. Alzu'bi and E. Elsoud (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*. Advance online publication.

[5]. Petrosyan (2024). Phishing most targeted industry sectors worldwide Q1 2024. Retrieved from (https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/#:~:text=During%20the%20first%20quarter%20of,for%209.8%20percent%20of%20attacks.)

[6]. A.K. Jain, S. Parashar, P. Katare and I. Sharma (2020). Phishskape: A content based approach to escape phishing attacks. Procedia Computer Science: Third International Conference on Computing and Network Communications (CoCoNet'19.

[7]. A.S. Raja, G. Pradeepa and N. Arulkumar (2022). Mudhr: Malicious URL detection using heuristic rules based approach. In AIP Conference Proceedings (Vol. 2393, No. 020176).

[8]. Coste (2024). Using Ensemble Models for Malicious Web Links Detection. In *Proceedings of the International Conference on Computer Science* (pp. 1-6).

[9]. E. Benavides, W. Fuertes, S. Sanchez and M. Sanchez (2020). Classification of phishing attack solutions by employing deep learning techniques: a systematic literature review. In: Rocha, Á., Pereira, R. (eds) Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152.

[10]. E.S. Shombot, G. Dusserre, R. Bestak and N.B. Ahmed (2024). An application for predicting phishing attacks: A case of implementing a support vector machine learning model. Cyber Security and Applications, 2, 100036.

[11]. F.A. Ghaleb, M. Alsaedi and M., Alasli (2022). Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. In *Proceedings of the Italian National Conference on Sensors and Microsystems. Sensors, 22(9), 3373.

[12]. G.J.W. Kathrine, P.M. Praise, A.A. Rose and E.C. Kalaivani (2019). Variants of phishing attacks and their detection techniques. Proceedings of the international Conference on Trends in Electronics and Informatics, ICOEI 2019, Icoei, pp. 255–259.

[13]. International Conference on Computing and Data Science (CDS).

[14]. J.M. Lindamulage, M.L. Pabasari and J. Krishara (2023). Vision GNN Based Phishing Website Detection. In *Proceedings of the International Conference on Computer Science and Engineering (ICSES)* (pp. 1-6). IEEE.

[15]. K.R. Nataraj, D.K. Yashaswini, R. Hema, N.S Pawar and S. Yashaswi (2022). Phishing attack detection using machine learning. In Proceedings of the 4th International Conference on Data Science, Machine Learning and Applications (ICDSMLA 2022) (pp. 355-370).

[16]. M. A. Adebowale, K.T. Awin and M.A. Hossain (2020). Intelligent phishing detection scheme using deep learning algorithms. Journal of Enterprise Information Management.

[17]. M. Babagoli, M.P. Aghababa and V. Solouk (2019). Heuristic nonlinear regression strategy for detecting phishing websites. Soft Comput., 23 (12) (2019), pp. 4315-4327.

[18]. M. D. Abdulrahaman, J. K. Alhassan, O. S. Adebayo, J. A. Ojeniyi and M. Olalere (2019). Phishing Attack Detection Based on Random Forest with Wrapper Feature Selection Method. International Journal of Information Processing and Communication, 7(2), 209-224.

[19]. M. Elsadig, A.O. Ibrahim and W. Nagmeldin, W (2022). Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. *Electronics*, 11(22), 3647.

[20]. M. Shoaib and M. S. Umar, "URL based Phishing Detection using Machine Learning," *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*

[21]. M.T. Suleman and S.M. Awan (2019). Optimization of URL-based phishing websites detection through genetic algorithms. Automatic Control and Computer Sciences.

[22]. M.V. Kunju, E. Dainel, H.C. Anthony and S. Bhelwa (2019). Evaluation of phishing techniques based on machine learning. International Conference on Intelligent Computing and Control Systems, ICCS 2019, Iciccs, pp. 963–968.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

[23]. R. Naresh, A. Gupta and S. Giri (2020). Malicious URL Detection System Using Combined SYM and Logistic Regression Model. *InfoSciRN: Information Architecture (Topic)*. Corpus ID: 237529693.

[24]. R. Sultana, M.A. Rahman and M.I. Khan (2023). Hybrid Model Based Phishing Websites Detection Using Deep Learning Technique. In 2023 26th International Conference on Computer and Information Technology (ICCIT) (pp. 1-6).

[25]. R. Yang, K. Zheng and X. Wang (2021). Phishing Website Detection Based on Deep Convolutional Neural Network and Random Forest Ensemble Learning. In *Proceedings of the Italian National Conference on Sensors and Microsystems*. Sensors, 21(24), 8281.

[26]. S. Goyal. (2020). Boosting performance with XGBoost. *Towards Data Science*, retrieved from Towards Data Science

[27]. S. Kaitholikkal and A. Balakrishnan (2024). Generative adversarial network-based phishing URL detection with variational autoencoder and transformer. IAES International Journal of Artificial Intelligence (IJ-AI), 13(2), 2165-2172.

[28]. T. Peng, I. Harris, Y. Sawa, Detecting phishing attacks using natural language processing and machine learning, in presented at the 2018 IEEE 12th International Conference on Semantic Computing (ICSC) (2018), pp. 300–301.

[29]. Telecommunication Systems.

[30]. V. Patil, P. Thakkar, C. Shah, T. Bhat and S.P. Godse (2018). Detection and prevention of phishing websites using machine learning approach. 2018 Fourth international conference on computing communication.

[31]. W. Bai (2020) "Phishing Website Detection Based on Machine Learning Algorithm," *2020 International Conference on Computing and Data Science (CDS)*, Stanford, CA, USA, 2020, pp. 293-298.

[32]. X. Liu and J. Fu (2020). SPWalk: Similar property-oriented feature learning for phishing detection. Ieee Access, 2020 - ieeexplore.ieee.org