

Deep Neural Network (Deep-NN) technique for detecting web phishing in transactional system

Vivian Onyinyechi Anthony¹, Ayobami Gabriel Ayeni²

¹Department of Computer Science, University of Port Harcourt, Nigeria, vivian.anthony@uniport.edu.ng

² Department of Computer Science, Dominion University, Nigeria, ayeni4great@yahoo.co.uk

Corresponding author's email: ayeni4great@yahoo.co.uk

Received: March 20, 2026 | Accepted: July 14, 2026 | Published: October 02, 2026

Abstract

Phishing is a prevalent cybercrime in which attackers deceive internet clients into divulging confidential details, such as credit card or financial information, in business-related transactions. Web phishing involves creating fraudulent websites that closely resemble legitimate ones, misleading users into submitting confidential information. Cybercriminals increasingly exploit phishing attacks to conduct security breaches because existing phishing detection systems lack robust defensive strategies. This study explores Deep Neural Networks (Deep-NN) as advanced classifiers for optimizing phishing detection performance. The dataset, sourced from a web repository, underwent pre-processing to extract relevant features and was cleaned for accurate classification. The experiment utilized 10,000 phishing data instances with 10 selected attributes, resulting in a 10,000 x 10 data dimension for simulation. The implementation was conducted using Python's machine learning libraries, MATLAB for simulation, and Microsoft Excel for data preparation. The Deep-NN system was evaluated using scientific experiments, achieving improved phishing detection performance. Key results include a mean squared error (MSE) of 1094. `6, indicating the average squared difference between the classified output and the expected target, and a regression (R) value of 0.99, demonstrating a strong correlation between the predicted and actual values. As well as a high similarity coefficient in the Jaccard index. These findings show significant improvement over existing models. The study recommends further exploration of supervised learning algorithms to filter legitimate web traffic from large datasets and optimize classification performance.

Keywords: Dataset, Deep-NN, Detection intrusion, Phishing, System

1. Introduction

Network security has now become a challenging subject, especially in the field of information technology. Nowadays, websites offer services of all kinds to network users, such as e-mail, instant messaging, file sharing, voice over IP, social media and electronic commerce websites which store users' confidential details (Smith, 2021). Fraudsters always try to steal users' confidential information by using misleading Uniform Resource Locators (URLs). Millions of people are connected to the internet, and it is essential to secure the data and information until it reaches its destination on time. The advent of Internet, one may readily obtain information and conduct numerous transactions. Beyond the convenience issue and accessibility, several cyber risks are hovering to assault and attack internet users, which is generally referred to as web phishing (Stallings, 2022).

Phishing is a cyber-offence that attempts to deceive the target users into divulging sensitive information. A false web page is created to look like the original website page, so the target does not realize they have been captured, and their personal information, such as login credentials, passwords, or account numbers, has been taken over and exploited by cybercriminals (Thompson, 2023). This phishing web mainly targets transactional websites such as financial institutions, e-commerce, airlines and travel, and banks (Müller, 2023). Securing communication and information in a public network is becoming more and more important with the advancement of internet or mobile networks day by day. Numerous approaches have been proposed to protect data; however, cryptography is one of the most dependable approaches used to secure data (Al-Qarni & Al-Asamani, 2024). Cryptographic

methods help in hiding original data into unimaginable data. Most common approaches to cryptographic application are symmetric and asymmetric keys (Zulfikri et al., 2024). The symmetric key normally uses just one key for handling the encryption and decryption of data and consumes little energy and small storage space (Mohammed et al., 2025). Intrusion detection is a security procedure for identifying likely attacks or threat through effective technique for detecting suspicious activities from the host and network ends (Mohammed et al., 2025); a security mechanism that defend a system by escalating to notify the users of security breach and in order to take proper action to stop the intruder (Chen & Zhao, 2023).

Consequently, the effectiveness of anomaly-based detection lies on the quality of the detection model or classifier, which is also dependent on the quality of the network data instances used for training. Once the classification algorithm has been trained as detection engine, it can correctly detect attacks (Solis-Escobedo et al., 2024). Intrusion Detection Systems (IDS) are defined in terms of three essential functional mechanisms: information sources, analysis, and response.

The sources of event information, such as incoming packets or data, are crucial in determining whether an intrusion is occurring or has already taken place (Sadre & Sperotto, 2021). The detection mechanism determines when the collected events indicate that intrusions are happening; most common analysis methods are misuse detection and anomaly detection. Once the system detects an intrusion, it sends a response (Johnson, 2020). Neural networks are computational models inspired by the human brain, consisting of interconnected artificial neurons (Janapa et al., 2022).

The deep neural network harnesses the capabilities of neural networks in conjunction with deep learning techniques and accompanying data mining algorithms to work with large datasets. In Deep Learning (DL), networks possess multiple hidden layers that learn hierarchical feature representations, enhancing performance across various tasks (Tang & Mahmoud, 2021; He et al., 2023). Phishing attacks have become a pervasive threat in the digital landscape, with cybercriminals creating counterfeit websites that imitate legitimate ones to steal sensitive information, including passwords, credit card details, and personal data.

The frequency and sophistication of these attacks have escalated, significantly impacting individuals, governments, and businesses. The primary method employed in phishing attacks involves distributing deceptive URLs, leading to considerable financial losses and breaches of confidential information. Despite the development of phishing detection systems, several limitations hinder their effectiveness; existing systems primarily identify specific, known types of attacks but lack the flexibility to adapt to new and evolving phishing techniques, creating security gaps. More importantly, performance precision and operational efficacy in analysing and detecting malicious incoming network traffic is a crucial gap that have not been adequately addressed.

2. Materials and Methods

Simulation based design was adopted by incorporating specificity-based filter functions in deep learning algorithms with neural network classification technique. Hybridization of deep learning and neural networks brings about deep neural networks, which were adopted as artificial intelligence and/or classification technique for mining traffic data in computer network in a bid to detect cyber threats that are specifically regarded as phishing attacks. Experimental analysis of detection framework in phishing intrusion involves the development of a deep neural network-based model, that classifies incoming data from network traffic or web server in real-time. These data instances were captured from the web repository for network data while relevant features were extracted and cleaned as pre-processed datasets to fit into the classifier's parameters or multivariate predictors of deep learning technique which were used to define the classifier's target or input/output variables.

2.1. Dataset Acquisition

The datasets used for experimental analysis in this study were sourced from Kaggle machine learning repository for web phishing. The data is adequate in size for deep neural networks to improve detection models, comprising ten thousand (10,000) instances of phishing datasets in terms of quantity. Phishing data was collected for experimental cases, and to evaluate functional performance of the improved (Deep-NN) classifier in this study, through a web repository for machine learning. Experimental design in this study involved ten thousand (10,000) data instances with exactly ten (10) attributes, thereby forming ten thousand by ten (10,000 x 10) dimensions.

The datasets emanating from ten thousand (10,000) data points of phishing were properly cleaned. A proportion or certain percentage of the dataset was used to validate the improved model (Deep-NN) for the proposed system after the training, before identifying matching patterns for phishing in test data or testing sets as shown in figures 1 and 2.

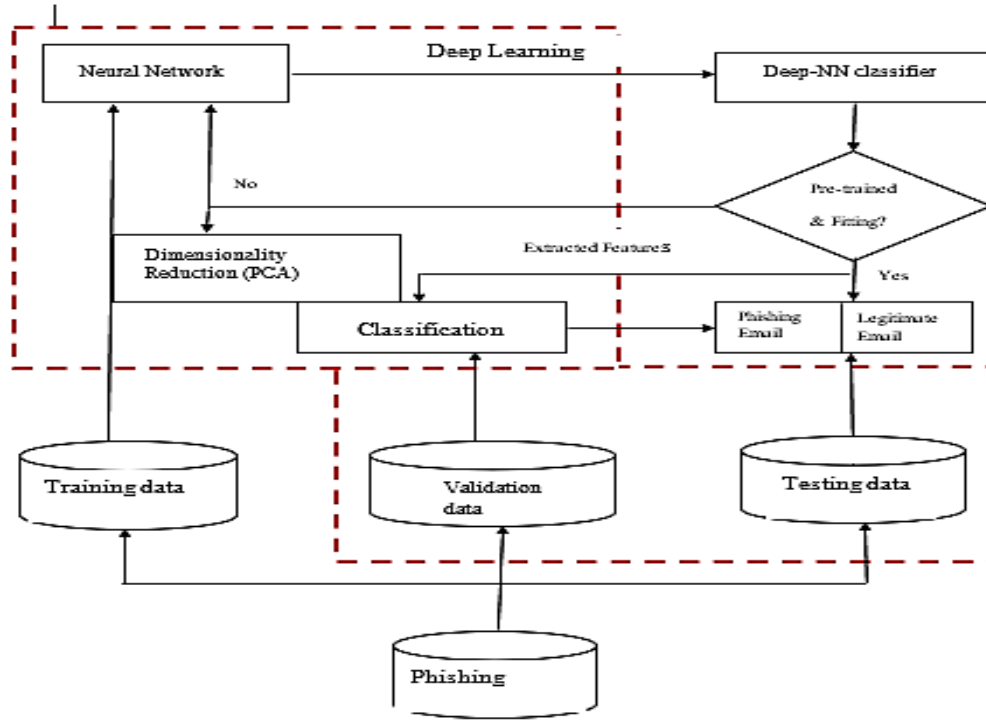


Figure 1: Architecture of the Deep-NN Phishing Detection System

Figure 1 shows the Deep-NN architecture in which each node performs its designated function on incoming signals according to the given chain to map enormous dependencies and patterns in huge volumes of data. The set of variables associated with a particular node becomes the input or incoming signals to that node and embedded in the chain rule as an inference mechanism. Figure 2 shows the inflow and outflow of traffic data during input and output operations by the classifier (Deep-NN) model, being the operational mechanism in approximating the observed sequence or matching pattern in the testing set according to a predefined rule (connection weight in each layer and cumulatively for multi-layers) of deep neural network (Deep-NN) for input variables during training and validation.

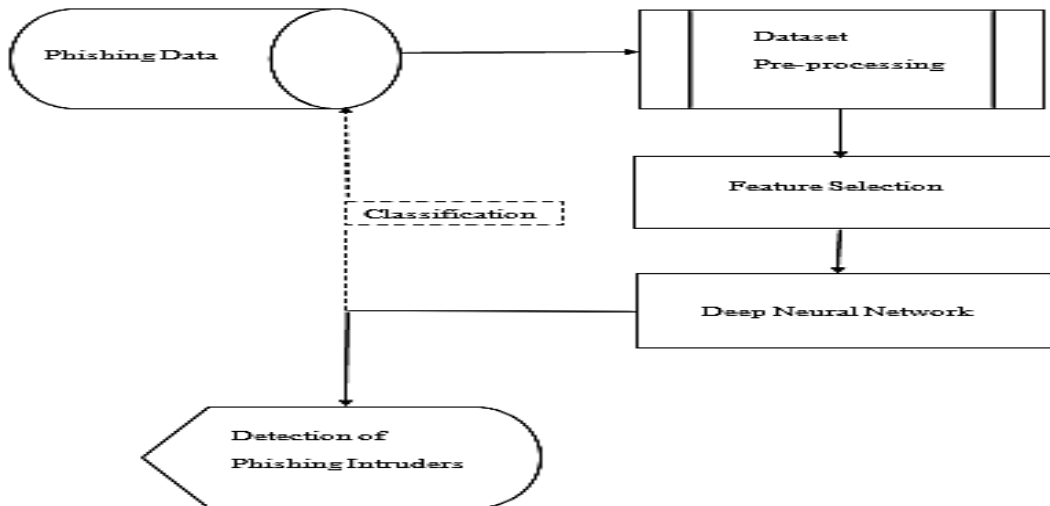


Figure 2: Deep Neural Network (Deep-NN) Detection Model

2.2. Data Pre-processing

Dimensionality reduction technique was applied to extract the ten (10) most relevant features, which capture the phishing data from fifty (50) attributes. Sci-kit Learn and Kiwi Solver libraries of the Python programming language were used to execute the method of dimensionality reduction as shown in figure 3. Thereafter, pre-processed phishing datasets were segmented into three proportions: sixty percent (60%) as a training set for machine learning with a predefined sequence of features, twenty percent (20%) for validation to substantiate the

appropriateness and readiness of the improved model for phishing detection; while the last twenty percent (20%) were used as a testing set to evaluate the experimental performance using Regression (R), Mean Squared Error (MSE), and Jaccard index as the metrics.



```

Python 3.8.8 (default, Apr 13 2021, 15:08:07) [MSC v.1916 32 bit (Intel)]
Type "copyright", "credits" or "license" for more information.

IPython 7.22.0 -- An enhanced Interactive Python.

In [1]: runfile('C:/Users/Dr. Bami/.spyder-py3/temp.py', wdir='C:/Users/Dr. Bami/.spyder-py3')
(1000, 20) (1000,)

In [2]: runfile('C:/Users/Dr. Bami/.spyder-py3/temp.py', wdir='C:/Users/Dr. Bami/.spyder-py3')
(1000, 20) (1000,)
Accuracy: 0.824 (0.034)
    
```

Figure 3: Spyder Interface for Python Program Output

Figure 3 shows the Python program which depicts the partitioning to reduce the high dimension of acquired datasets from fifty (50) features to a lower dimensional subspace of ten (10) features as input.

3. Results and Discussion

The attributes of the dataset are the given data samples, pre-defined in two major clusters: features/independent variables and target/dependent variable. Essential features like NumDash, NumDashInHostname, AtSymbol, PathLevel, UrlLength, DomainInPaths, HostnameLength, DomainInSubdomains, httpsInHostname, and IP address were carefully extracted as key indicators for Class_Label, which is the target to determine the presence of a phishing intruder.

MATLAB's toolbox is embedded with computational capabilities in machine learning or data mining, making it possible to simulate hypothetical networks for experimental scenarios due to the cost implications of setting up a network environment. Python is a general-purpose programming language with a design approach that emphasizes code modularity with proper use of space and block indentation. The outcome of valid and invalid data in performance testing as independent indicators or input variables are shown in Figures 4 to 6, as well as the detection mechanism related to the presence or absence of phishing intruders, which helps to accomplish the major objectives of this study.

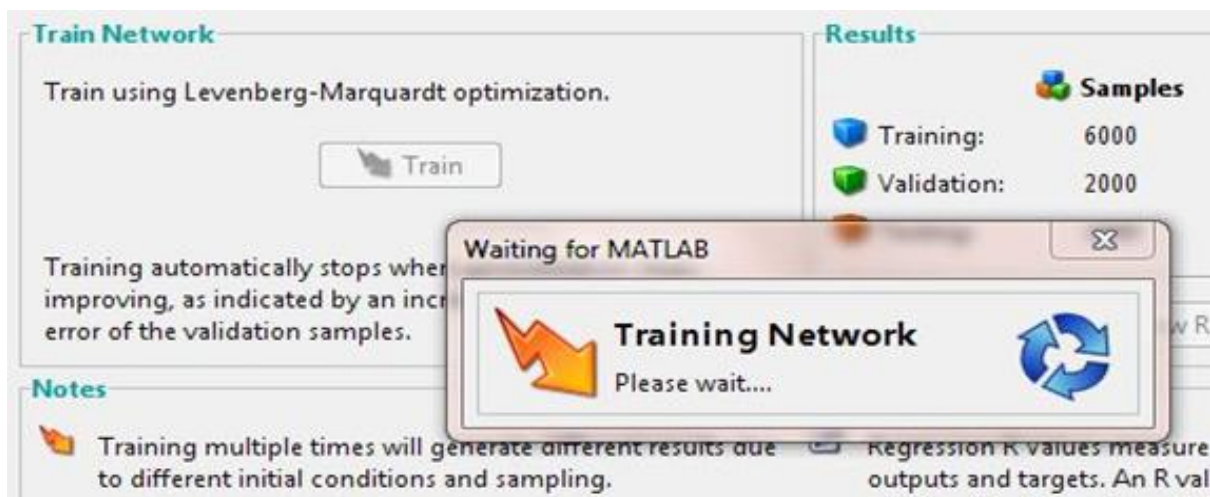


Figure 4: Training Phase for Deep Neural Network using Pre-processed Sample

Figure 4 shows the training of a deep neural network in progress, having initialized the network training phase with sixty percent (60%) of the acquired and pre-processed dataset which constitutes six thousand (6000) instances as the training set.

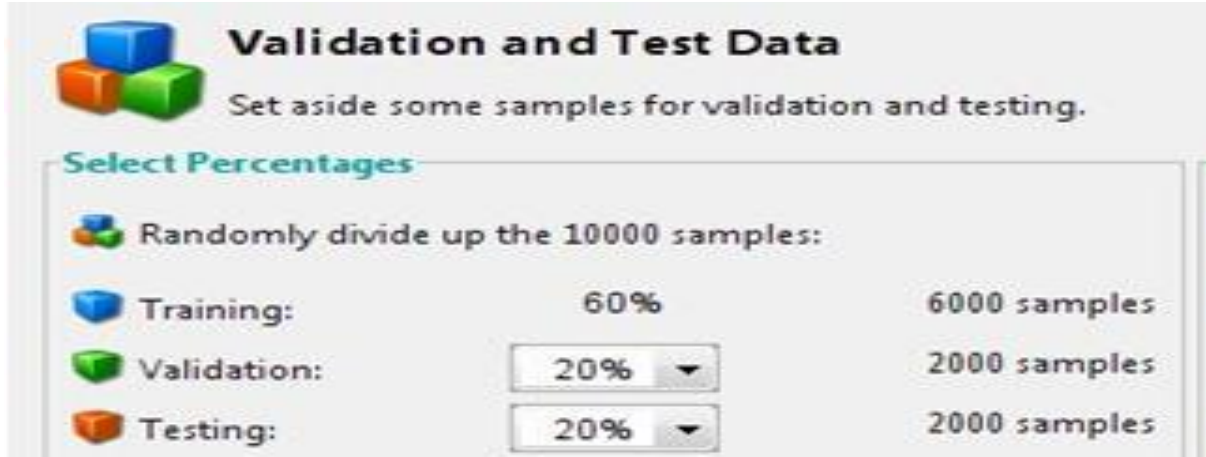


Figure 5: Validation and Testing Clusters using Pre-processed Samples

Figure 5 shows random segmentation of pre-processed data as the validation and testing sets. Having trained the proposed system in consequent upon features' optimization with sixty percent (60%) of the pre-processed dataset, which constitutes six thousand (6000) instances of data as training set. Twenty percent (200%) of the acquired and pre-processed dataset which constitutes two thousand (2000) instances or data samples as validation set. And the last twenty (20%) of the acquired and pre-processed dataset which constitutes two thousand (2000) instances.

Experimental analysis of the Deep-NN model for phishing detection revealed multi dimension nature of phishing data, while the model reliability was ascertained through simulation. Filtering the feature set of huge data instances helped to optimize the performance of phishing detection system. The results obtained, returned a regression value of 1 to validate Class_Label showing close relationship between classified outputs and the class targets as shown in table 1. The discretized values from the validated test data, were used to measure network generalization by expected output. Class_Label value of 0 refers to the presence of phishing or simply the phishing threat while Class_Label value of 1 refers to legitimate content or the normalcy.

S/N	Path	URL	Num	At	Ip	Domain	Class_
	Level	Length	Dash	Symbol	Address	In Paths	Label
1	5	72	0	0	0	0	1
2	3	144	0	0	0	0	1
3	2	58	0	0	0	0	1
4	6	79	1	0	0	1	0
5	4	46	0	0	0	1	1
6	1	42	1	0	0	1	1
7	5	60	0	0	0	1	0
8	3	30	0	0	0	1	1
9	2	76	1	0	0	1	1
10	2	46	0	0	0	1	1
11	2	64	1	0	0	1	1
12	2	47	0	0	0	0	1
13	2	61	1	0	0	0	1
14	3	35	0	0	0	0	0
15	2	60	1	0	0	0	1
16	4	73	0	0	0	1	1

17	5	50	0	0	1	0	1
18	2	59	1	0	0	1	1
19	3	28	0	0	0	1	1
20	4	59	0	0	0	1	1
21	4	32	0	0	0	0	0
22	2	52	0	0	0	0	1
23	6	62	1	0	0	0	1

Table 1: Extract from Experimental Results of the (Deep-NN) Phishing Detection

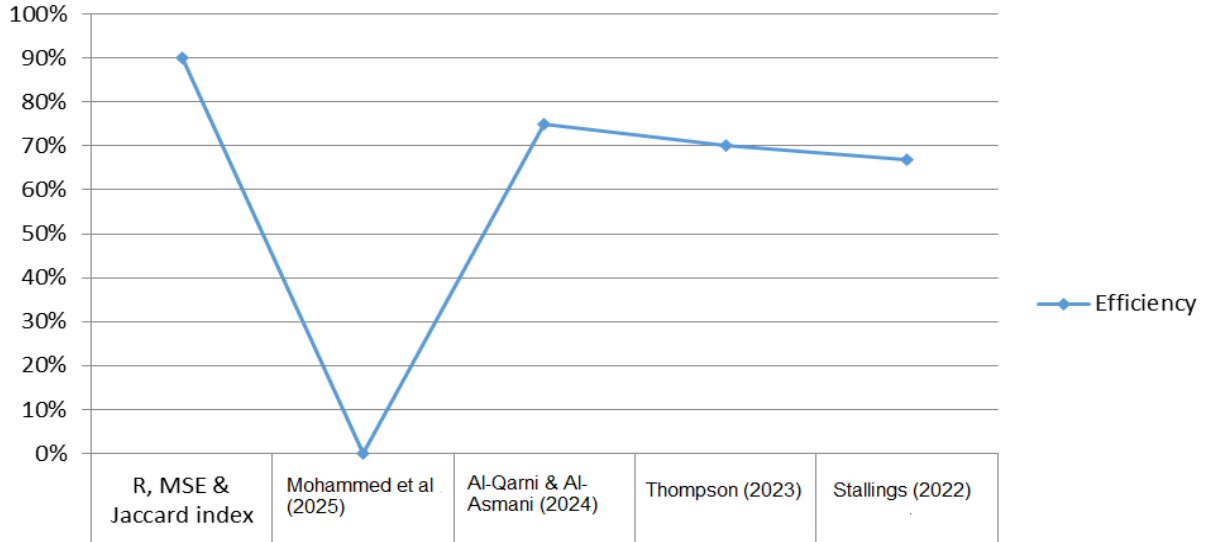


Figure 6: Efficiency Line chart for Graphical comparison

Figure 6 also showed that efficacy of detection algorithm gave Deep-NN technique higher efficiency over others, and to handle optimal features from phishing elements of instances which aligns with other scholars (Mohammed et al., 2025).

4. Conclusion

The efficiency of the improved technique being provided is evident in regression value (R) of 0.99; thereby classifies phishing link from web payment domain of transactional system, paving the ways for timely mitigation strategies. The regression (R) value obtained with a very meagre mean square error implies a resounding success, with swift response to cyber threats emanating from phishing intruders.

Potential data analytics or simulation tools set the pace for further enhancements and ethical consideration necessary for seamless integration into information security frameworks. Unwavering commitment to ethical practices is also germane to system evolution, yielding significant impact on cyber threats prevention, optimizing mitigation method, and thereby preserving the personal financial information.

References

1. Al-Qarni, E.A. and Al-Asmari, G.A., 2024. Addressing imbalanced data in network intrusion detection: A review and survey. *International Journal of Advanced Computer Science & Applications*, 15(2), p.136.
2. Junhua, C. and Shengjun, W., 2009, August. Stability analysis of worm propagation dynamics based on quarantine. In *2009 2nd IEEE International Conference on Computer Science and Information Technology* (pp. 380-384). IEEE.
3. He, K., Kim, D.D. and Asghar, M.R., 2023. Adversarial machine learning for network intrusion detection systems: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 25(1), pp.538-566.
4. Janapa Reddi, V., Kanter, D., Mattson, P., Duke, J., Nguyen, T., Chukka, R., Shiring, K., Tan, K.S., Charlebois, M., Chou, W. and El-Khamy, M., 2022. MLPerf mobile inference benchmark: An industry-standard open-source machine learning benchmark for on-device AI. *Proceedings of Machine Learning and Systems*, 4, pp.352-369.
5. Johnson, B., 2020. Impact of Phishing on Governments and Businesses. *Tech Insights*, 12(4) 40-55. Retrieved from <https://example.com/impact-of-phishing>

6. Mohammed, S.A.A.Q., Osman, Y.M.M., Ibrahim, A.M. and Shaban, M., 2025. Ethical and regulatory considerations in the use of AI and machine learning in nursing: A systematic review. *International nursing review*, 72(1), p.e70010.
7. Möller, D.P., 2023. Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Cham: Springer Nature Switzerland.
8. Solis-Escobedo, J.R. Gomez-Rodriguez, J.R. and Rodriguez-Abdala, V.I., 2024. Modern Intrusion Detection Systems: A Review and Comparative Analysis. *Journal of Software Engineering and Applications*, 14(5), 340-350.
9. Sadre, A. and Sperotto, M., 2021. Advances in Intrusion Detection Systems: A Comprehensive Review. *International Journal of Information Security*, 20(2), 147-169. <https://doi.org/10.1007/s10207-021-00515-6>
10. Stallings, W., 2022. *Cryptography and Network Security: Principles and Practice*. Proceedings of the 8th Pearson Annual Computing Conference.
11. Smith, A., 2021. Phishing Detection and Prevention Techniques, *Journal of Cyber Security*, 45, 23-35. Retrieved from <https://example.com/phishing-detection-techniques>
12. Thompson, E., 2023. Emerging Trends in Phishing Attacks: A Comprehensive Overview. *International Journal of Cyber Security*, 7, 11-20.
13. Tang, L., and Mahmoud, Q.H., 2021. A survey of machine learning-based solutions for phishing website detection. *Machine Learning and Knowledge Extraction*, 3(3), pp.672-694.
14. Zulfikri, A., Arifin, G., and Ilhamsyah, F.E, 2024. Analysis of phishing attack trends, impacts and prevention methods: literature study. *International Journal of Artificial Intelligence*, 4(1), 413-421.