Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

A Phishing Detection Model for Financial Web-Based Applications

Akinkitan Ajose ALLEN[1] and Solomon Olalekan AKINOLA[2]

[1]Department of Computer Science,
[2]Lead City University, Ibadan

akin_allen@yahoo.com[1]

Abstract

Phishing is a prevalent cybercrime in which attackers deceive internet users into divulging sensitive information, such as login credentials, financial details, or business-related data. 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, highlighting the need for more effective detection mechanisms. Existing phishing detection systems lack robust defensive strategies, particularly in mitigating phishing emails and handling limited test data for experimental analysis. This study explores Deep Neural Networks (Deep-NN) as advanced classifiers for optimizing phishing detection performance. A quasi-experimental design is employed, integrating specificity-based filter functions into a Deep Neural Network for unsupervised classification. The research involves building a deep learning model capable of analyzing real-time web traffic data. The dataset, sourced from a web repository, underwent preprocessing to extract relevant features and was cleaned for accurate classification. The experiment utilized 10,000 data phishing 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 proposed Deep-NN system was evaluated using scientific experiments, achieving an improved phishing detection performance. Key results include a mean square error (MSE) of 1094.6, indicating the average squared difference between classified output and expected target, and a regression (R) value of 0.99, demonstrating a strong correlation between the predicted and actual values. These findings show significant improvement over existing models. This research developed an enhanced model for detecting illegitimate activities in financial web-based applications but further exploration of other unsupervised learning algorithms to filter legitimate emails from large datasets and optimize classification performance is required in the future.

Keywords: Website, Applications, Model, Detection, Phishing.

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 networks, and online shopping, among others; these websites store users' confidential information (Tariq et al., 2023; Solis-Escobedo et al., 2024). 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. With the Internet, one may readily obtain

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

information and conduct numerous transactions. Behind the convenience and accessibility, numerous cybercrime risks are waiting to assault and harm internet users; this is sometimes referred to as web phishing. Phishing is a cybercrime that attempts to deceive the target (internet users) into divulging sensitive information (Erdogan et al., 2021; Zulfikri et al., 2024). A false website 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. This phishing web mainly targets transactional websites such as financial institutions, e-commerce, airlines and travel, and banks. 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 (Schneier et al., 2023; Singh et al., 2024). Numerous approaches have been proposed to protect data; however, cryptography is one of the most dependable approaches used to secure data. Cryptographic techniques help in altering original data into incomprehensible data. Two major approaches to cryptography are symmetric keys and asymmetric keys. The symmetric key approach uses only one key for both encryption and decryption of the data, which consumes less energy and memory. In contrast, the asymmetric cryptographic approach is much more secure than symmetric encryption because it uses two keys. However, generating two key results in higher energy, time, and memory consumption. A Wireless Network consists of a collection of mobile nodes connected wirelessly. Ad hoc networks require minimal configuration and can be deployed quickly, making them suitable for emergencies (Chen & Zhao, 2023; Shparlinski, 2025). A wireless ad-hoc network comprises various equipment, including a wireless router, stations, the Packet Tracer simulation tool, a network switch, a modem, MATLAB, PHP-MYSQL, laptop computers, an Intrusion Detection System, and software. An Intrusion Detection System (IDS) is a security procedure for detecting attacks. It is an effective technique for identifying suspicious activities at both the host and network levels (Solis-Escobedo et al., 2024). An IDS is a mechanism that protects a system by using alarms to notify of a security breach and can take measured action to stop the intruder. IDSs can be categorized into three main types: signature-based, specification-based, and anomaly-based. A signature-based IDS identifies bad patterns; if a match is found, an alarm is raised. While a signature-based IDS has high accuracy and a low false alarm rate, it is incapable of detecting new attacks. Specification-based network IDS match traffic behaviour (parameters) against a predefined set of rules and values (specifications) to detect malicious activities. Anomaly-based IDS distinguishes deviations from the norm. If a deviation exceeds a specified threshold, an alarm is raised to signify attack detection (Sadre & Sperotto, 2021). The normal network profile is learned using machine learning (ML) algorithms. Anomaly-based IDS are preferred over signature-based and specification-based IDS because of their ability to detect new attacks; however, this comes with the trade-off of a higher false alarm rate. Consequently, the effectiveness of anomaly-based IDS depends on the quality of the detection engine (model or classifier), which is influenced by the quality of the network traffic patterns (dataset instances) used for training the engine; hence this research.

2. Related Works

Numerous researchers have explored various aspects of phishing intrusion detection models and web-enabled information systems utilizing modified Diffie-Hellman algorithms. This section discusses several recent publications in this domain: A study on the implementation of the Diffie-Hellman algorithm for information security has been conducted (McDaniel et al., 2021). They employed the

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Diffie-Hellman key exchange protocol in cryptography to create a shared secret key between two users. The study provided an overview of the algorithm and detailed its implementation strategy, including various tests to evaluate its effectiveness. The results indicated that the Diffie-Hellman key exchange algorithm is a reliable cryptographic technique that secures information by establishing a shared secret key over insecure communication channels. The implementation utilized Python 3.11.0, leveraging standard library modules for generating random numbers and performing modular exponentiation. The findings confirmed that this method is dependable and efficient for establishing secure shared keys, which can safeguard sensitive information through encryption and decryption (Singh et al., 2024).

There is research that focused on Modified Elliptic Curve Cryptography (ECC) for secured data transfer in multi-tenant cloud computing environments74. Their research aimed at enhancing cryptographic efficiency by generating alternate keys to improve security. The performance evaluation covered various metrics, including encryption and decryption times, upload and download computation times, and overall memory usage. The results demonstrated that the MECC algorithm had lower processing times for these tasks compared to traditional algorithms like AES, Blowfish, and Twofish. Specifically, they noted a reduction in ciphertext key size by 836KB, alongside a key generation time of 35 seconds and encryption and decryption times of 51 and 159 milliseconds, respectively (Mondal et al., 2023).

A researcher has explored techniques associated with securing data transmission against Man-In-The-Middle (MITM) attacks using the Diffie-Hellman key exchange encryption mechanism75. They adopted Structured System Analysis and Design Methodology (SSADM) for their research. The Diffie-Hellman key exchange algorithm was integral to their key generation process, which involved encrypting files using the generated key. A notable aspect of their implementation was sending the key over a separate channel from the encrypted file, enhancing security during transmission. The study utilized a laptop with specific hardware configurations and employed Java for front-end programming and MySQL for database management. The results of the tests indicated significant improvements in data security against MITM attacks (Shparlinski, 2025). In another study, some group of researchers investigated digital envelope removal using an enhanced Diffie-Hellman Key Exchange in the Secure Electronic Transaction (SET) protocol (Chaudhary et al., 2022). They focused on employing hashing technologies for data integrity alongside advanced cryptography for secure data transfer. Their findings indicated that the improved SET protocol outperformed existing implementations by reducing overheads associated with encryption, decryption, key exchanges, and certificate management. Their approach utilized digital certificates for verifying transaction parties and included multiple cryptographic operations, successfully resisting various cryptanalysis techniques, including brute force and MITM attacks (Shparlinski, 2025). Enhancements to the Diffie-Hellman algorithm to improve network security have been developed (Chaudhary et al., 2022). Their study introduced additional security codes to strengthen encryption, enhancing the public key encryption protocol used within the network. They also analyzed vulnerabilities in the network and explored potential encryption mechanisms. The implementation utilized the C programming language, with comparisons drawn between the classical and improved Diffie-Hellman algorithms using the CrypTool. Implementing a key aggregate cryptosystem with the Diffie-Hellman key exchange algorithm for secured data sharing in cloud computing has been presented (Prastyo et al., 2020). They explained the use of public-key cryptosystems to create classes of fixed-size ciphertexts, resulting in efficient key decryption and enhanced confidentiality. Their system integrated the Diffie-Hellman key exchange algorithm with AES, significantly increasing security. An optical secret key sharing method based on the Diffie-Hellman key exchange algorithm has been proposed (Malik & Kumar, 2015). Their research involved

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

numerical simulations and modifications of the Diffie-Hellman protocol using optical XOR logic operations. They demonstrated a new method utilizing Mach-Zehnder type interferometers to facilitate secure key sharing. This method improved security through double key encryption, achieving a higher level of cryptographic protection than traditional Diffie-Hellman implementations. An improved cryptanalysis of provable certificateless generalized signcryption has been proposed (Minocha & Singh, 2022). The proposed scheme demonstrated security against IND-CCA2 and EUF-CMA in the presence of a malicious key generation center, proving effective for both secrecy and authenticity. A novel technique for generating keys in the Diffie-Hellman algorithm using image pixels has been proposed (Smith & Anderson, 2021). They proposed a method for calculating p and g values as true random numbers, enhancing security against potential leaks in prior algorithms. A technique that focused on minimizing packet drop due to black hole attacks in wireless ad-hoc networks using intrusion detection systems has been established (Kumar & Patel, 2023). Their study employed a packet transmission scheme to reduce packet loss, utilizing MATLAB and PHP-MYSQL for simulation. A watermarking and intrusion detection system framework for insider attack detection in cloud-based e-healthcare data management have been explored (Lee & Chang, 2023). They utilized convolutional neural networks and improved algorithms for resource allocation, focusing on watermarking techniques to identify malicious insiders. A method for generating private keys in the Diffie-Hellman algorithm through user-defined equations already exist (Johnson & Wu, 2023). Their experimental results demonstrated the algorithm's effectiveness in producing secure factors resistant to external attacks. A deep learning algorithm for intrusion detection in IoT networks has been developed (Malik & Kumar, 2023). Their study utilized a recently released IoT dataset to classify traffic flows, achieving high accuracy and precision in identifying various types of attacks. A systematic literature review on IoT security, focusing on deep learning-based intrusion detection systems have been explored (Yousif, 2021). They examined known security threats within the Cisco IoT reference model architecture, providing insights into existing research on IoT vulnerabilities and threats. These studies collectively contribute to the understanding of the role of modified Diffie-Hellman in enhancing security in various systems, particularly in the realms of cryptography, secure data transmission, and intrusion detection.

3. Methodology

In this research, a quasi-experimental design was adopted by incorporating specificity-based filter functions in deep learning or machine learning algorithms with unsupervised classification techniques. Hybridization of deep learning and neural networks brings about deep neural networks, which were adopted as artificial intelligence and/or classification techniques for mining traffic data in computer networks for financial systems 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.

3.1 Data Source, Nature, Size and Pre-processing

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

The datasets used for experimental analysis in the proposed system were sourced from Kaggle Machine Learning Repository; incorporated by Shash Watwork for the phishing data (https://kaggle.com/datasets/shashwork/phishing-dataset-for-ml/). The data is adequate in size for deep neural networks to improve detection models, comprising ten thousand (10,000) instances or elements of phishing datasets in terms of quantity. The multivariate nature of the data instances being inherited from open repositories was well handled by the filtering approach during data preparation; hence, multiple characteristics or attributes of acquired datasets which could have generated several variables for the classification task were eventually limited to a few significant features as principal components for the predictor. The whole datasets emanating from ten thousand (10,000) data points of phishing were properly cleaned. Also, special characters or unrecognized tokens were excluded, as well as avoiding dense data due to missing values for some attributes or the outlier

3.2 System Design

The benchmark for this research is a novel framework and notable technique of an existing system, which was developed for phishing detection. The concerns of the existing system were borne out of frequent cases of social engineering attacks and the need for defensive approaches through machine learning to address these issues in cyberspace to mitigate economic consequences. A data mining algorithm was applied to selected features, being extracted from different datasets to generate seventy percent (70%) labeled data as a training set, while the rest thirty percent (30%) of labeled data was used as a testing set. Data cleaning was necessary to allow the removal of irrelevant text and special characters that come as metadata from the dataset repository. Text data emanating from captured data packets and incoming traffic were discretized to numeric values. The linear algebra approach helps to handle the high dimensional nature of the dataset with linear discriminant analysis (LDA), for projecting the attributes of data instances in lower-dimensional subspace. The LDA algorithm was inculcated as a dimensionality reduction technique which ensures a perfect degree of freedom due to limited input variables by few relevant features posing the essence of data in the training and testing phase of the novel model in the existing system. The explosive growth of phishing attacks is severe among other threats in social engineering, thereby optimizing the sensitivity of the detection mechanism by combining binary modified optimization technique with K-nearest neighbor (KNN) for the classification task. Experimental simulation of the detection model with unsupervised learning for testing and evaluation was not embraced in the existing system. The proposed system is shown in Figure 3.1.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

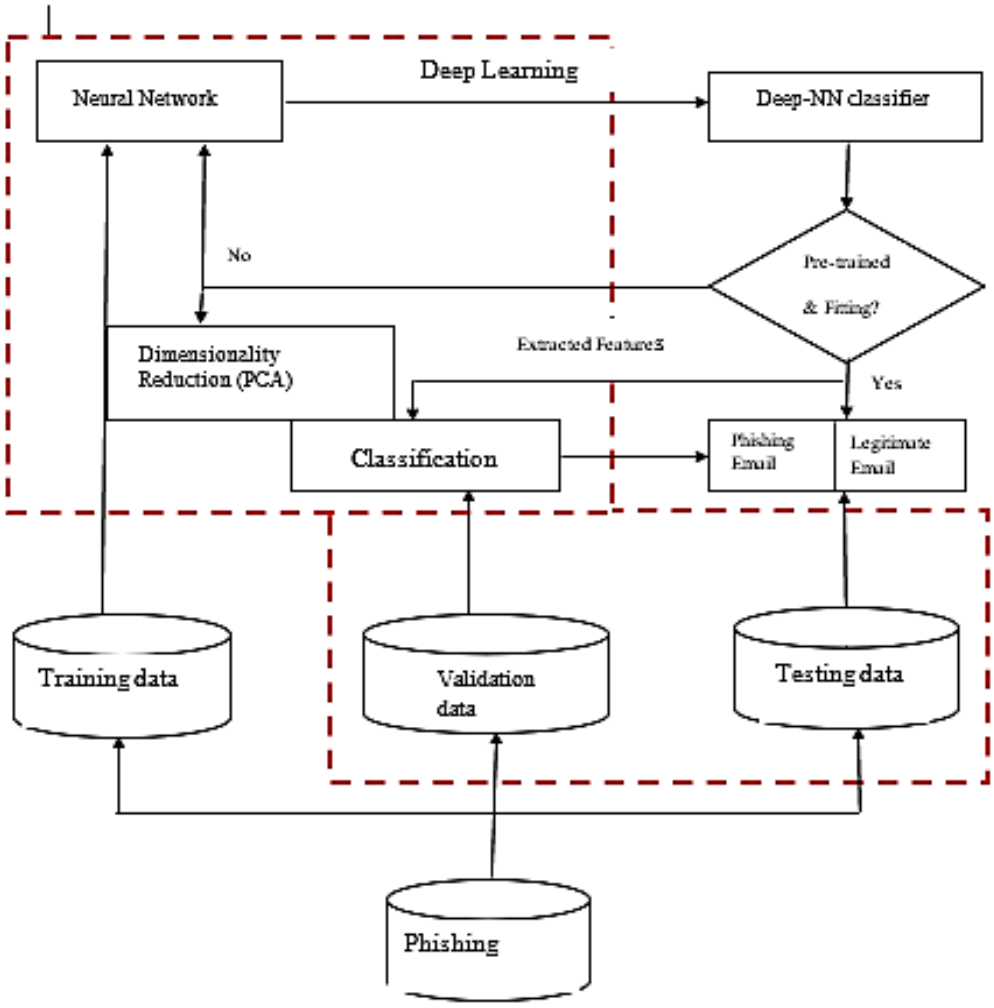

Figure 3.1: Architecture of the Proposed System.

3.3 Description of Proposed System's Functionality

The improved framework of the proposed system depicts how Sci-kit Learn and Kiwi Solver libraries of the Python programming language were used to execute the principal component analysis (PCA) method of dimensionality reduction; after the cleaning and scaling of the dataset which was acquired by remote capturing from the web repository. Thereafter, pre-processed phishing datasets were segmented into three proportions as follows: sixty percent (60%) as a training set for unsupervised learning with a predefined sequence of features, twenty percent (20%) for validation to substantiate the applicability or 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 of the proposed system using the specified metrics for performance evaluation. Conclusively, the deep neural network optimizes the classification function and learning rule of the improved model when the datasets are imported into the matrix laboratory (MATLAB). Computational dynamism was derived by the connection weights of Deep-NN, which were explored and manipulated to automate the model for effective system precision through experiments using pre-processed data and its efficient algorithm.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3.4 Pre-processing Phase and Feature Selection

In all the instances and experimental samples of phishing data, the datasets are discretized and multivariate in nature due to several characteristics of numeric values, but data pre-processing was done to reduce the dimension of the phishing dataset. The principal component analysis (PCA) method of dimensionality reduction was applied to extract the ten (10) most relevant features, which capture the phishing data from fifty (50) attributes. Removal of outliers limited the data instances to ten thousand (10,000) elements with ten (10) samples or features for input-target juxtaposition.

4. Results and discussion

The proposed system for phishing detection was subjected to experimental simulation and performance testing on a computing workstation or microcomputer with the installation of a matrix laboratory (MATLAB). It embedded the compatible plug-in or application programming interface (API) of Python programming language with necessary libraries or essential functions for discretization, vectorization, model fittings, and intelligent classification. The operational flow of data during input and output operations is executed by the classifier (Deep-NN) model, being the operational mechanism. A system prototype was created to experiment with the classification mode through a simulation program, by 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. Experimental analysis in this research involves ten thousand (10,000) instances of phishing datasets, whereby ten (10) samples (i.e., data attributes) were selected against ten thousand (10,000) elements (i.e., data points); thereby creating 10,000 x 10 dimensions of experimental data for simulation. The whole datasets emanating from ten thousand (10,000) cases of phishing were properly cleaned and scaled to exclude special characters or unrecognized tokens, as well as avoiding dense data due to missing values for data attributes or even with outlier values. The multivariate nature of the data instances being inherited from open repositories was well handled by the filtering approach during data preparation; hence, multiple characteristics or attributes of acquired datasets which could have generated several variables for the classification task were eventually limited to few significant features as principal components for predictors. Figure 4.1 shows the performance graph of network training, having completed the training cycle in three (3) epochs which learns algorithmically how to build the (DNN) model by using training datasets with expected outputs; and to estimate how well the model has been trained.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

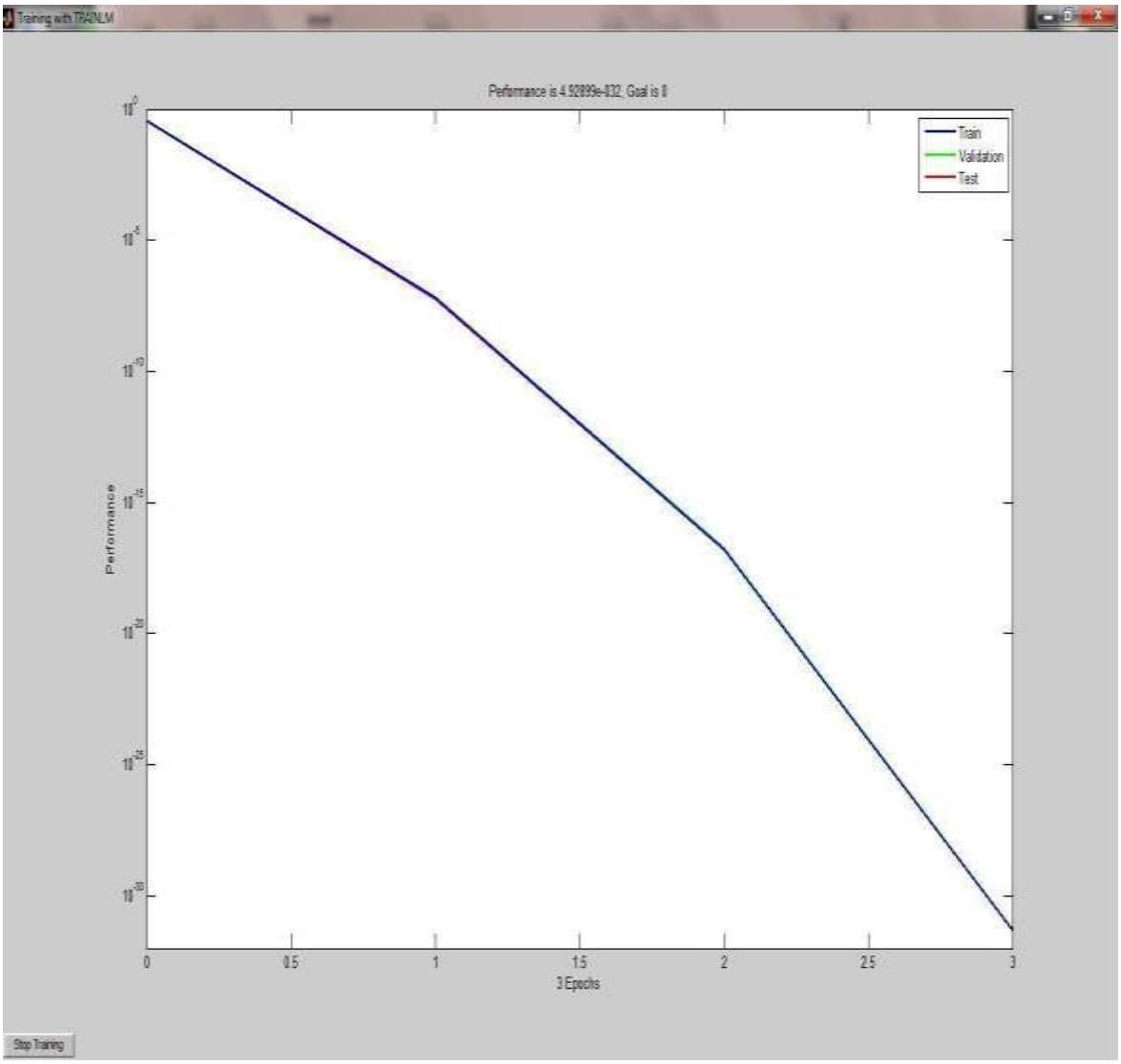

Figure 4.1: Graphical Representations of Training Cycle

Figure 4.2 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 (20%) 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.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

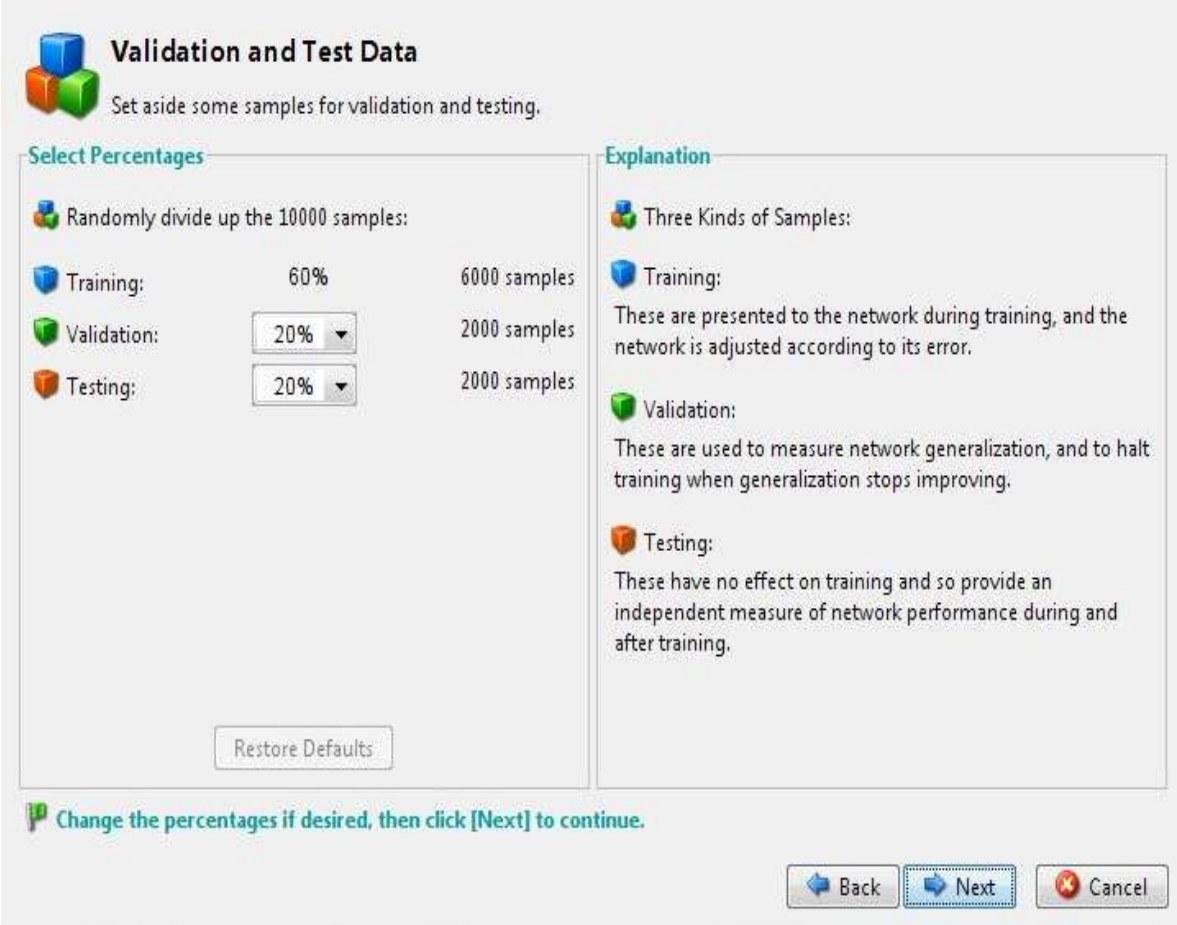

Figure 4.2: Validation and Testing Clusters using Pre-processed Samples

Six thousand (6000) datasets were used for training, two thousand (2000) datasets were used for validation, while two thousand (2000) datasets were used in evaluating the model performance. From Table 4.1, the efficiency of the improved technique being provided is evident in regression value (R) of 0.99; thereby proficiently identifies and classifies phishing mails from web servers or payment platforms of financial institutions, paving the way for timely mitigation strategies. Key results include a mean square error (MSE) of 1094.6, indicating the average squared difference between classified output and expected target, and a regression (R) value of 0.99, demonstrates a strong correlation between the predicted and actual values. These findings show significant improvement over existing models. The results recommend further exploration of unsupervised learning algorithms to filter legitimate emails from large datasets and optimize classification performance.

Kasu Journal of Computer Science Vol.2 No.3 [September, 2025], pp. 229-240
https://doi.org//10.47514/kjcs/2025.2.3.003

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Table 4.1: Experimental Results of the (Deep-NN) Phishing Detection System

S/N	Path Level	URL Length	Num Dash	At Symbol	Ip Address	Domain In Paths	Class_ 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	1
5	4	46	0	0	0	1	1
6	1	42	1	0	0	1	1
7	5	60	0	0	0	1	1
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	1
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

Hybridization of unsupervised methodologies and/or data mining algorithms of deep learning and artificial neural networks underscores the system's capacity to fill existing gaps in phishing detection and mitigation techniques. Its proficiency level accommodates diverse phishing scenarios as security threats and demonstrates substantial enhancements in performance precision compared to existing systems, thereby signifying its potential for transformative impact. Development of improved techniques and experimental simulation of the Deep-NN System for detecting phishing intruders in financial information systems is a far-reaching milestone in mining web-inclined traffic or communication data in the financial domain through classification mechanisms. The regression (R) value obtained with a very meager 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 stage for future enhancements, amalgamation, and ethical matters 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 strategies, and ultimately contributing to the preservation of financial data, personal information, and critical resources.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

5. Conclusion

The basic prerequisites in terms of hardware and software were delineated to clearly stipulate the operational landscape for the proposed system, emphasizing the functional boundary as an experimental artifact which requires optimal performance in decision-making. Experimental analysis of the improved detection model was technically inclined with simulation, encompassing critical routines like feature selection, data pre-processing, unsupervised learning, model validation, training, and testing. Scientific experiments for validating the model functionality substantiated the efficacy of the improved detection system; with a remarkable regression (R) value of approximately 1 showing correlation coefficient for a higher precision rate. Acquiring more datasets and increasing the proportion of the training set for the proposed Deep-NN model would be necessary in future work. The peculiarity of deep learning and huge data as the basis for validating unsupervised learning strategies in phishing detection invariably aligns with the rationale behind experimental analysis. Hence, algorithm refinement for selecting and handling optimal features in localized data instances from the financial domain of indigenous firms is automatically inclusive in the area for further study. Further exploration of the unsupervised learning approach is quite germane to examine the performance variability of datasets on an ensemble of machine learning techniques. Additional metrics in performance evaluation are essential in ascertaining its scalability prior to real-time integration in financial information systems.

References

B. Schneier (2023). A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back. Norton, 120-140.

C. Lee & T. Chang (2023). Unsupervised Learning Techniques for Feature Extraction in Phishing Detection: A Comparative Study. Cybersecurity and Privacy, 3(1), 42-60.

D. Mondal, N. Thangarasu, Y. S. Ingle, A. Saxena & J. R. Kumar (2023). Investigating the Effectiveness of Internet Key Exchange (IKE) Protocol in Wireless Network Security. In: 3rd International Conference on Smart Generation Computing, Communication and Networking, 1-5. IEEE.

F. P. E Zulfikri, A. Arifin, G. & R. M. Ilhamsyah (2024). Analysis of phishing attack trends, impacts and prevention methods: literature study. Brilliance: Research of Artificial Intelligence, 4(1), 413-421.

G. Erdogan, M. Ozkaya & E. Karaman (2021). Web Browser Fingerprinting: Techniques and Countermeasures. Journal of Privacy and Confidentiality, 12(1), 50-68. Available at: https://doi.org/10.29012/jpc.748

H. Chaudhary, H. Chaudhary & A. K. Sharma (2022). Optimized genetic algorithm and extended Diffie Hellman as an effectual approach for DOS-attack detection in cloud. International Journal of Software Engineering and Computer Systems, 8(1), 69-78.

I. Shparlinski. Computational Diffie Hellman problem (2025). In: Encyclopedia of Cryptography, Security and Privacy, 403-407. Cham: Springer Nature Switzerland.

I. Shparlinski (2025). Computational Diffie Hellman problem. In: Encyclopedia of Cryptography, Security and Privacy, 403-407. Cham: Springer Nature Switzerland.

J. Chen & Y. Zhao (2023). Stability Analysis of Worm Propagation Dynamics Based on Quarantine. IEEE Conference on Network Protocols and Cybersecurity, IEEE, 1:1, 27-35. https://doi.org/10.1109/INFCOM.2023.5234704.

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

J. R. Solis-Escobedo, J. R. Gomez-Rodriguez & V.I. Rodriguez-Abdala (2024). Modern Intrusion Detection Systems: A Review and Comparative Analysis. Journal of Software Engineering and Applications, 14(5), 340-350.

J. Smith & R. Anderson (2021). Evaluating the Impact of Dataset Quality on Phishing Detection Algorithms. International Journal of Information Security, 20(4), 321-336.

P. Johnson & Y. Wu (2023). Advanced Feature Extraction Methods for Phishing Email Detection. Journal of Information Systems, 38(3), 267-284.

R. M. McDaniel, R. A. Lewis & S. W. Y. Choi (2021). The Evolution of XHTML: Enhancing Flexibility and Interoperability in Web Development. International Journal of Web Engineering and Technology, 17(2), 105-122.

R. Malik & P. Kumar (2015). Cloud computing security improvement using Diffie Hellman and AES. International Journal of Computer Applications, 118(1), 30-40.

R. Malik & P. Kumar (2023). Cloud computing security improvement using Diffie Hellman and AES. International Journal of Computer Applications, 118(1), 112-119.

R. Sadre, & M. Sperotto (2021). Advances in Intrusion Detection Systems: A Comprehensive Review. International Journal of Information Security, 20(2), 147-169. Available at: https://doi.org/10.1007/s10207-021-00515-6.

S. F. Yousif (2021). Secure voice cryptography based on Diffie-Hellman algorithm. In: IOP Conference Series: Materials Science and Engineering, 1076:1, 121-129. IOP Publishing.

S. Minocha & R. Singh (2022). Phishing Detection Techniques: A Review and Future Directions. Journal of Cybersecurity, 5(2), 112-130.

U. Tariq, I. Ahmed, A.K. Bashir, & K. Shaukat (2023). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), 4117.

V. Kumar & A. Patel (2023). An Analysis of User Behavior Patterns in Phishing Scenarios: Implications for Detection Systems. Computers & Security, 118, 10-22.

V. Singh, P. Pandey, S. Chowhan, S. Hemelatha & Y. D. Deshpande (2024). An Analytical Study of Internet Key Exchange (IKE) Protocol for Wireless Network Security. In: 2nd World Conference on Communication & Computing, 1-5. IEEE.

Y. B. Prastyo, I. W. W. Pradnyana & M. Adrezo (2020). Diffie-Hellman Algorithm for Securing Medical Record Data Encryption keys. In: International Conference on Informatics, Multimedia, Cyber and Information System, 296-300. IEEE.