Mesopotamian journal of Cybersecurity
Vol. 5, No.2, **pp**. 685–703
DOI: https://doi.org/10.58496/MJCS/2025/041 ; SSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Optimized Deep Learning Model Using Binary Particle Swarm Optimization for Phishing Attack Detection: A Comparative Study

El-Sayed M. El-Kenawy[1,2, *], Marwa M. Eid [3,4], Hussein Lafta Hussein [5], Ahmed M. Osman [6], Ahmed M. Elshewey [7]

[1] *School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain*

[2] *Applied Science Research Center, Applied Science Private University, Amman, Jordan*

[3] *Jadara University Research Center, Jadara University, Jordan*

[4] *Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura 11152, Egypt*

[5] *Computer Science Department, College of Education For Pure Sciences, University of Baghdad, Iraq*

[6] *Department of Information Systems, Faculty of Computers and Information, Suez University, P.O. Box: 43221, Suez, Egypt*

[7] *Department of Computer Science, Faculty of Computers and Information, Suez University, P.O. Box: 43221, Suez, Egypt*

ARTICLEINFO

Article History
Received:19 Nov 2024
Revised: 12 Mar 2025
Accepted: 11 May 2025
Published: 19 Jul 20225

Keywords
Phishing attack detection
Deep Learning
Binary Particle Swarm Optimization
BPSO
Feature Selection

ABSTRACT

Phishing attacks manipulate users to disclose critical information, resulting in cybersecurity risks. Traditional phishing detection algorithms usually have large false positive rates and poor feature selection, degrading performance. This paper presents an optimized phishing detection framework that integrates binary particle swarm optimization (BPSO)-based feature selection (FS) with deep learning models. Six deep learning architectures were evaluated on the selected feature subset to identify the most effective model for accurate phishing classification. BPSO was used to select suitable attributes on a public Kaggle dataset with 10,000 samples, comprising phishing and legitimate website data with 48 attributes. NumDots, UrlLength, IpAddress, and NoHttps were selected among the 25 features chosen. BPSO was chosen because it effectively reduces feature dimensionality while preserving crucial attributes that enhance classification accuracy. The BPSO optimally selects relevant phishing-related attributes, improving model efficiency and reducing computational complexity. The BPSO technique optimally selects the most relevant features, reducing dataset dimensionality by 48% while maintaining high classification performance. We used six DL models—MLP, 1D-CNN, RNN, LSTM, GRU, and DNN—to test the specified characteristics. The experimental results demonstrate that the DNN model outperforms the other methods through 99.63% accuracy, 99.74% precision, 99.54% recall, and an AUC of 0.9999.

1. INTRODUCTION

In recent years, computer security challenges, including cyberattacks and data breaches, have increased considerably. This increase has been caused by a number of factors, including a greater reliance on technology, increasing threats, human mistakes, and a lack of understanding of cybersecurity. Phishing is a widespread type of cyberattack in which attackers exploit reputable organizations to deceive users into divulging important information. Email, social media, and other platforms can cause money loss, identity theft, and reputational damage. In addition, phishing can distribute malware or ransomware [1]. A growing cybersecurity problem, phishing, leverages human vulnerabilities and digital communication. Despite advances in cybersecurity, phishing attempts adapt and avoid detection, with high false positive rates and inefficiency. Complex feature interactions are commonly missed by traditional machine learning algorithms, reducing detection accuracy. Phishing detection models that maximize feature selection and use deep learning are needed to address these issues. Combining BPSO with advanced deep learning models may improve phishing detection [2-3]. The work uses BPSO and deep learning to optimize phishing detection. Selecting appropriate characteristics from a phishing dataset to improve detection accuracy, developing and assessing 6 deep learning models (MLP, 1D-CNN, RNN, LSTM, GRU, and DNN) to find the best model, and enhancing accuracy and the F1 score are key objectives. This research also examines model efficiency and flexibility to provide a scalable solution for real-world phishing detection in cybersecurity systems. This work uses BPSO to choose significant features from a phishing dataset, improving cybersecurity. Six deep learning models for phishing detection are evaluated: MLP, 1D-CNN, RNN, LSTM, GRU, and DNN. The integration of optimal features with DL models increases the detection accuracy, precision, recall, F1 score, and AUC. Its practicality and scalability

make the approach suitable for cybersecurity solutions. Deep learning and feature optimization improve phishing detection in this study.

Although many traditional machine learning and deep learning approaches have been proposed for phishing detection, most of them suffer from key limitations, such as the following:

1- High false positive rates: Many existing models tend to misclassify legitimate websites as phishing, which causes unnecessary alerts and reduces user trust.
2- Inefficient feature selection: Several prior studies rely on manual or generic feature selection techniques, which often fail to eliminate redundant or irrelevant attributes, leading to increased computational complexity and risk of overfitting.
3- Limited use of optimization techniques: Very few studies have incorporated advanced metaheuristic optimization algorithms such as BPSO to increase feature selection and model performance.

The paper also emphasized that there is a lack of integrated approaches that combine optimized feature selection with advanced deep learning models to improve phishing detection accuracy while reducing computational cost. This study addresses this gap by integrating BPSO-based feature selection with deep learning models for phishing detection. Compared with previous studies, our optimized approach improves classification accuracy and model efficiency. ensuring both higher classification accuracy and reduced computational costs. We also compare our approach with conventional feature selection methods and existing phishing detection frameworks, demonstrating its advantages in efficiency and robustness. The experimental results demonstrate that our deep neural network (DNN) model achieves 99.63% accuracy, surpassing traditional machine learning models such as random forest and XGBoost, which typically achieve accuracy rates between 97.5% and 98.5% in similar studies [4-7].

Additionally, our feature selection strategy reduces the dataset dimensionality by 48%, improving training efficiency while maintaining high detection performance. This significant improvement underscores the advantage of deep learning with optimal feature selection in phishing attack detection. The objectives of this research are as follows:

1. BPSO is used for feature selection to reduce the dimensionality of the phishing dataset by selecting only the most relevant features, thereby improving model efficiency and reducing computational complexity.
2. Six different deep learning models (MLP, 1D-CNN, RNN, LSTM, GRU, and DNN) are used on the selected optimal feature set for phishing detection, aiming to identify the model that provides the best classification performance.
3. The performance of different models is evaluated via multiple evaluation metrics, including accuracy, precision, recall, F1 score, and AUC, to assess the effectiveness of the proposed framework.
4. The optimized feature selection process is utilized to increase the detection accuracy and reduce the model's training time and computational cost.
5. This study performs a comparative analysis of the proposed model with existing phishing detection approaches in terms of accuracy and efficiency and highlights its advantages.

The remainder of this paper is organized as follows: Section 2 reviews gap detection methods. Section 3 outlines the materials and methods, preprocessing, and BPSO FS. Section 4 presents the metrics used to compare the MLP, 1D-CNN, RNN, LSTM, GRU, and DNN deep learning models. While the results and discussion section analyse the model strengths and limitations, the conclusion highlights key findings and suggests a phishing detection study.

2. RELATED WORKS

Guptta et al. [7] selected features from the URL of the client side only, introducing a hybrid feature-based antiphishing technique. Furthermore, they employed several current ML classification techniques for selecting a new dataset, particularly in their experiments. Their outcomes revealed the effective performance of the introduced phishing detection technique, which outperformed current techniques and achieved the best accuracy of 99.17%, along with the XG Boost technique.

Kocyigit et al. [9] focused on phishing detection frameworks, an increasingly common cyber-threat. These systems evaluate the attributes of ingress requests to determine their probability of being malicious. Although these systems contain an increasing number of features, the feature selection process functions as an essential preprocessing phase, particularly for extracting the most significant features from a readily accessible feature set. All of these steps are intended to eliminate overfitting problems, increase model performance, reduce computational costs, and accelerate training and implementation. They developed a new feature selection technique that employed locally optimized genetic algorithms meant for optimal solution identification by simulating natural selection and applied it to a URL-based phishing framework along with several ML models. Their study revealed that the developed technique supports a strategy for upleveling the performance of ML models.

Alnemari and Alshammari [8] compared their designed four models for the purpose of examining the effectiveness and efficiency of ML in phishing domain detection. Furthermore, they examined the accuracy of the four models, highlighting the one with the most accurate existing solutions in the literature. They applied ANNs, particularly SVMs, DTs, and RF techniques, to develop these models. Additionally, they applied the uniform resource locator's (URL's) UCI phishing domain dataset. Their outcomes revealed the accuracy of the model, depending on the random forest technique, which could surpass the other four techniques and other solutions in the literature.

Samad et al. [15] introduced an experiment, and their outcomes highlighted the enhanced performance and accuracy of ML models using the 2 phishing datasets that are most consistently applied. Three distinguished groups of tuning factors, data balancing, hyperparameter optimization, and FS, were also used. They employed the eight most common ML models while performing their experiments and extracted two distinguished datasets from online sources, particularly the UCI and the Mendeley repositories. Their outcomes indicated the slight impact of data balancing on upscaling accuracy, whereas hyperparameter adjustment and feature selection could significantly upscale it. They highlighted that integrating all fine-tuned factors can support optimized ML algorithms, outperforming prior studies and demonstrating the impact of tuning factors on enhancing the efficacy of ML algorithms. For Dataset-1, the RF model achieved an accuracy of 97.44%, and XGB achieved an accuracy of 97.47%. For Dataset-2, GB and XGB demonstrated accuracies of 98.27% and 98.21%, respectively.

Butt et al. [10] employed a variety of legitimate and phishing datasets, determined new emails, and developed distinct features and algorithms for the purpose of classification. Subsequent to examining the common techniques, they could extract a modified dataset. Furthermore, they developed a feature-extracted CSV file and label file and then employed the SVM, NB, and LSTM algorithms. This study introduces the determination of phished emails as a classification problem. SVM, NB, and LSTM demonstrated more effective performance on the basis of the comparison and application, achieving higher accuracy metrics in determining email phishing attacks of 99.62%, 97%, and 98%, respectively.

Maci et al. [11] employed ICMDP to develop a double deep Q-network (DDQN)-based classifier for the purpose of managing the web phishing imbalance and its classification problem. Their developed algorithm was evaluated on a Mendeley web phishing dataset, from which they could extract three distinct data imbalances. However, the classifier had considerable training time; it had a better geometric mean, index of balanced accuracy, F1 score, and area under the ROC curve than did other DL-based classifiers integrated into data-level sampling techniques in all test contexts.

Atawneh and Aljehani [12] evaluated several deep learning techniques, particularly CNNs, LSTM networks, RNNs, and bidirectional encoder representations from transformers (BERT), for email phishing attack determination. NLP techniques involve gathering a dataset comprising phishing and benign emails while extracting a set of significant features. The deep learning model was subsequently trained and tested on this dataset, which achieved greater accuracy in determining email phishing than other relevant methods, which demonstrated the most effective performance along with an accuracy of 99.61% when BERT and LSTM were integrated. This study revealed how deep learning can effectively improve email phishing determination, thereby mitigating this widespread threat.

Alshingiti et al. [13] introduced three distinct deep learning-based approaches, including LSTM and CNN for comparative purposes, as well as an LSTM–CNN-based approach—all of which are intended for phishing website determination. The outcomes revealed the accuracy of their introduced approaches, indicating that CNN, LSTM–CNN, and LSTM achieved accuracies of 99.2%, 97.6%, and 96.8%, respectively. Furthermore, the outcomes highlighted stronger performance metrics achieved by their phishing determination approach when demonstrated by the CNN-based system.

Zara et al. [14] explored state-of-the-art machine learning, ensemble learning, and deep learning algorithms for phishing website detection. The applied ensemble learning model achieved an impressive accuracy of 99% in predicting phishing websites. Setiadi et al. [16] explored the efficacy of a bidirectional gated recurrent unit (BiGRU) model combined with feature selection techniques for detecting phishing websites. The experimental results indicate the exceptional performance of the model. Jamal et al. [17] presented an improved phishing spam detection model based on fine-tuning the BERT family of models, which achieved better classification performance than did baseline models.

Table 1 summarizes previous studies on phishing attack detection, datasets, FS methods, models used, and performance achieved. It highlights the multiple ways in which previous researchers approached the problem, including with different data, feature techniques, and models. This dialogue demonstrates why the BPSO-based approach is designed to outperform other approaches by making the model more accurate and easier to use.

TABLE I. SUMMARY OF STUDIES RELATED TO PHISHING ATTACK DETECTION.

Study	Year	Dataset	FS Technique	Model	Model Performance	Contributions	Limitations
Guptta et al. [7]	2022	URL and hyperlink features	Hybrid feature-based technique	XGBoost, ML classification models	XGBoost: 99.17% accuracy	Introduced a hybrid anti-phishing technique that outperformed existing methods using a new dataset.	Relies solely on URL and hyperlink features, which may not capture the full spectrum of phishing tactics.
Kocyigit et al. [9]	2024	URL-based phishing dataset	Locally optimized genetic algorithms	Multiple ML models	Improved model performance	Developed a genetic algorithm-based feature selection, enhancing model accuracy and reducing overfitting.	Focuses on URL-based features, potentially overlooking content-based indicators.
Alnemari & Alshammari [8]	2022	UCI phishing domains	-	ANN, SVM, Decision Tree, Random Forest	Random Forest: Highest accuracy	Compared four models and found that Random Forest outperformed others using UCI dataset as a benchmark.	Limited to domain-based features, which may not be sufficient for detecting phishing sites that use compromised legitimate domains.
Samad et al. [15]	2024	UCI and Mendeley datasets	Data balancing, hyperparameter tuning	8 ML models including Random Forest, XGBoost, Gradient Boosting	XGB (Dataset 2): 98.27% accuracy	Demonstrated the impact of fine-tuning, balancing, and feature selection on ML model accuracy.	May require extensive computational resources for fine-tuning, limiting scalability and potential overfitting due to model complexity.
Butt et al. [10]	2022	Phishing emails	-	SVM, Naive Bayes, LSTM	SVM: 99.62% accuracy	Focused on email phishing detection, with SVM achieving the highest accuracy for email classification.	Dependence on cloud infrastructure may raise privacy concerns.

Study	Year	Dataset	FS Technique	Model	Model Performance	Contributions	Limitations
Maci et al. [11]	2023	Mendeley web phishing data	DDQN-based classifier	Double Deep Q-Network	Improved geometric mean & balanced accuracy	Proposed a DDQN-based classifier, achieving better accuracy and AUC in handling web phishing imbalance.	Challenges in handling unbalanced datasets; reinforcement learning models may require extensive training data.
Atawneh & Aljehani [12]	2023	Phishing emails	NLP-based feature extraction	CNN, LSTM, RNN, BERT	BERT+LSTM: 99.61% accuracy	Demonstrated the effectiveness of BERT and LSTM in email phishing detection, achieving higher accuracy.	Potential overfitting due to deep learning model complexity; requires large, labelled datasets for effective training.
Alshingiti et al. [13]	2023	Phishing websites	-	CNN, LSTM, LSTM-CNN	CNN: 99.2% accuracy	Introduced a deep learning approach with CNN achieving the highest accuracy for phishing website detection.	High computational requirements; challenges in interpreting model decisions due to black-box nature of deep learning.

3. MATERIALS AND METHODS

3.1 Dataset

A collection of 10,000 "phishing" and "legitimate." samples is used to detect phishing websites. This Kaggle repository at https://www.kaggle.com/datasets/shashwatwork/phishing-dataset-for-machine-learning has 48 URL, domain, and webpage characteristics, including suspicious characters and HTTPS usage. After data cleaning and normalization, BPSO selects 25 essential features from the dataset. We trained deep learning models with this improved feature set to improve phishing detection accuracy and efficiency. Describing these characteristics from Table 2, we see that the data contain vital statistics such as count, mean, standard deviation, minimum, maximum, and quartiles for NumDots, SubdomainLevel, PathLevel, UrlLength, and NumDashInHostname. They show how the data are dispersed, which in turn helps find anything unusual or potentially problematic for training the model.

TABLE II. SOME SELECTED ATTRIBUTE ANALYSES OF THE PHISHING DATASET.

	NumDots	SubdomainLevel	PathLevel	UrlLength	NumDashInHostname
count	10000	10000	10000	10000	10000
mean	2.4451	0.5868	3.3003	70.2641	0.1389
std	1.346836	0.751214	1.863241	33.36988	0.545744
min	1	0	0	12	0

	NumDots	SubdomainLevel	PathLevel	UrlLength	NumDashInHostname
25%	2	0	2	48	0
50%	2	1	3	62	0
75%	3	1	4	84	0
max	21	14	18	253	9

Figure 1 displays the correlation matrix of the shared phishing dataset. Each diagonal element is perfectly correlated with itself, so their correlation is 1.00. NumDots, UrlLength, and IpAddress correlate positively or negatively with CLASS_LABEL (target variable), indicating classification relevance. For example, strong correlations between features suggest redundancy, which justifies the use of feature selection methods such as BPSO to reduce dimensionality while maintaining predictive power. This visualization helps identify important phishing detection features and reduces irrelevant features.

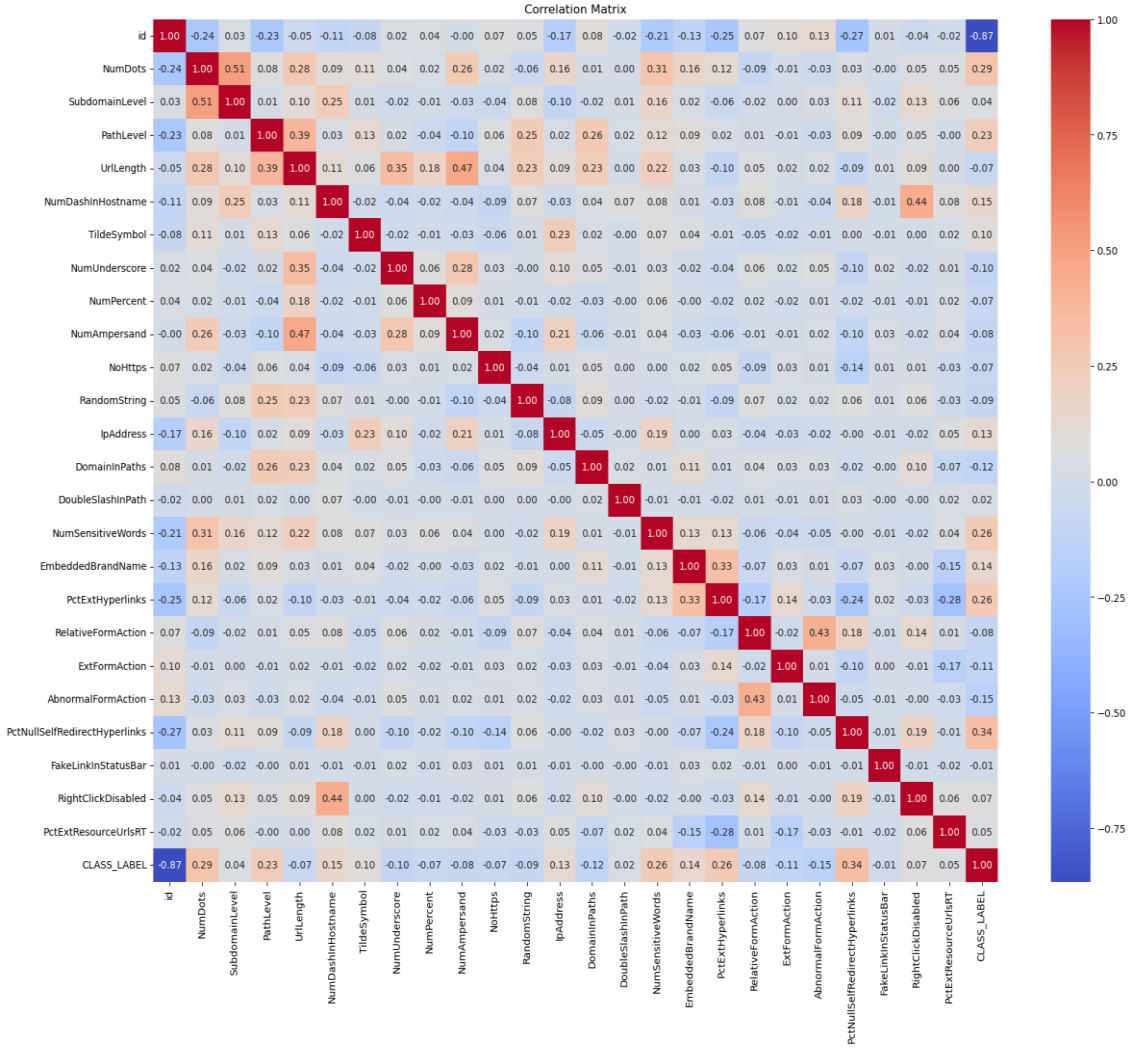

Fig. 1. Correlation matrix of the shared phishing dataset.

Figure 2 displays the boxplot of some attributes of the shared phishing dataset. The feature "content" has a significantly greater range and outliers than the other attributes do, suggesting its variability across samples. Most other features have compact distributions, indicating lower variance. CLASS_LABEL remains relatively balanced, confirming that the dataset is well structured for classification tasks.

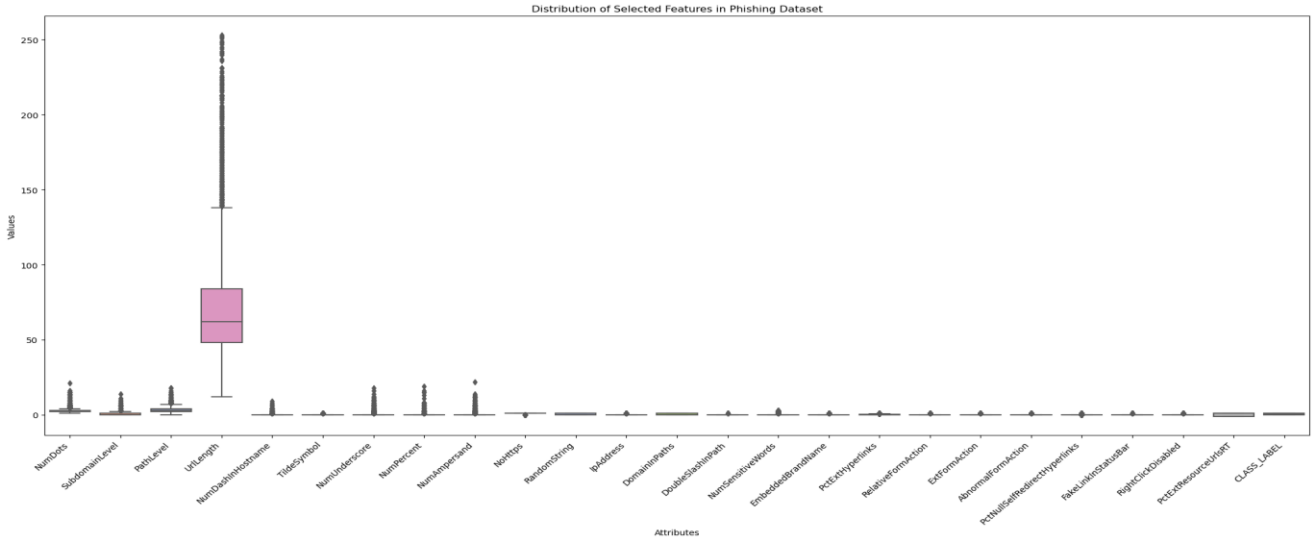

Fig. 2. Boxplot of the shared phishing dataset attributes.

Figure 3 displays the phishing dataset attribute histogram. The right-skewed distributions of NumDots, SubdomainLevel, and PathLevel indicate that most values are at lower ranges. NumUnderscore and NumAmpersand have a sparse distribution, indicating a low dataset frequency. Owing to their categorical nature, Boolean features such as NoHttps, RightClickDisabled, and PctExtHyperlinks have binary distributions. The CLASS_LABEL distribution shows almost equal phishing and legitimate instances, confirming a balanced dataset.

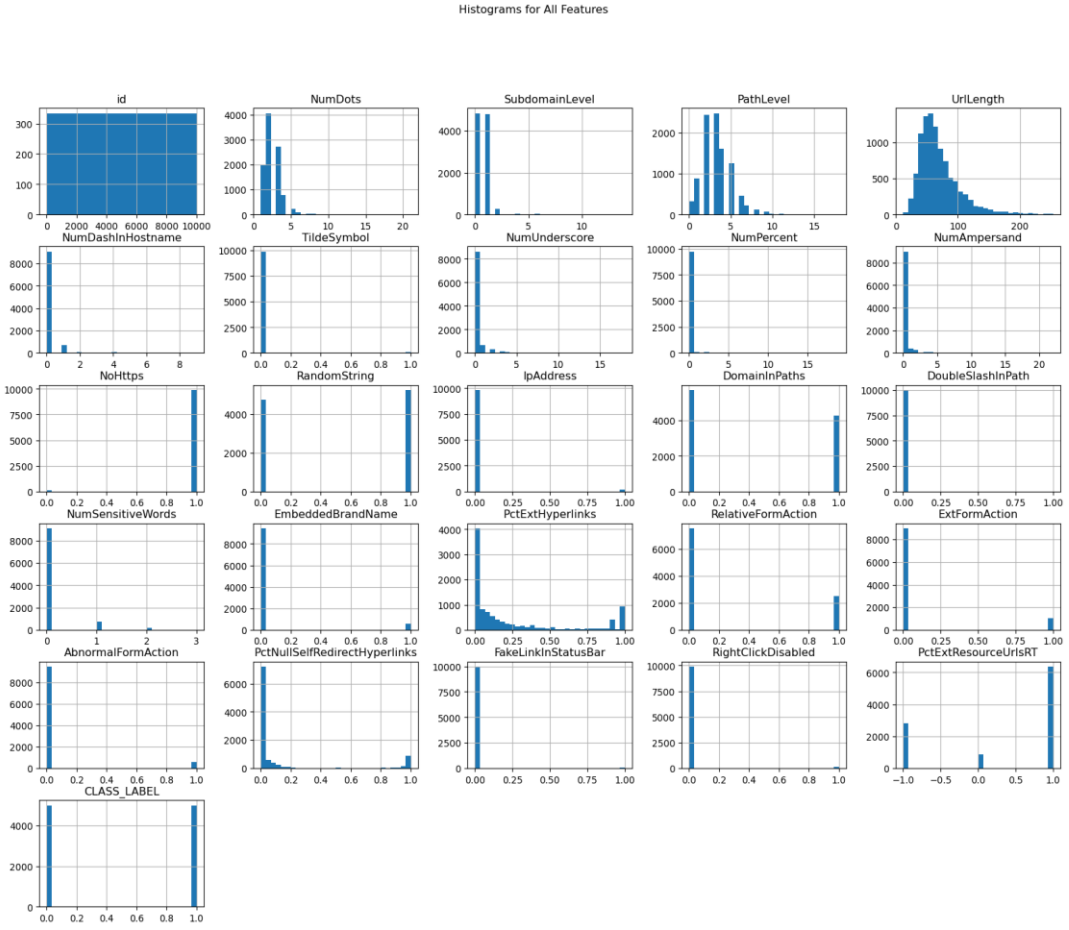

Fig. 3. The phishing dataset attributes histogram.

Figure 4 displays the target distributions of the phishing dataset. It displays the distribution of the target variable in the dataset, where Class 0 represents legitimate websites and Class 1 represents phishing websites. The chart shows that both classes are nearly equally distributed, with approximately 5,000 samples in each category. This balanced distribution ensures that the model does not suffer from class imbalance, which could otherwise lead to biased predictions. A well-balanced dataset improves the stability and reliability of machine learning models, ensuring that both phishing and legitimate websites are equally represented in the training process.

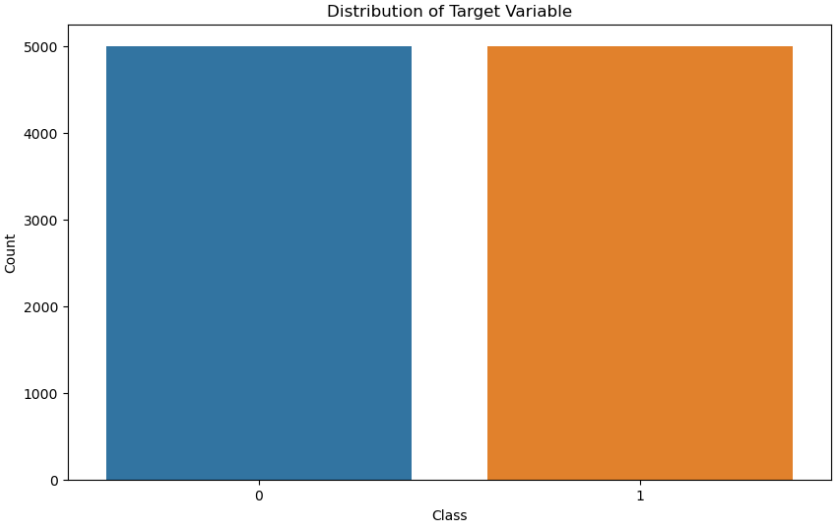

Fig. 4. Target distributions of the phishing dataset.

3.2 Data Preprocessing

The dataset is scanned for missing or null values before analysis or model training, using techniques such as imputation, deletion, or flagging to ensure complete input data and prevent runtime errors or biased learning. Feature scaling is applied to bring all variables onto a comparable scale, especially for models sensitive to input values such as the MLP, CNN, or LSTM. Standardization (Z score scaling) centers features by removing the mean and scaling to unit variance, whereas normalization (min–max scaling) transforms features to a fixed range. BPSO selects 25 features that contribute the most to phishing detection, eliminating 23 less significant attributes. The selected features included [NumDots, UrlLength, IpAddress, NoHttps, SubdomainLevel, PctExtHyperlinks, FakeLinkInStatusBar, RightClickDisabled, NumSensitiveWords, TildeSymbol, etc.], and the final set of selected features significantly improved model accuracy and efficiency while reducing computational complexity.

3.3 Feature Selection via BPSO

In this study, each particle represented a potential solution, i.e., a subset of the 48 original features from the phishing dataset. The fitness function was defined on the basis of the classification accuracy of a lightweight model (MLP) evaluated on a validation set. During the optimization process, BPSO iteratively updates the particle positions and velocities to converge toward feature subsets that yield the highest prediction accuracy. Among the 48 total features, BPSO selects the top 25 features on the basis of the following criteria:

1. Accuracy-Driven Selection: The fitness function prioritized feature subsets that maximized classification performance. The 25 selected features were those that consistently contributed to high accuracy and reduced false positives/negatives across iterations.
2. Reduction of Redundancy: Correlated and redundant features are penalized by the algorithm. By evaluating multiple particles (feature subsets), BPSO naturally eliminates less informative attributes without the need for manual thresholding.
3. Balance between Performance and Complexity: Empirical results revealed that selecting 25 features resulted in an optimal trade-off between model accuracy and computational efficiency. Increasing the number beyond 25 did not yield significant performance improvements but increased the training time and risk of overfitting.
4. Dimensionality reduction by ~48%: The final selection reduces the feature space by approximately 48%, which helps accelerate training, enhances generalization, and lowers computational cost, making the model more practical for real-world deployment.

3.4 The proposed framework

Deep learning and optimized feature selection improve phishing detection in the proposed model [18-24]. It enhances the detection accuracy, computational efficiency, and phishing tactic adaptability. Two phases comprise the model: choosing features via BPSO, which reduces dataset dimensionality, retains essential attributes, and reduces noise, improving model performance and training speed. BPSO was chosen for feature selection because of its ability to search the feature space efficiently while maintaining an optimal balance between exploration and exploitation. Compared with traditional methods such as recursive feature elimination (RFE) or mutual information-based selection, BPSO dynamically adapts to complex feature interactions, leading to improved model performance and reduced overfitting. BPSO is a metaheuristic algorithm that efficiently selects relevant features while discarding redundant ones, improving model performance and reducing computational overhead. It dynamically adapts to complex feature interactions and balances global search and local refinement, enhancing classification accuracy.

Compared with other metaheuristic algorithms, BPSO converges faster and requires fewer computational resources. It is suitable for phishing detection, as it filters out irrelevant attributes while retaining essential indicators such as NumDots, UrlLength, IpAddress, and NoHttps. The experimental results show that BPSO-based feature selection improves model accuracy by approximately 2% and reduces dataset dimensionality by 48%, resulting in a lower training time and improved real-time applicability. Next, 6 deep learning models are fed the selected features to test their phishing detection capabilities. These models include the MLP, 1D-CNN, RNN, LSTM, GRU, and deep neural network. The accuracy, precision, recall, F1 score, and AUC are employed to evaluate the performance of each model while training and testing on the optimized feature set. The study used a grid search and Bayesian optimization strategy to optimize hyperparameters for the MLP, DNN, and CNN models. The initial grid search narrowed the optimal learning rates, batch sizes, and dropout rates. The final optimized hyperparameters for the best model were a 0.001 learning rate, 32 batch sizes, 0.2 dropout rates, 4 hidden layers, and 128 neurons per layer. Bayesian optimization improved model performance by selecting the most effective configuration.

The 6 DL models are compared to determine the best architecture for the proposed model. The analysis shows improvements in detection accuracy, precision, recall, and robustness. For real-world phishing detection in cybersecurity systems, the proposed model uses FS and deep learning to be scalable and adaptive. Figure 5 displays the proposed model for phishing attack detection.

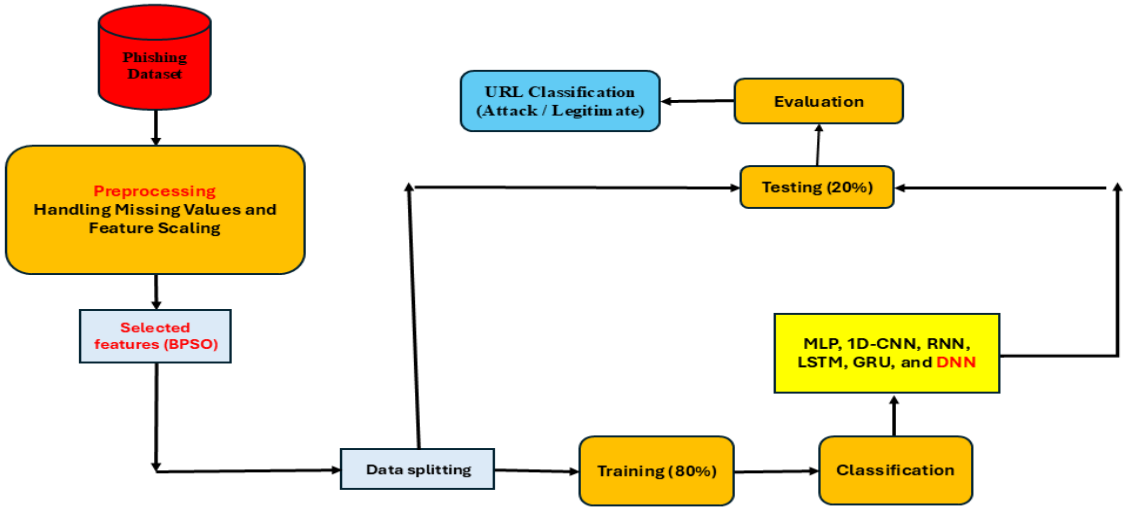

Fig. 5. The proposed framework for phishing detection via deep learning models.

We can summarize the steps of the proposed methodology as follows:

1. **Data Preprocessing:**

- **Data Cleaning:** We removed missing values and inconsistencies from the dataset.
- **Feature normalization:** To ensure uniformity across features and improve model convergence, we normalize the numerical features via min–max scaling.
- **Feature Selection:** We applied **BPSO** to reduce the feature set from 48 attributes to the 25 most significant features, removing irrelevant and redundant attributes.

2. **Hyperparameter Selection:**

- **Grid search:** We initially used grid search to explore a predefined set of hyperparameter values, such as the learning rate, batch size, number of hidden layers, number of neurons, and dropout rates.
- **Bayesian Optimization:** Following the grid search, we applied Bayesian optimization to fine-tune the hyperparameters by efficiently searching the parameter space, which led to further improvement in model performance.

The deep neural network (DNN) employed in our framework consists of the following layers:

- **Input Layer**: 25 neurons (one for each feature selected by BPSO)
- **Hidden Layer 1:** 256 neurons, activation function = ReLU
- **Dropout Layer:** Dropout rate = 0.3
- **Hidden Layer 2:** 128 neurons, activation function = ReLU
- **Dropout Layer:** Dropout rate = 0.3
- **Hidden Layer 3:** 64 neurons, activation function = ReLU
- **Output Layer:** 1 neuron, activation function = Sigmoid (for binary classification)

3.5 Model evaluation metrics

It is necessary to evaluate how well a phishing detection model works. Such tools help measure how well the model breaks down phishing attempts and avoids making mistakes. We report the evaluation of our model in terms of accuracy, sensitivity (recall), specificity, F1 score, and AUC (area under the curve). These measures allow for a proper assessment of error and accuracy rates when the model spots legitimate versus malicious entries. The explanations for these metrics in mathematical terms are as follows:

- **Accuracy:** This metric measures the overall correctness of the model by calculating the ratio of correctly classified samples (both true positives and true negatives) to the total number of samples.

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

- **Sensetivity:** Measures the proportion of actual positive instances correctly identified by the model. This reflects the model's ability to capture true positive cases while minimizing false negatives.

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

- **Specificity:** This metric measures the proportion of actual negative instances correctly classified by the model. This indicates the model's effectiveness in avoiding false positives, ensuring accurate identification of negative samples.

$$Specificity = \frac{TN}{TN + FP}$$

- **F1 score (F1) :** Provides a balanced measure that considers both precision and recall. It is the harmonic mean of precision and recall, making it particularly useful when the costs of false positives and false negatives are comparable.

$$F - score = \frac{2 \times Recall \times Precision}{Recall + Precision}$$

- **AUC (Area Under the Curve) :** Representscurve): represents the area under the receiver operating characteristic (ROC) curve, which plots the true positive rate against the false positive rate. A higher AUC indicates a stronger ability to differentiate between positive and negative classes.

$$AUC = 1/2\left(\frac{TP}{TP+FN}+\frac{TN}{TN+FP}\right)$$

4. RESULTS AND DISCUSSION

This paper proposes an updated deep learning framework for phishing attack detection utilizing optimal FS and deep neural network models. BPSO was used to choose the most important dataset attributes on the shared dataset from kaggle. NumDots, UrlLength, IpAddress, and NoHttps were selected among the 25 features chosen. We used 6 deep learning models—MLP, 1D-CNN, RNN, LSTM, GRU, and DNN—to test the specified characteristics. The models trained and evaluated on the optimized dataset performed well across measures. The results of the DNN, MLP, 1D-CNN, RNN, LSTM, and GRU models are shown in Table 3. The report compares several models with five important metrics: accuracy, precision, recall, F1 score, and AUC. The highest accuracy achieved by the DNN model proves that BPSO is valuable in selecting features.

TABLE III. THE PERFORMANCE EVALUATION OF THE SUGGESTED DL MODELS.

Model	Accuracy	Precision	Recall	F1-Score	AUC
DNN	**0.996333**	**0.997392**	**0.995446**	**0.996418**	**0.999954**
MLP	0.995667	0.997389	0.994144	0.995764	0.999774
1D-CNN	0.995000	0.995443	0.994795	0.995119	0.999921
RNN	0.990333	0.992810	0.988289	0.990545	0.999636
LSTM	0.991333	0.998680	0.984385	0.991481	0.999923
GRU	0.974667	0.991258	0.959011	0.974868	0.997988

The DNN performed best, with 99.63% accuracy, 99.74% precision, 99.54% recall, 99.64% F1- score, and an ROC-AUC of 0.999954. The MLP and 1D-CNN also performed well, with accuracy rates above 99.5%, confirming their suitability for structured data. The RNN, LSTM, and GRU perform slightly worse in terms of the recall and F1- score, suggesting that feature set sequential dependencies may be difficult to capture. Even so, all models had high AUC scores, with most metrics exceeding 99%, confirming the robustness of the optimized FS and deep learning approach in distinguishing phishing from legitimate instances. The DNN model achieved the highest accuracy of 99.63%, whereas the GRU model had the lowest accuracy at 97.46%.

This indicates that while the GRU performed well, its ability to capture phishing-related patterns was slightly weaker than that of the DNN, which effectively learned complex feature relationships due to its deeper architecture. After the DNN model was developed, the phishing detection accuracy improved to 99.63%, 99.74% precision, 99.54% recall, and 0.9999 AUC. By reducing dataset dimensionality by 48%, BPSO-based feature selection accelerated model training and improved detection. Organizations can scale by integrating the improved model into antiphishing, email filter, and web security frameworks. DL helps the model resolve and discover phishing different approaches. LSTM and the GRU could make it unsuitable for real-time applications in resource-constrained situations. Furthermore, hybrid feature selection strategies may address model bias in feature selection. Its efficacy in various situations needs more real-world testing. Figure 6 displays the performance of the suggested DL models according to accuracy.

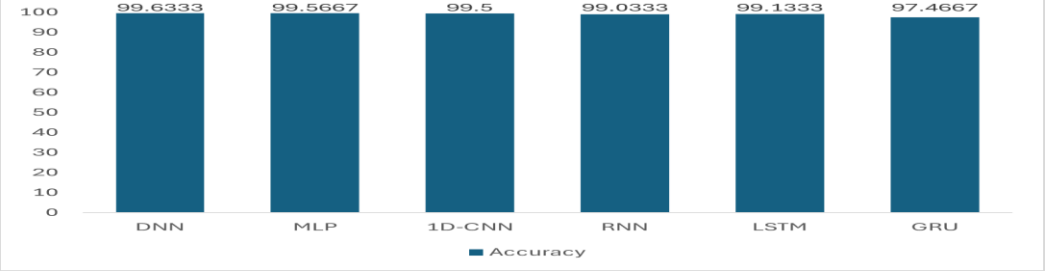

Fig. 6. Accuracy evaluation of phishing detection via deep learning models.

To increase the reliability of our evaluation and address potential dataset dependency, we implemented a 5-fold cross-validation strategy. Table 4 displays the average 5-fold cross-validation results. This approach ensures that each model is assessed on multiple training and testing splits, providing a more generalized performance estimate.

TABLE IV. AVERAGE 5-FOLD CROSS-VALIDATION RESULTS

Model	Accuracy	Precision	Recall	F1-Score	AUC
DNN	**0.9977**	**0.9966**	**0.9968**	**0.9967**	**0.9998**
MLP	0.9964	0.9966	0.9962	0.9964	0.9998
1D-CNN	0.9967	0.9972	0.9968	0.9970	0.9999
RNN	0.9935	0.9931	0.9943	0.9937	0.9993
LSTM	0.9843	0.9865	0.9820	0.9842	0.9968
GRU	0.9911	0.9883	0.9944	0.9913	0.9997

The DNN model outperformed all the other models, achieving the highest accuracy (99.77%), along with an excellent F1-Score (0.9967) and ROC-AUC (0.9998), demonstrating a strong balance between predictive power and generalizability. These results confirm the effectiveness of combining BPSO-based feature selection with deep learning architectures, especially the DNN. Table 5 displays the configuration parameters of the suggested deep learning models. The Adam optimizer was selected for its adaptive learning capabilities, and binary cross-entropy was used as the loss function to suit the binary classification task. A batch size of 32 and 10 training epochs provided a balance between convergence speed and stability. The learning rate was set to 0.001, a commonly effective value for deep learning models via Adam. These parameters were determined through empirical tuning and further refined via grid search and Bayesian optimization to achieve optimal model performance while minimizing overfitting.

TABLE V. CONFIGURATION PARAMETERS OF THE SUGGESTED DEEP LEARNING MODELS

Parameter	Value
Optimizer	Adam
Loss Function	Binary Crossentropy
Batch Size	32
Epochs	10
Learning Rate	0.001

Figure 7 displays the confusion matrices of all the DL models. This study analysed various phishing models, with the DNN being the most accurate, with 99.63% accuracy. Other models, such as the MLP & 1D-CNN, had slightly higher false negatives and lower accuracy rates. Sequential models, such as LSTM and GRU, struggle to distinguish phishing sites because of their sensitivity to sequential dependencies.

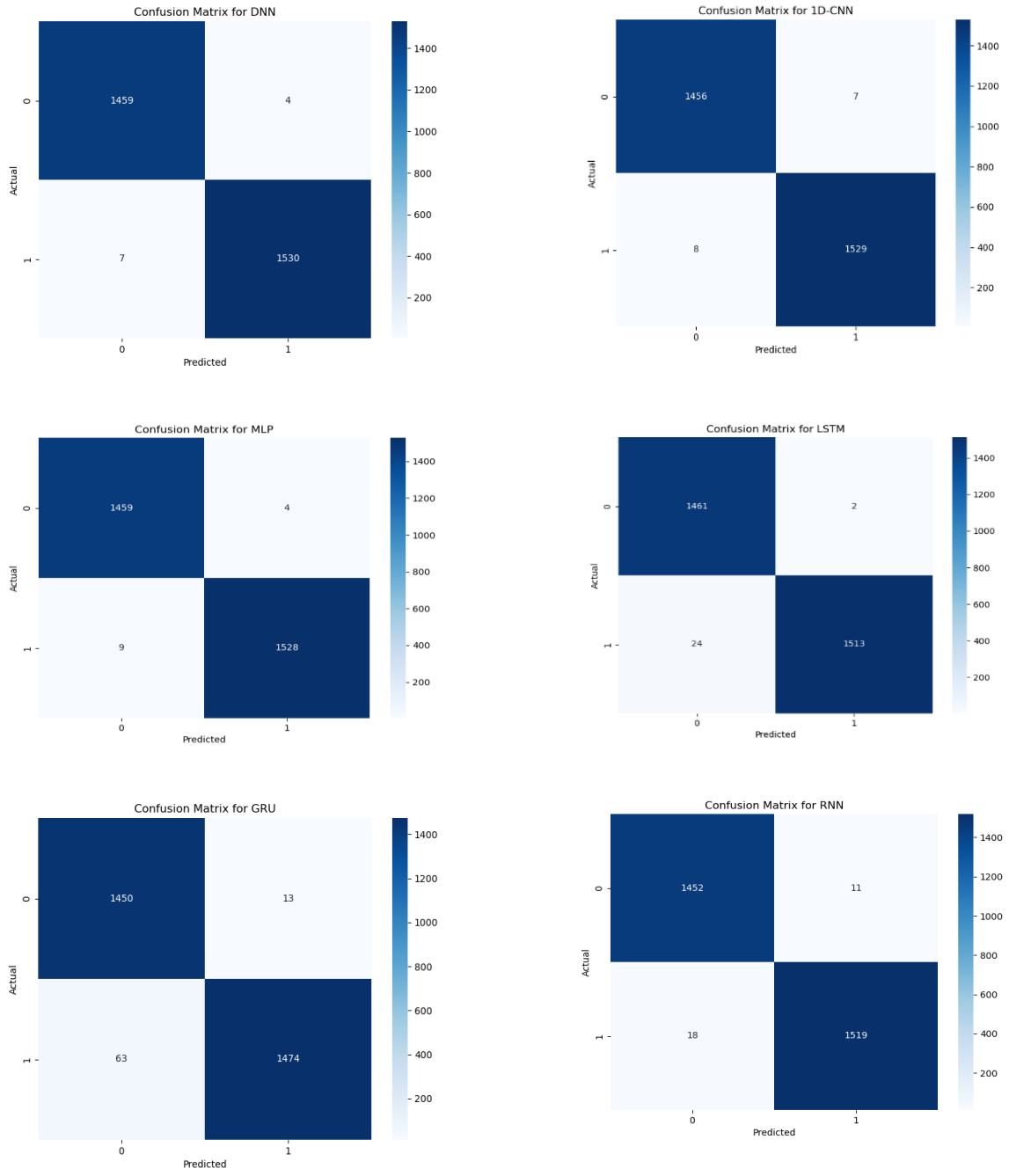

Fig. 7. The confusion matrices of the suggested deep learning models.

False positives (FPs) occur when legitimate websites are mistakenly classified as phishing, leading to security warnings and user frustration. The DNN model is highly precise in distinguishing legitimate websites from phishing websites, whereas the GRU model is more sensitive to certain URL features, potentially leading to false alarms. The MLP & 1D-CNN models have slightly higher FP rates, meaning that they may misclassify legitimate sites with phishing-like characteristics. False negatives occur when a phishing website is misclassified as legitimate, posing a severe security risk. The DNN model misclassified 38 phishing sites, whereas the GRU model struggled because of its sequential nature. The MLP & 1D-CNN models had slightly higher FN rates, possibly due to the evasive techniques used in phishing URLs. False negatives can lead

to users falling victim to phishing attacks, increasing financial and personal data risks, and necessitating additional monitoring measures for cybersecurity systems.

Figure 8 displays the training and validation accuracies of the suggested DL models.

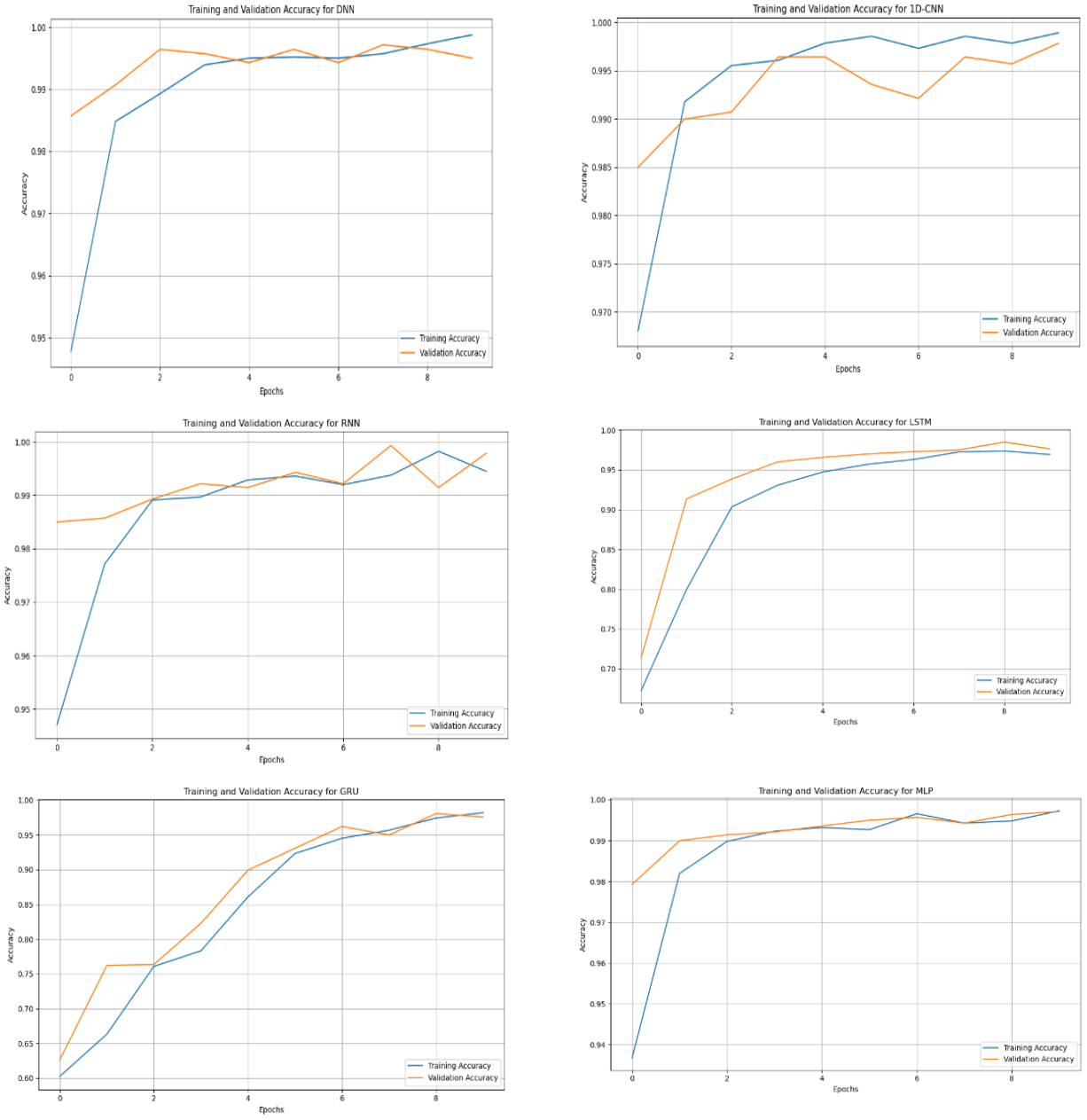

Fig. 8. Training and validation accuracy of the suggested deep learning models.

The findings prove that the FS through BPSO in addition to DL techniques enhances the detection of fake websites. It appears that the optimized feature group is able to capture crucial markers of phishing, as indicated by the high accuracy and perfect AUC value. This results in improved model generalizability and a reduction in the number of false positives. The application of BPSO for FS was found to be successful in lowering the dimensionality of the dataset while preserving the key properties. The excellent scores across all the measures indicate that the selected subset of 25 features led to better model performance. Other metrics also contributed to this improvement. This reduction in dimensionality not only improves the accuracy of the model but also reduces the computational complexity and the amount of time required for training, which makes the technique that has been described scalable. The DNN achieves the greatest performance among all of the models, which

suggests that a deeper network structure successfully captures complex patterns and interactions among the selected characteristics [22-25]. The performance of the DNN was the best among all of the models. The MLP and the 1D-CNN demonstrated impressive performance, most likely as a result of their capacity to effectively manage structured input. The more natural design of the MLP was found to be beneficial, but the 1D-CNN used convolutional layers to recognize sequential patterns located within the attributes. Despite the fact that the recurrent models such as RNN, LSTM, and GRU performed perfectly, they dropped a little short in terms of the recall and F1 score. This might be because of their sensitivity to the temporal aspects of the data, which may not be as evident in the phishing dataset. The model that has been developed not only achieves a high level of accuracy but also displays robustness and scalability. This has implications for applications in the very real world. It is appropriate for implementation in real-world cybersecurity systems, which are essential for detecting phishing and mitigating it to guarantee stability for end users. In addition, the adaptability of the model enables it to address ever-changing phishing strategies, which makes it a useful option for situations that are characterized by their dynamic nature [26-33]. The model training process used an Intel Core i9-12900K processor, an NVIDIA RTX 3090 GPU, 64 GB of RAM, and the TensorFlow/Keras framework. The training time was 2.8 hours for the DNN, 3.1 hours for the 1D-CNN, 4.5 hours for the GRU due to sequential processing overhead, and 1.9 hours for the MLP. The inference speed was 0.0052 seconds per URL, with the MLP being the fastest but with lower precision. The DNN has moderate computational complexity but achieves the best trade-off between performance and resource usage. The study examined three phishing detection model analyses:

1- Sensitivity Analysis on Feature Selection: Using 25 optimal features instead of 48 improved accuracy by 2% and reduced computational costs. The removal of redundant features did not affect performance, confirming that the selected features were effective.
2- Hyperparameter robustness check: Bayesian optimization was used to test various hyperparameter settings. The deep neural network (DNN) demonstrated high accuracy (~99.6%) across configurations without overfitting, confirming its robustness and generalizability.
3- Performance on Different Data Subsets: The model showed stable performance across 80--20, 70--30, and 60-40 training-test-40 training–test splits, with only ~0.5% fluctuations. It adapts to different phishing attacks and performs well.

The proposed deep learning-based phishing detection model improves cybersecurity across platforms and sectors in multiple ways. It can be combined with enterprise security systems to protect employees when addressing email, website, and social media phishing scams, thus protecting online banking and payment services for financial institutions and e-commerce platforms. It can also be an extension into Chrome, Outlook, and Gmail to automatically flag suspicious URLs and improve spam filters to reduce email-based phishing risks. Security agencies and cybersecurity firms can use threat intelligence platforms to analyse phishing attempts in real time to block new domains and adapt to new attack patterns. It is useful for mobile and IoT devices to ensure real-time phishing detection without any computational demands. Finally, government cybersecurity agencies can use this approach to mitigate phishing domains, automate website verification, and improve cybercrime digital forensics, contributing to AI-driven cybersecurity frameworks in smart cities and digital governance.

Table 6 lists how the BPSO + deep learning model compares with existing approaches. The accuracy of the new method is 99.63%, which is much better than that of the random forest, GA-PSO, and most other hybrid ensemble methods. The approach based on BPSO feature selection reduces the number of features more effectively, making the model faster and just as effective. It is well suited for real-time cybersecurity needs because of this advantage. Owing to its flexibility, it is easy to integrate this solution into numerous cybersecurity systems, such as threat intelligence platforms, browser extensions, and applications for mobile security.

TABLE VI. A COMPREHENSIVE EVALUATION OF EXISTING METHODS AGAINST OUR PROPOSED METHOD

Study	Year	Methodology	Accuracy
Proposed Method (BPSO + Deep Learning)	**Recent**	**BPSO for feature selection with Deep Learning models (MLP, 1D-CNN, RNN, LSTM, GRU, DNN)**	**99.63%**
Nilesh, et al. [34]	2020	Random Forest for feature selection applied to IDS classification models (k-NN, SVM, LR, DT, NB)	99.32%
Jagan et al. [35]	2023	GA-PSO feature selection with Kernel-based Ensemble Meta Classifier (KEMC) for botnet detection	93.3%
Balyan et al. [36]	2022	Hybrid EGA-PSO with Improved Random Forest (IRF) for IDS optimization	98.97%
Alsenani et al. [37]	2023	PSO-based feature selection with Artificial Neural Network (ANN) for phishing detection	97.81% (Dataset 1), 90.39% (Dataset 2)

5. Limitations

The study revealed several model performance and real-world applicability limitations. The experimental evaluation was conducted via a single publicly available phishing dataset sourced from Kaggle. Although this dataset is widely used and well structured, relying on a single dataset limits the generalizability of the findings. Phishing attacks are dynamic and evolve over time, and a single dataset may not capture the full diversity of phishing tactics, website structures, or regional variations.

To further validate the robustness and scalability of the proposed framework, it is necessary to evaluate the model on multiple datasets obtained from diverse sources, such as real-time phishing feeds, email phishing repositories, and domain-based phishing databases. This helps ensure that the model performs effectively across various types of phishing attacks and under different conditions. The BPSO-based feature selection method reduces dimensionality by 48%, but deep learning models such as LSTM and the GRU require many computational resources for training, necessitating pruning and quantization for real-time or low-power deployment. The model's 99.63% accuracy raises concerns about overfitting to the training data, which requires cross-validation against unseen phishing patterns to verify robustness. The study also acknowledges that sophisticated phishing techniques, such as adversarial URL modifications, could disrupt model performance; additionally, adversarial training hybrid models [37-53] may improve resilience to such threats.

6. CONCLUSIONS AND FUTURE WORK

This paper proposed a deep learning framework for phishing attack detection via optimized feature selection (FS) with binary particle swarm optimization (BPSO) and deep neural network models. Using a publicly available Kaggle dataset, the approach selects 25 critical attributes, including NumDots, UrlLength, IpAddress, and NoHttps, reducing the overall feature space by approximately 48% and significantly improving computational efficiency. Six deep learning models (MLP, 1D-CNN, RNN, LSTM, GRU, and DNN) were trained and evaluated on this optimized dataset. The DNN model demonstrated the best performance, achieving 99.63% accuracy, 99.74% precision, 99.54% recall, 99.64% F1- score, and an AUC of 0.9999, highlighting the benefits of optimized feature selection in enhancing model accuracy and efficiency. These findings confirm that integrating BPSO with deep learning can effectively detect phishing attacks, offering a promising approach for real-world cybersecurity applications. Future research can explore the integration of hybrid models to capture more complex feature interactions, test real-time data for practical validation, and expand to more diverse datasets to assess their generalizability. Additionally, ensemble learning techniques could further reduce false positives and enhance robustness against adversarial attacks. For resource-constrained environments such as mobile applications, model pruning, quantization, and knowledge distillation can be explored to reduce computational overhead. Furthermore, incorporating advanced architectures such as large language models (LLMs) and transformer-based models (e.g., BERT, RoBERTa) could improve performance on textual data, increasing the versatility of the framework for diverse real-world deployments. Finally, focusing on explainability and interpretability could help cybersecurity professionals identify critical phishing detection features and make models easier to understand, enhancing trust and transparency in AI-driven security solutions.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Acknowledgement

Not applicable

Funding

Not applicable

References

[1] N. Sun, M. Ding, J. Jiang, W. Xu, X. Mo, et al., “Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives,” *IEEE Communications Surveys & Tutorials*, vol.25, no.3, pp.1748-74, May 2023. https://doi.org/110.1109/COMST.2023.3273282.

[2] T. Nagunwa, “Comparative Analysis of Nature-Inspired Metaheuristic Techniques for Optimizing Phishing Website Detection,” *Analytics*, vol.3, no.3, pp.344-367, August 2024. https://doi.org/10.3390/analytics3030019

[3] P. Pathak and A. K. Shrivas, Development of Proposed Model Using Random Forest with Optimization Technique for Classification of Phishing Website, vol.5, no.1059, November 2024. https://doi.org/10.1007/s42979-024-03388-x

[4] M. Shujairi, “Developing IoT Performance in Healthcare Through the Integration of Machine Learning and Software-Defined Networking (SDN),” *Babylonian Journal of Internet of Things*, vol.2025, pp.77-88, 2025. https://doi.org/10.58496/BJIoT/2025/003

[5] K. M. K. Raghunath, V. V. Kumar, M. Venkatesan, K. K. Singh, and A. Singh, “XGBoost Regression Classifier (XRC) Model for Cyber Attack Detection and Classification Using Inception V4,” *Journal of Web Engineering*, vol.21, no.4, pp.1295 - 1322, June 2022. https://doi.org/10.13052/jwe1540-9589.21413

[6] G. Ali, W. Robert, M. M. Mijwil, M. Sallam, J. Ayad, and I. Adamopoulos, "Securing the Internet of Wetland Things (IoWT) Using Machine and Deep Learning Methods: A Survey," *Mesopotamian Journal of Computer Science*, vol. 2025, pp.17–63, 2025. https://doi.org/10.58496/MJCSC/2025/002

[7] S. D. Guptta, K. T. Shahriar, H. Alqahtani, D. Alsalman, and I. H. Sarker, "Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques," *Annals of Data Science*, vol.11, no.1, pp.217-42, March 2024. https://doi.org/10.1007/s40745-022-00379-8

[8] S. Alnemari and M. Alshammari, "Detecting Phishing Domains Using Machine Learning," *Applied Sciences*, vol.13, no.8, pp. 4649, April 2024. https://doi.org/10.3390/app13084649

[9] E. Kocyigit, M. Korkmaz, O. Koray Sahingoz, and B. Diri, "Enhanced Feature Selection Using Genetic Algorithm for Machine-Learning-Based Phishing URL Detection," *Applied Sciences*, vol.14, no.14, pp.6081, July 2024. https://doi.org/10.3390/app14146081

[10] U. A. Butt, R. Amin, H. Aldabbas, S. Mohan, B. Alouffi, and A. Ahmadian, "Cloud-based email phishing attack using machine and deep learning algorithm," *Complex & Intelligent Systems*, vol.9, pp.3043–3070, June 2022. https://doi.org/10.1007/s40747-022-00760-3

[11] A. Maci, A. Santorsola, A. Coscia, and A. Iannacone, "Unbalanced Web Phishing Classification through Deep Reinforcement Learning," *Computers*, vol.12, no.6, pp.118, June 2023. https://doi.org/10.3390/computers12060118

[12] S. Atawneh and H. Aljehani, "Phishing Email Detection Model Using Deep Learning," *Electronics*, vol.12, no.20, pp.4261, October 2023. https://doi.org/10.3390/electronics12204261

[13] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, Q. E. U. Haq, K. Saleem, and M. H. Faheem, "A Deep Learning-Based Phishing Detection System Using CNN, LSTM, and LSTM-CNN," *Electronics*, vol.12, no.1, pp.232, January 2023. https://doi.org/10.3390/electronics12010232

[14] U. Zara, K. Ayyub, H. U. Khan, A. Daud, and T. Alsahfi, "Phishing Website Detection Using Deep Learning Models," *IEEE Access*, vol.12, pp.167072 - 167087, October 2024. https://doi.org/10.1109/access.2024.3486462

[15] S. R. A. Samad, S. Balasubaramanian, A. S. Al-Kaabi, B. Sharma, S. Chowdhury, A. Mehbodniya, et al., "Analysis of the Performance Impact of Fine-Tuned Machine Learning Model for Phishing URL Detection," *Electronics*, vol.12, no.7, pp.1642, March 2023. https://doi.org/10.3390/electronics12071642

[16] D. R. I. M. Setiadi, S. Widiono, A. N. Safriandono, and S. Budi, "Phishing Website Detection Using Bidirectional Gated Recurrent Unit Model and Feature Selection," *Journal of Future Artificial Intelligence and Technologies*, vol.1, no.2, pp.75-83, July 2024. https://doi.org/10.62411/faith.2024-15

[17] S. Jamal, H. Wimmer, and I. H. Sarker, "An improved transformer-based model for detecting phishing, spam and ham emails: A large language model approach," *Security and Privacy*, vol.7, no.5, pp.e402, April 2024. https://doi.org/10.1002/spy2.402

[18] A. Aljofey, Q. Jiang, Q. Qu, M. Huang, and J-P. Niyigena, "An Effective Phishing Detection Model Based on Character Level Convolutional Neural Network from URL," *Electronics*, vol.9, no.9, pp.1514, September 2020. https://doi.org/10.3390/electronics9091514

[19] E. M. Elkenawy, A. A. Alhussan, D. S. Khafaga, Z. Tarek, and A. M. Elshewey, "Greylag goose optimization and multilayer perceptron for enhancing lung cancer classification," *Scientific Reports*, vol.14, no.23784, pp.1-23, October 2024. https://doi.org/10.1038/s41598-024-72013-x

[20] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," *Cluster Computing*, vol.25, pp.3819–3828, May 2022. https://doi.org/10.1007/s10586-022-03604-4

[21] M. Almousa, T. Zhang, A. Sarrafzadeh, and M. Anwar, "Phishing website detection: How effective are deep learning-based models and hyperparameter optimization?," *Security and Privacy*, vol.5, no.6, pp.e256, August 2022. https://doi.org/10.1002/spy2.256

[22] L. Lakshmi, M. P. Reddy, C. Santhaiah, and U. J. Reddy, "Smart Phishing Detection in Web Pages using Supervised Deep Learning Classification and Optimization Technique ADAM," *Wireless Personal Communications*, vol.118, pp.3549–3564, March 2021. https://doi.org/10.1007/s11277-021-08196-7

[23] F. Aljuaydi, B. K. Behera, A. M. Elshewey, and Z. Tarek, "A Deep Learning Prediction Model to Predict Sustainable Development in Saudi Arabia," *Applied Mathematics & Information Sciences*, vol.18, no.6, pp.1345-1366, 2024. http://dx.doi.org/10.18576/amis/180615

[24] D. Han, H. Li, and X. Fu, "Reflective Distributed Denial of Service Detection: A Novel Model Utilizing Binary Particle Swarm Optimization—Simulated Annealing for Feature Selection and Gray Wolf Optimization-Optimized LightGBM Algorithm," *Sensors*, vol.24, no.19, pp.6179, September 2024. https://doi.org/10.3390/s24196179

[25] A. J. S. Albahadili, A. Akbas, and J. Rahebi, "Detection of phishing URLs with deep learning based on GAN-CNN-LSTM network and swarm intelligence algorithms," *Signal, Image and Video Processing*, vol.18, pp.4979-95, June 2024. https://doi.org/10.1007/s11760-024-03204-2

[26] A. Denis, A. Thomas, W. Robert, A. Samuel, S. Peter Kabiito, Z. Morish, M. Sallam, G. Ali, and M. M. Mijwil, "A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities," *SHIFRA*, vol.2025, pp.1-45, Januanry 2025. https://doi.org/10.70470/SHIFRA/2025/001

[27] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "An effective fraud detection using competitive swarm optimization based deep neural network," *Measurement: Sensors*, vol.27, pp.100793, June 2023. https://doi.org/10.1016/j.measen.2023.100793

[28] P. H. Kyaw, J. Gutierrez, and A. Ghobakhlou, "A Systematic Review of Deep Learning Techniques for Phishing Email Detection," *Electronics*, vol.13, no.19, pp.3823, September 2024. https://doi.org/10.3390/electronics13193823

[29] J. Aljabri, N. Alzaben, N. NEMRI, S. Alahmari, S. D. Alotaibi, S. Alazwari, et al., "Hybrid stacked autoencoder with dwarf mongoose optimization for Phishing attack detection in internet of things environment," *Alexandria Engineering Journal*, vol.106, pp.164-171, November 2024. https://doi.org/10.1016/j.aej.2024.06.070

[30] S. Minocha and S. Birmohan, "A novel phishing detection system using binary modified equilibrium optimizer for feature selection," *Computers & Electrical Engineering*, vol. 98, pp.107689., 2022. https://doi.org/10.1016/j.compeleceng.2022.107689.

[31] G. Mohamed, J. Visumathi, M. Mahdal, J. Anand, and M. Elangovan, "An Effective and Secure Mechanism for Phishing Attacks Using a Machine Learning Approach," *Processes*, vol.10, no.7, pp.1356, July 2022. https://doi.org/10.3390/pr10071356

[32] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, and J.Q. Wang, "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, vol.15, pp. 1865–1879, April 2018. https://doi.org/10.1007/s12652-018-0786-3

[33] K. Bitirgen and Ü. B. Filik "A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid," *International Journal of Critical Infrastructure Protection*, vol.40, pp.100582, March 2023. https://doi.org/10.1016/j.ijcip.2022.100582

[34] N. Kunhare, R. Tiwari, and J. Dhar, "Particle swarm optimization and feature selection for intrusion detection system," Sādhanā, vol.45, pp.109, May 2020. https://doi.org/10.1007/s12046-020-1308-5

[35] S. Jagan, A. Ashish, M. Mahdal, K. R. Isabels, et al., "A Meta-Classification Model for Optimized ZBot Malware Prediction Using Learning Algorithms," *Mathematics*, vol.11, no.13, pp.2840, June 2023. https://doi.org/10.3390/math11132840

[36] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, et al., "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method," *Sensors*, vol.22, no.16, pp.5986, August 2022. https://doi.org/10.3390/s22165986

[37] T. R. Alsenani, S. I. Ayon, S. M. Yousuf, F. B. K. Anik, and M. E. S. Chowdhury, "Intelligent feature selection model based on particle swarm optimization to detect phishing websites," *Multimedia Tools and Applications*, vol.82, pp.44943–44975, April 2023. https://doi.org/10.1007/s11042-023-15399-6

[38] C. Yang, W. Guan, and Z. Fang, "IoT Botnet Attack Detection Model Based on DBO-Catboost," *Applied Sciences*, vol.13, no.12, pp.7169, June 2023. https://doi.org/10.3390/app13127169

[39] S. K. Towfek, "CNN-Based Multiclass Classification for COVID-19 in Chest X-ray Images," *Journal of Artificial Intelligence and Metaheuristics*, vol. 6, no. 1, pp. 48-55, 2023. https://doi.org/10.54216/jaim.060105

[40] M. Abotaleb, W. H. Lim, P. Mishra, A. T. Qenawy, and E. M. ALmetwally, "Enhancing Stock Price Prediction Accuracy Using ARIMA and Advanced Greylag Goose Optimizer Algorithm," *Journal of Artificial Intelligence in Engineering Practice*, vol.1, no.1, pp. 49-65, April 2024. https://doi.org/10.21608/jaiep.2024.355004

[41] N. Innab, A. A. F. Osman, M. A. M. Ataelfadiel, M. A-Zanona, B. M. Elzaghmouri, et al., "Phishing Attacks Detection Using Ensemble Machine Learning Algorithms," *Computers, Materials & Continua*, vol.80, no.1, pp.1325-1245, 2024. https://doi.org/10.32604/cmc.2024.051778

[42] S. A. Elsaid, E. Shehab, A. M. Mattar, A. T. Azar, and I. A. Hameed, "Hybrid intrusion detection models based on GWO optimized deep learning," *Discover Applied Sciences*, vol.6, no.531, pp.1-34, October 2024. https://doi.org/10.1007/s42452-024-06209-1

[43] M. F. Alghenaim, N. A. A. Bakar, and F. A. Rahim, "Anti-Phishing Tools: State of the Art and Detection Efficiencies," *Applied Mathematics & Information Sciences*, vol.16, no.6, pp. 929-34, 2022. https://doi.org/10.18576/amis/160609

[44] M. A. Elberri, Ü. Tokeşer, J. Rahebi and J. M. Lopez-Guede, "A cyber defense system against phishing attacks with deep learning game theory and LSTM-CNN with African vulture optimization algorithm (AVOA)," *International Journal of Information Security*, vol.23, no.4, pp. 2583-606, May 2024. https://doi.org/10.1007/s10207-024-00851-x

[45] A. B. Majgave, and N. L. Gavankar, "Automatic Phishing Website Detection and Prevention Model Using Transformer Deep Belief Network," *Computers & Security*, vol. 147, pp.104071, 2024. https://doi.org/10.1016/j.cose.2024.104071

[46] L. Das, L. Ahuja, and A. Pandey, "A novel deep learning model-based optimization algorithm for text message spam detection," *The Journal of Supercomputing*, vol.80, pp.17823–17848, May 2024. https://doi.org/10.1007/s11227-024-06148-z

[47] S. Anupam and A. K. Kar, "Phishing website detection using support vector machines and nature-inspired optimization algorithms," *Telecommunication Systems*, vol.76, pp.17-32, November 2020. https://doi.org/10.1007/s11235-020-00739-w

[48] Y. Fouad, N. E. Abdelaziz, and A. M. Elshewey, "IoT Traffic Parameter Classification based on Optimized BPSO for Enabling Green Wireless Networks," *Engineering Technology & Applied Science Research*, vol. 14, no. 6, pp. 18929-34, 2024. https://doi.org/10.48084/etasr.9230

[49] A. M. Salman, H. I. Wahhab, A. B. Alnajjar, B. Al-Attar, R. Sekhar, and N. Itankar, "Revolutionizing Wireless Sensor Networks through an Effective Approach for Quality of Service Enhancement," *Applied Data Science and Analysis*, vol.2025, pp.144-154, April 2025. https://doi.org/10.58496/ADSA/2025/012

[50] A, Desai and M. Desai, "A Review of the State of Cybersecurity in the Healthcare Industry and Propose Security Controls," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol.2023, pp.82-84, 2023. https://doi.org/10.58496/MJAIH/2023/016

[51] N. Kamble and N. Mishra, "Hybrid Optimization Enabled Squeeze Net for Phishing Attack Detection," *Computers & Security*, vol. 144, pp.103901, May 2024. https://doi.org/10.1016/j.cose.2024.103901.

[52] M. Nanda and S. Goel, "URL based phishing attack detection using BiLSTM-gated highway attention block convolutional neural network," *Multimedia Tools and Applications*, vol.83, pp.69345–69375, January 2024. https://doi.org/10.1007/s11042-023-17993-0

[53] S. Jafari and N. Aghaee-Maybodi. "Detection of Phishing Addresses and Pages With a Data Set Balancing Approach by Generative Adversarial Network (GAN) and Convolutional Neural Network (CNN) Optimized With Swarm Intelligence," *Concurrency and Computation Practice and Experience*, vol. 36, no. 11, Jan. 2024, https://doi.org/10.1002/cpe.8033