A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF ÇANKIRI KARATEKİN UNIVERSITY

DETECTION OF PHISHING URLS WITH DEEP LEARNING BASED ON THE GAN-CNN-LSTM NETWORK AND SWARM INTELLIGENCE ALGORTHIMS

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
ELECTRONICS AND COMPUTER ENGINEERING

BY

ABBAS JABR SALEH ALBAHADILI

ÇANKIRI

2023

DETECTION OF PHISHING URLS WITH DEEP LEARNING BASED ON THE GAN-CNN-LSTM NETWORK AND SWARM INTELLIGENCE ALGORTHIMS

By Abbas Jabr Saleh ALBAHADILI

August 2023

We certify that we have read this thesis and that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science

Advisor **:** Asst. Prof. Dr. Ayhan AKBAŞ

Examining Committee Members:

Chairman **:** Asst. Prof. Dr. Ayhan AKBAŞ
Computer Engineering
Abdullah Gül University

Member **:** Assoc. Prof. Selim BUYRUKOĞLU
Electronics and Computer Engineering
Çankırı Karatekin University

Member **:** Assoc. Prof. Cevat RAHEBI
Computer Engineering
Istanbul Topkapı University

Approved for the Graduate School of Natural and Applied Sciences

Prof. Dr. Hamit ALYAR
Director of Graduate School

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Abbas Jabr Saleh ALBAHADILI

ABSTRACT

DETECTION OF PHISHING URLS WITH DEEP LEARNING BASED ON THE GAN-CNN-LSTM NETWORK AND SWARM INTELLIGENCE ALGORITHMS

Abbas Jabr Saleh ALBAHADILI

Master of Science in Electronics and Computer Engineering

Advisor: Asst. Prof. Dr. Ayhan AKBAŞ

August 2023

Phishing attacks are one of the challenges of the Internet and its users. Phishing attacks are an example of social engineering attacks based on deceiving users. In phishing attacks, fake pages that are very similar to legitimate pages are created on the Internet. In phishing attacks, the victim is directed to fake pages, and their valuable information is stolen. Most of the targets of phishing attacks include online payment services, banking, and online sales, so the losses of these attacks are significant. One way to detect phishing attacks is to use machine learning and deep learning methods. The challenge of machine learning and deep learning methods is intelligent feature selection. The lack of feature extraction and intelligent feature selection reduces the accuracy of learning methods in detecting phishing attacks. This paper presents a combined method with deep learning, machine learning, and swarm intelligence algorithms to detect phishing attacks. In the first phase, the dataset is balanced by deep learning based on the GAN network. In the second step, the convolutional neural network extracts the primary features from the links and code of web pages. In the third step, the White Shark Optimizer (WSO) algorithm selects the essential features. In the last step, the LSTM neural network classifies the samples. The proposed method has been evaluated on ISCX-URL-2016 and Phishtank datasets for feature extraction and selection. The proposed method's accuracy, precision, and sensitivity in the ISCX-URL-2016 data set are 97.94%, 97.82%, and 97.76%, respectively. In the Phishtank dataset, the proposed method has accuracy, precision, and sensitivity of 96.78%, 95.67%, and 95.71%. The proposed method is more accurate than

LSTM, CNN, CNN-LSTM, CNN+GA, DNN, VAE-DNN, and AE-DNN methods in detecting phishing.

2023, 45 pages

Keywords: Fake pages, Phishing attacks, Generative adversarial network, Convolutional neural network, Feature selection, Swarm intelligence algorithm

ÖZET

GAN-CNN-LSTM AĞI VE SWARM ZEKA ALGORİTMALARINI TABANLI DERİN ÖĞRENME İLE E-DOLANDIRICILIK URL'LERİNİN TESPİTİ

Abbas Jabr Saleh ALBAHADILI
Elektronik ve Bilgisayar Mühendisliği, Yüksek Lisans
Tez Danışmanı: Dr. Öğr. Üyesi Ayhan AKBAŞ
Ağustos 2023

Kimlik avı saldırıları, İnternet ve kullanıcılarının karşılaştığı zorluklardan biridir. Kimlik avı saldırıları, kullanıcıları aldatmaya dayalı sosyal mühendislik saldırılarına bir örnektir. Oltalama saldırılarında, internette yasal sayfalara çok benzeyen sahte sayfalar oluşturulur. Oltalama saldırılarında kurban sahte sayfalara yönlendirilir ve değerli bilgileri çalınır. Kimlik avı saldırılarının hedeflerinin çoğu çevrimiçi ödeme hizmetleri, bankacılık ve çevrimiçi satışları içerir, bu nedenle bu saldırıların kayıpları önemli düzeydedir. Kimlik avı saldırılarını tespit etmenin bir yolu, makine öğrenimi ve derin öğrenme yöntemlerini kullanmaktır. Makine öğrenimi ve derin öğrenme yöntemlerinin zorluğu, akıllı özellik seçimidir. Özellik çıkarımının ve akıllı özellik seçiminin olmaması, kimlik avı saldırılarını tespit etmede öğrenme yöntemlerinin doğruluğunu azaltır. Bu belge, kimlik avı saldırılarını algılamak için derin öğrenme, makine öğrenimi ve sürü zekası algoritmaları ile birleştirilmiş bir yöntem sunmaktadır. İlk aşamada, veri kümesi GAN ağına dayalı derin öğrenme ile dengelenir. İkinci adımda, evrişimli sinir ağı, birincil özellikleri web sayfalarının bağlantılarından ve kodundan çıkarır. Üçüncü adımda, White Shark Optimizer (WSO) algoritması temel özellikleri seçer. Son adımda, LSTM sinir ağı örnekleri sınıflandırır. Önerilen yöntem, özellik çıkarımı ve seçimi için ISCX-URL-2016 ve Phishtank veri kümeleri üzerinde değerlendirilmiştir. Önerilen yöntemin ISCX-URL-2016 veri setindeki doğruluğu, kesinliği ve duyarlılığı sırasıyla %97,94, %97,82 ve %97,76'dır. Phishtank veri setinde, önerilen yöntem %96.78, %95.67 ve %95.71 doğruluk, kesinlik ve duyarlılığa sahiptir. Önerilen yöntem oltalama tespitinde LSTM,

CNN, CNN-LSTM, CNN+GA, DNN, VAE-DNN ve AE-DNN yöntemlerinden daha doğru sonuç vermektedir.

2023, 45 sayfa

Anahtar Kelimeler: Sahte sayfalar, Kimlik avı saldırıları, Üretken düşman ağı, Evrişimli sinir ağı, Özellik seçimi, Sürü zekası algoritması

PREFACE AND ACKNOWLEDGEMENTS

I would like to thank my thesis advisor, Asst. Prof. Dr. Ayhan AKBAŞ, for his patience, guidance and understanding.

Abbas Jabr Saleh ALBAHADILI

Çankırı-2023

CONTENTS

LIST OF ABBREVIATIONS

APWG	Anti-phishing working group
CNN	Convolutional neural networks
DNN	Deep neural networks
GA	Genetic algorithm
GAN	Generative adversarial network
RCNN	Recurrent convolutional neural networks
RNN	Recurrent neural networks
WSO	White shark optimizer

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

With the Internet's expansion and social media's spread, security challenges have also increased (Zieni *et al.* 2023). Phishing attacks are an example of security challenges that threaten Internet users. Phishing attacks are a method of stealing user information using social engineering techniques. In phishing attacks, a legitimate website is forged by a hacker or Fisher, and a fake version of the legitimate website is uploaded to the Internet. Fake pages look very similar to legal pages; therefore, fake pages deceive users. In fake pages, facilities similar to legal sites, such as fields for entering user information, such as user name and password, are considered (Zieni *et al.* 2023, Buckley *et al.* 2023). By stealing user information such as user names and passwords, a Fisher or thief can use this information to enter a legal website (Anuar *et al.* 2022). In phishing attacks, phishers use communication tools such as email, chat, phone, and social networks to communicate with their victims. In these cases, links to fake pages are sent to the victim through communication media, and the victim is requested to click on the fake links. Fishers use different methods of deception and social engineering to convince users to click on fake links (Siddiqi *et al.* 2022).

Phishing attacks have increased significantly during the spread of the Covid-19 disease because most people in the community have tried to receive services such as online sales through the Internet during quarantine. Reports show phishing attacks target targets such as payment gateways, banking, financial institutions, and online sales (Al-Qahtani and Cresci 2022, Zahra *et al.* 2022). Phishing attacks have significant losses, and estimates show that these attacks cause billions of dollars in damage to users and Internet infrastructure. According to the Anti-Phishing Working Group (APWG), threats related to phishing attacks on social media increased by 47% from the first quarter to the second quarter of 2022. According to this report, the number of fake pages and phishing attacks has grown significantly in recent years (Wei and Sekiya 2022).

Today, blacklist methods (Oest *et al.* 2020), heuristic methods (Da Silva *et al.* 2020), visual methods (Paturi *et al.* 2020), machine learning methods (Divakaran and Oest

2022), and deep learning (Aljabri and Mirza 2022) are used to detect phishing attacks. Blacklist methods store the addresses of fake sites in a database, and to detect attacks, it is necessary to search this database. Memory consumption, long search time, and inability to detect zero-day attacks are the challenges of blacklist methods (Aljofey *et al.* 2022). Heuristic methods use heuristic mechanisms such as address length, JavaScript codes, and domain information to detect phishing. Heuristic methods have a high false positive alarm rate (Raja *et al.* 2022). Visual methods to detect fake pages using elements related to images like Logo to detect fake pages. Visual methods for detecting phishing attacks consider visual information; therefore, visual methods are not very accurate (Van et al. 2021). Unlike other approaches, machine learning and deep learning methods have a learning mechanism and can detect zero-day attacks (Xiao *et al.* 2020, Zhu *et al.* 2022). To detect phishing attacks, approaches such as artificial neural networks (Zhu *et al.* 2020), support vector machines (Rambabu *et al.* 2022), decision-tree (Balogun *et al.* 2021), convolutional neural networks (Roy *et al.* 2022), LSTM networks (Nepal *et al.* 2022), and GAN (Rahman *et al.* 2022) have been presented. A major challenge in machine learning and deep learning methods is feature extraction and selection. Feature engineering and selecting basic features are essential factors in reducing the detection error of phishing attacks by machine learning and deep learning methods (Hota *et al.* 2022, Ahmed *et al.* 2022).

One of the efficient methods to select the feature is a meta-heuristic method. Meta-heuristic methods are modeled on living beings' biological, physical, and behavioral phenomena. Meta-heuristic methods such as the Genetic algorithm (GA) (Wang 2022), Particle swarm algorithm (Priya *et al.* 2022), Whale optimization algorithm (Shuaib *et al.* 2019), and Spotted hyena optimizer (Sabahno and Safara 2022), have been used to detect phishing attacks.

Another challenge in detecting phishing attacks is the imbalance between phishing samples and typical data sets. Methods such as SMOTE have been proposed to solve the dataset's imbalance challenge. Deep learning methods such as GAN have also been proposed for the challenge of the lack of training samples. One of the main challenges in

detecting phishing attacks is the false positive alarm rate. Intelligent methods should be used to reduce the false positive alarm rate.

This paper aims to present a method of detecting phishing attacks with a low error rate to reduce the threats caused by phishing attacks. The proposed method in this paper is a multi-step approach. In the proposed method, samples are balanced by GAN deep learning method. In the next step, the convolution neural network features related to the link and code of the web pages are extracted. In the next step, the white shark optimization algorithm (Braik *et al.* 2022) is used to select the main feature. In the final stage, the selected features are considered as the input of the LSTM neural network. The role of the LSTM neural network is to classify fake and legal links. The contribution of our authors and innovation in this article includes the following:

- Balancing the data set of phishing attacks with the GAN deep learning method
- Feature extraction with an improved version of the CNN neural network
- Providing a binary version of the white shark optimization algorithm
- Practical use of white shark optimization algorithm in feature selection and detection of phishing attacks
- Presenting a hybrid approach of CNN, LSTM, and swarm intelligence to detect phishing attacks

This study is divided into several parts. The second part delves into the background and related works. In the third part, a proposed method for detecting phishing attacks is formulated and presented. The fourth part implements the proposed method and compares it to similar approaches. The fifth part presents the conclusions and discusses future work.

1.1 Thesis Organization

The thesis is divided into five chapters. The first chapter presents the introduction. The second chapter offers a literature review and discusses related works. Chapter three details

the materials and methods. Chapter four presents the results and discussion. Finally, chapter five concludes the thesis.

2. LITERATURE REVIEW

Reports show that phishing attacks are very effective attacks against Internet users. Fishers do not need much knowledge to carry out phishing attacks. In these attacks, fake websites that look very similar to legal websites are loaded on the Internet. The goal of phishers is to steal user information from fake sites. Estimates like the graph in Figure 2.1 show that the number of phishing attacks has increased between 2020 and 2021 (Guo *et al.* 2021).

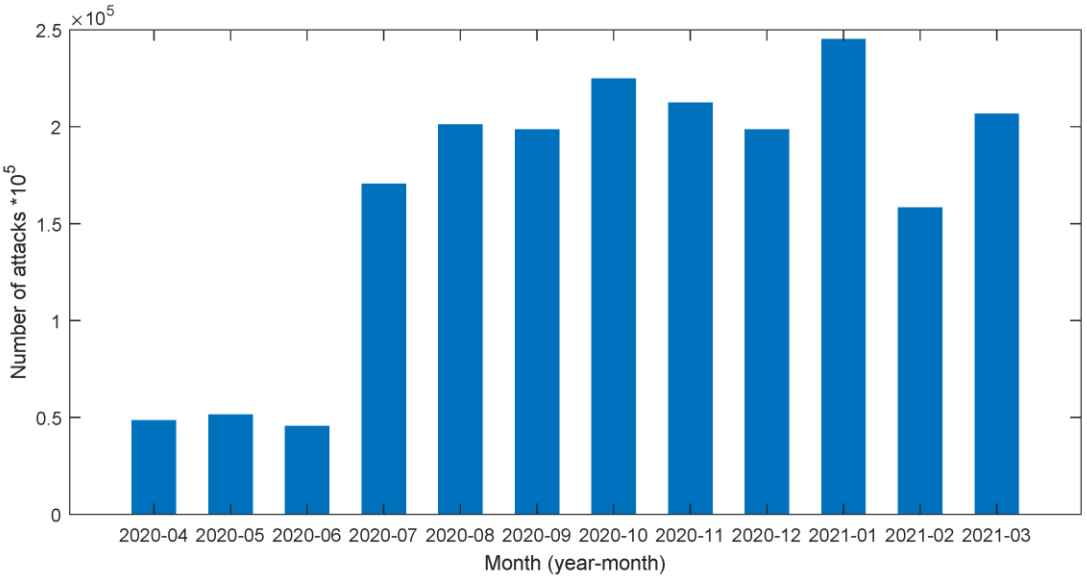

Figure 2.1 Increase in the number of phishing attacks in 2020 and 2021 (Guo *et al.* 2021)

The increase in phishing attacks causes many users to become victims of these harmful attacks. The main focus and target of phishing attacks are financial and commercial websites on the Internet with many users. Therefore the number of phishing victims is significant. The diagram of the Figure 2.2 shows the percentage of phishing attacks in each area of the Internet. The focus on phishing attacks on financial institutions, banks, and payment gateways has made the losses of these attacks significant (Basit *et al.* 2021).

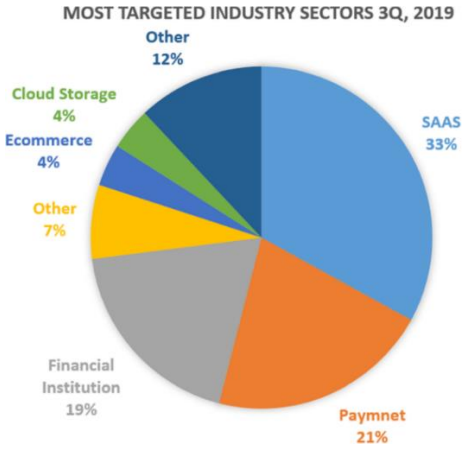

Figure 2.2 Concentration of phishing attacks in different sectors (Basit *et al.* 2021)

Reports show that most phishing attacks are against online payment gateways and financial services. Considering that the goal of phishing attacks in most cases is to steal money, the losses of these attacks are expected to be significant. According to the diagram in Figure 2.2, 33% of phishing attacks are against cloud services, and 21% and 19% are against payment gateways and financial organizations, respectively.

In the era of Covid-19, the number of online users on the Internet has increased, leading to increased security challenges and social engineering attacks. The diagram of Figure 2.3 shows the share of phishing attacks among the challenges related to social engineering attacks (Hijji and Alam 2021).

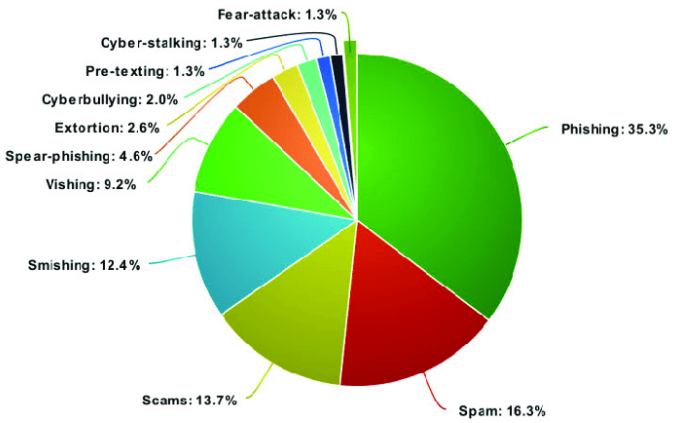

Figure 2.3 Significant contribution of phishing attacks in social engineering attacks (Hijji and Alam 2021)

Reports show that phishing attacks have the largest share among social engineering attacks, with a share of 35.3%, and this shows the importance of detecting these attacks. It is essential to understand the process and cycle of phishing attacks to detect phishing attacks. In the diagram of Figure 2.4, the cycle of phishing attacks is displayed. In phishing attacks, a legitimate website is faked by a fisher, and then fake links are sent to users through communication tools such as email (Daengsi *et al.* 2021).

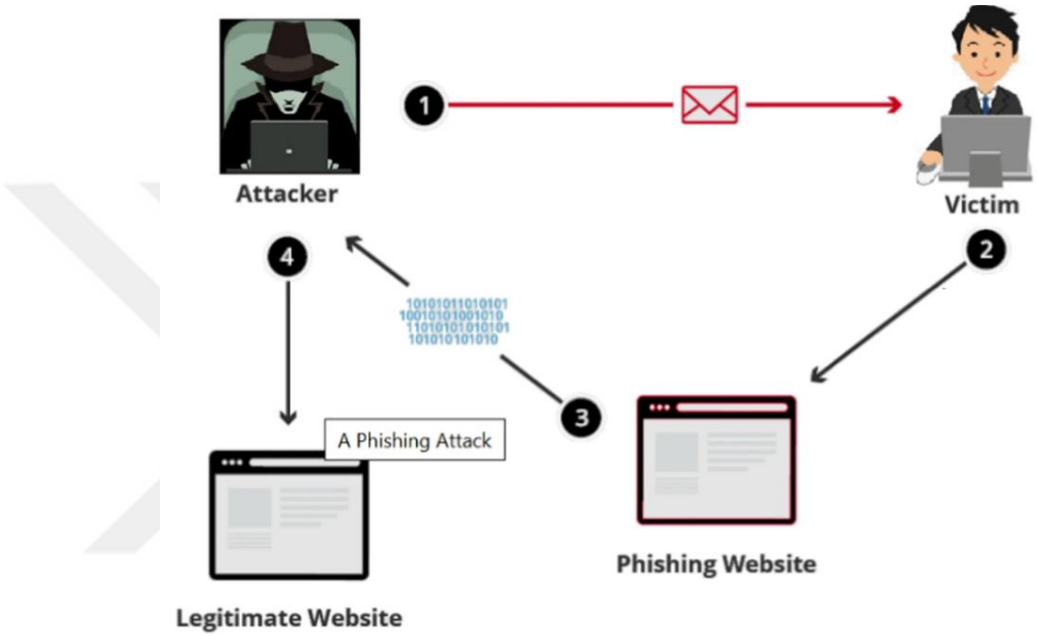

Figure 2.4 The cycle of phishing attacks (Daengsi *et al.* 2021)

Users can be chosen as a victim if they receive an email containing unnatural links. Users who click on unnatural links will enter fake websites, and their valuable information, such as usernames and passwords, will be stolen. By stealing users' sensitive information, a phisher can use this information to enter the main website and steal users' information (Daengsi *et al.* 2021). Several approaches to detect phishing attacks, such as blacklist, heuristics, and methods based on deep learning and machine learning, are discussed below. Unlike other approaches, the advantage of machine learning and deep learning methods is the ability to detect zero-day attacks. Machine learning and deep learning methods combined with feature selection methods accurately detect phishing attacks.

In (Benavides *et al.* 2023), a method for detecting phishing attacks by deep learning methods based on HTML and the source code of web pages is presented. In this research, deep neural networks (DNN), recurrent neural networks (RNN), convolutional neural networks (CNN), and recurrent convolutional neural networks (RCNN) have been compared for detecting phishing attacks. Evaluations showed that deep learning methods had achieved an accuracy of about 84% in detecting phishing attacks.

In (Adane and Beyene 2023), the detection of phishing websites with feature selection methods and a machine learning approach is presented. Their tests showed that the Cat-Boost classification has the highest accuracy of 97.46% in detecting phishing attacks. Experiments showed that the PCA technique is the most accurate feature selection method among the compared methods.

In (Asiri *et al.* 2023), reviewed the detection of phishing attacks based on URL and HTML information. This paper comprehensively examines phishing attacks based on information related to HTML and URLs.

In (Bountakas and Xenakis 2023), presented an embedded and hybrid learning method to detect phishing emails. This article has implemented group learning methods to identify phishing emails. The results are performed on an unbalanced data set (including 32051 benign email samples and 3460 phishing email samples). Tests show that their method has an F1 index of about 99%.

In (Wen *et al.* 2023), presented a new method for detecting phishing fraud in cryptocurrencies with the deep neural network. This paper proposes a deep neural network method based on LSTM-FCN and BP neural networks. The results of the tests show that feature selection is very effective in detecting phishing accounts, and the accuracy of this method is reported to be around 97.86%.

In (Tan *et al.* 2023), presented a method of detecting phishing attacks using common visual and textual identity. Their method detects phishing attacks with an accuracy of

about 98.6% with the help of information related to website logos and website content information. Their method can reduce the false positive rate by about 3.4 compared to the compared methods.

In (Bozkir *et al.* 2023), presented a neural network to identify phishing web pages with an N-gram-based feature selection mechanism. This paper uses two deep-learning neural networks, CNN and LSTM, in phishing detection. Their approach to detecting phishing attacks has an accuracy of about 98.27%.

In (Shirazi *et al.* 2023), presented a hybrid deep learning method to improve phishing detection algorithms. Machine learning algorithms are prone to attacks that hackers can bypass the machine learning-based classifier by manipulating data. This challenge can reduce the effectiveness of machine learning methods in detecting phishing attacks. In this paper, to solve this challenge, they teach machine learning methods with a generative adversarial network (GAN). Experiments show that the GAN network can reduce the accuracy of machine learning methods in detecting phishing attacks.

In (Nordin and Ismail 2023), presented a combination of butterfly optimization algorithm and harmony search in detecting phishing attacks. Their method's average accuracy for WPD and PWD datasets is 98.69% and 98.80%, respectively.

Examining related works showed that detecting phishing attacks is a complex classification problem. In this issue, website pages and links are considered input and classified into standard and phishing. Various approaches have been proposed to detect phishing attacks, which are placed in the following three categories:

- Blacklist method: This method uses a list containing addresses of fake pages to detect phishing attacks. The information on links and fake pages is placed in a database. To detect phishing attacks, web pages and internet links are matched with this List. The web page or link is considered phishing if the input pattern is detected in the List. The

challenge and disadvantages of this method are high memory consumption, powerful novel search, and inability to detect zero-day attacks.

- Heuristic methods: In this method, discoveries such as the length of the address, the number of dots used in the address, and the presence of special characters are used to detect phishing attacks. These methods' disadvantages are high False Positive(FP) rates, lack of learning, and inability to detect zero-day attacks.

- Visual methods: These methods use matching elements such as logo websites and matching them with other pages. These methods require image processing and have high complexity, and on the other hand, their error rate is significant.

- Machine learning and deep learning methods: These methods can detect zero-day attacks and have high accuracy. A balanced data set is needed to increase the accuracy of learning models. Another disadvantage of these methods is that if learning is not done on the basic features, they have a significant error rate.

3. MATERIALS AND METHODS

In Related works showed that machine learning and deep learning could detect new attacks and zero-day phishing. It is necessary to generate artificial samples to balance the data set for detecting phishing attacks with high accuracy. Another approach to increase the accuracy of machine learning and deep learning methods is feature engineering, such as feature extraction and selection. The innovation of this research to detect phishing attacks is as follows:

- Balancing training and test samples based on the production of synthetic samples with the GAN deep learning method
- Presenting a new approach for mapping URL strings to a suitable format for deep learning
- Extracting features of internet links with CNN neural network
- Presenting a binary version of the white shark optimization algorithm to select the essential features in the CNN neural network output
- Adjusting the LSTM neural network inputs with the features of the White Shark Optimizer (WSO) algorithm selected to classify the samples into two categories, legal and phishing.

A proposed method for detecting phishing attacks is introduced in the rest of this section. The proposed method has different parts, such as balancing the data set with GAN, feature extraction with CNN, feature selection with the WSO algorithm, and classification of LSTM samples.

3.1 Proposed Framework

The proposed method in this paper is called CNN-WSO-LSTM. The framework of the proposed method for detecting phishing attacks is shown in Figure 3.1.

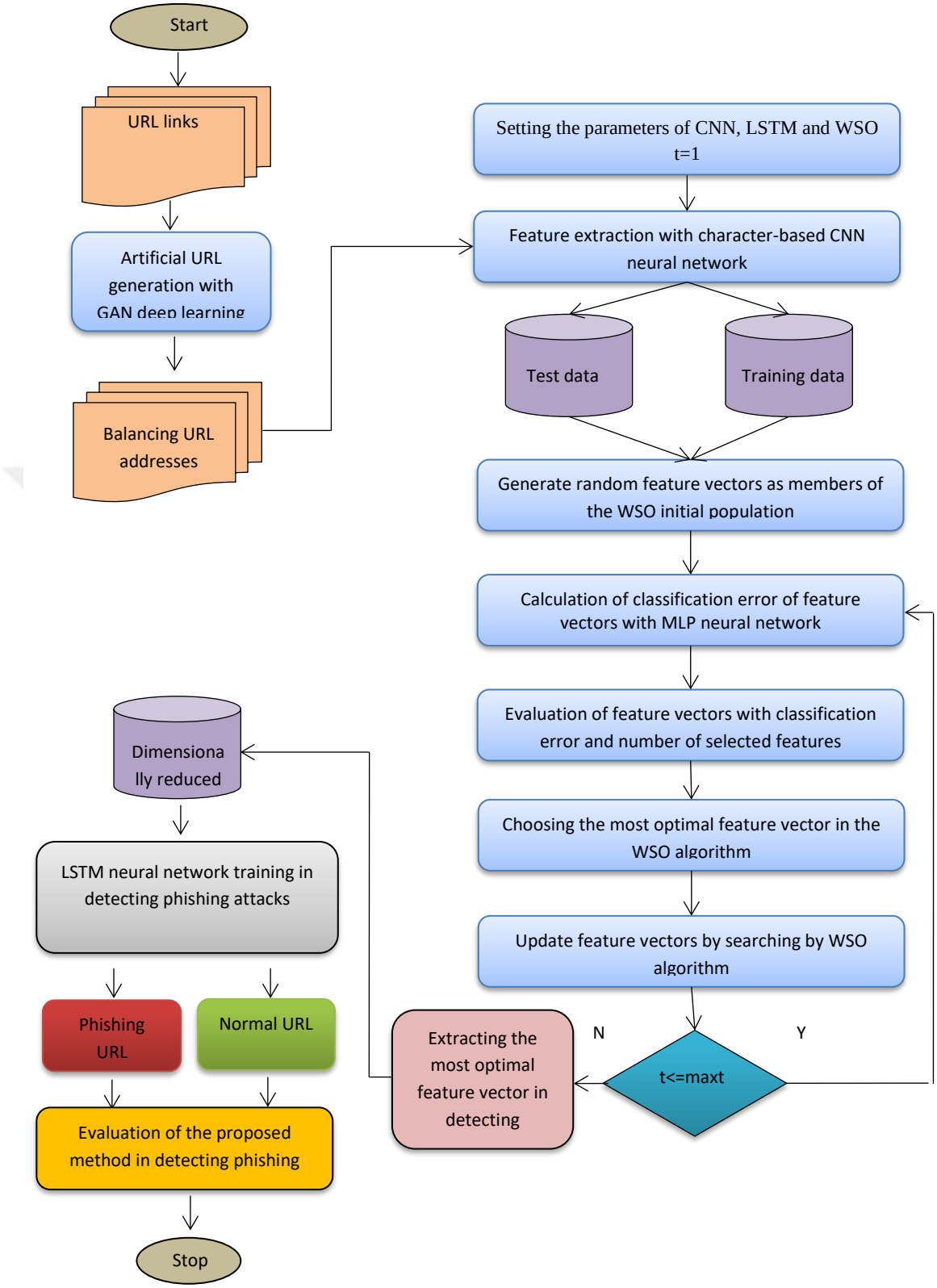

Figure 3.1 The framework of the proposed method in detecting phishing attacks

According to the proposed framework of the proposed method or CNN-WSO-LSTM, the following steps are suggested to detect phishing attacks:

- Setting deep learning parameters of CNN and LSTM and WSO algorithm
- Setting the WSO Algorithm counter such as t=1, Maxt
- Collection of incoming URLs
- GAN deep learning training with training examples
- Generating artificial URLs with GAN and balancing the dataset
- CNN neural network training to extract features
- Coding a feature vector as a member of the WSO algorithm
- Creating an initial population of feature vectors as the initial population of the WSO algorithm
- Evaluation of each feature vector with MLP neural network based on the average detection error of fake links
- Determining the fitness of each feature vector with the average error of detecting phishing attacks and the number of selected features
- Update feature vectors with the WSO algorithm
- Repeating the steps of the feature selection algorithm and updating the feature vectors with the WSO algorithm
- LSTM neural network trained with the optimal feature vector.
- Evaluation of the proposed model in detecting phishing attacks based on indicators such as accuracy

3.2 Balancing Dataset

In most cases, the number of regular records exceeds the number of phishing samples. This problem needs to be fixed for the balance of the data set. Learning on an unbalanced dataset increases the detection error of phishing attacks. Artificial samples were created with deep learning methods such as GAN to balance the dataset to solve this challenge. The structure of a URL must be properly understood to generate artificial URLs.

According to studies (Lin *et al.* 2017), a URL has 84 different characters such as (a-z, A-Z, 0-9, -. !∗'();:&=+$,/?#[]). A matrix with 84 rows can be considered, the columns of which are addresses to represent a URL numerically. The structure of this matrix is shown in Equation (3.1)

$$\text{Coding(URL)} = \begin{array}{c} \\ \vdots \\ 3 \\ \vdots \\ 8 \\ \vdots \\ 13 \\ \vdots \\ 15 \\ 16 \\ \vdots \\ 20 \\ \vdots \\ 82 \\ 83 \\ 84 \end{array} \begin{array}{c} \textit{https://www.domian.com} \\ \begin{bmatrix} 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & & 1 & 0 & 0 \\ 1 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & & 0 & 1 & 0 \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 1 & 1 & & 0 & 0 & 0 \\ & \vdots & & \ddots & & \vdots & \\ 0 & 0 & 0 & & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & & 0 & 0 & 0 \end{bmatrix} \end{array} \tag{3.1}$$

The URL converts to a numerical matrix containing zero and one element in the proposed encoding. Each element "1" indicates which URL character is mapped to a number between 1 and 84. As in Equation (3.1), the example is the letter h, the eighth letter of the alphabet, and row number 8, and the first column where the character "h" is located is coded with the number one. The reason for using numerical and matrix coding is that this matrix is the input of GAN and CNN deep learning methods. The input of deep learning methods should be numerical, and matrix coding, and Equation (3.1) is used in the proposed coding method.

The generative adversarial network (GAN) can generate an artificial sample in the data set and balance the data set. This network includes two models named Generator and Discriminator. The structure of the GAN network for generating fake and artificial samples is shown in Figure 3.2. The generator and the discriminator compete to examine, capture and replicate changes within the dataset. A generator is an artificial neural network that generates fake and artificial URLs. The purpose of the generator is to generate fake data and artificial URLs so that the discriminator is deceived and considers

them legal URLs. The purpose of the discriminator is to distinguish the fake and artificial data produced by the generator from the legal URLs.

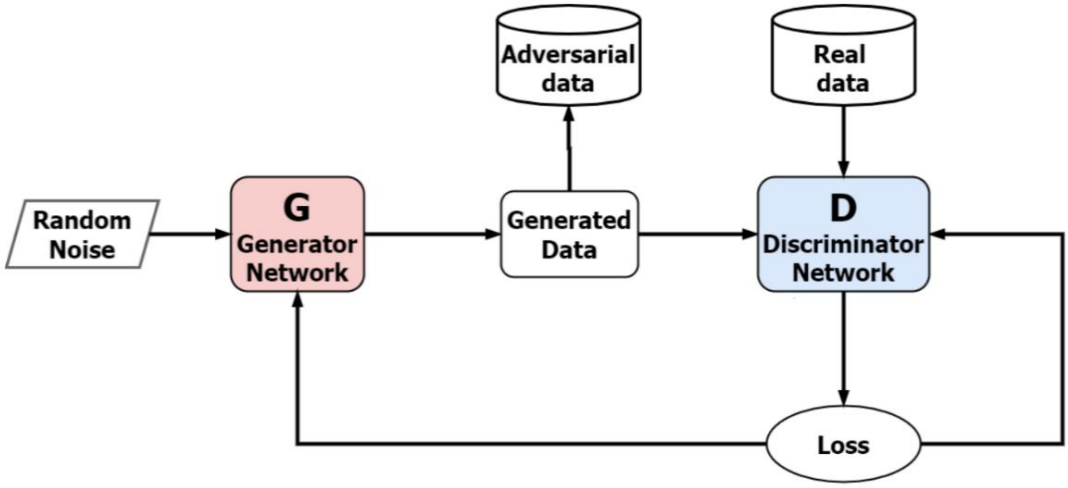

Figure 3.2 GAN deep learning structure (Shieh *et al.* 2015)

The steps to generate artificial and fake URLs in the GAN network are as follows:

- Creating a noisy and random input vector
- The generative network transforms the random input into a fake sample.
- The discriminant network categorizes the data produced by the generator.
- If the discriminator correctly classifies the fake sample, the generator is penalized.

In the GAN network, the generator and the discriminator are denoted by G and D, respectively. The real and random input is set by x and z, respectively. The part of random samples created with G(x) is displayed in the GAN network.

The objective function for the discriminator has two objective functions in Equation (3.2) and Equation (3.3):

$$l_{d_1} = \log\ \sigma(D(x)) \tag{3.2}$$

$$l_{d_2} = \log\ (1 - \sigma(D(G(z)))) \tag{3.3}$$

To maximize the efficiency of the GAN network in the discriminator part, the objective function in Equation (3.4) needs to be maximized. The numbers inside the log are between zero and one, and for depreciation, it is enough to multiply a negative number in Equation (3.4) and minimize the objective function like Equation (3.5).

$$L_D = l_{d_1} + l_{d_2} = \log\ \sigma(D(x)) + \log\,(1 - \sigma(D(G(z)))) \tag{3.4}$$

$$L_D = l_{d_1} + l_{d_2} = -(\log\ \sigma(D(x)) + \log\,(1 - \sigma(D(G(z))))) \tag{3.5}$$

The objective function for the generator is placed in Equation (3.6), and the objective of minimizing this objective function is:

$$L_G = -\log\ \sigma(D(G(z))) \tag{3.6}$$

3.3 Feature Extraction

The convolutional neural network is used at the character level to extract the features of the URLs used in the address in the proposed method. The structure of the convolutional neural network at the character level is presented in (Zhang *et al.* 2015); It is used for processing text strings and classifying them. The convolutional neural network structure is displayed at the character level according to Figure 3.3.

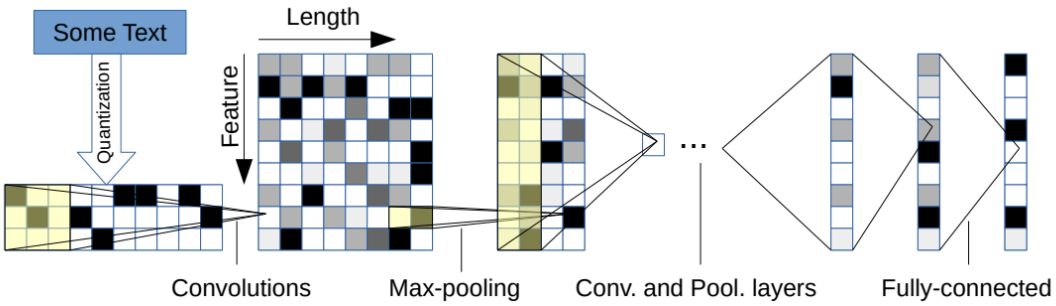

Figure 3.3 Character-level convolutional networks structure (Zhang *et al.* 2015)

Six convolution layers are used in the Character-level convolutional networks, and three fully connected layers are also defined. Weights are initialized using Gaussian distribution. The mean and standard deviation initializing the model is between 0 and 0.2. In the CNN network, the inputs are initially considered URLs. Then, according to equation (1), the URL addresses are converted into a numerical matrix, similar to this research process (Alshehri *et al.* 2022). The numerical matrix is considered the input of the convolution layers. In the proposed method, the output of the pooling layer is used for feature extraction. The features extracted in this step are set as the input of the LSTM network.

3.4 Feature Selection

The output of the feature extraction phase in the proposed method yields a set of features for detecting phishing attacks. However, some of these extracted features are unimportant and can diminish learning accuracy. Feature selection is employed to enhance the accuracy of the LSTM model. This feature selection phase is undertaken after the feature extraction phase and is framed as an optimization problem. Indeed, the feature selection challenge can be viewed as an optimization problem that can be tackled using meta-heuristic methods. The White Shark Optimization (WSO) algorithm (Braik *et al.* 2022) has been introduced as a swarm intelligence method. Advantages of the White Shark Optimization algorithm include the following:

- More accuracy in finding the optimal solution than popular meta-heuristic algorithms such as GA and PSO
- Balanced national and local search
- The behavior of swarm intelligence in the WSO algorithm makes it possible to search the parallel problem space and reduce the probability of getting caught in local optima.
- The WSO algorithm has been presented recently, and its capabilities in feature selection have been neglected.

The WSO algorithm is a meta-heuristic method for solving optimization problems and is modeled on the hunting behavior of sharks. The WSO algorithm is inspired by the scientific behavior of white sharks while searching for food in nature to survive in the deep ocean successfully. In the white shark optimizer algorithm, the exploratory search and exploitation process is well modeled. Figure 3.4 shows the white shark searching for food and the surrounding environment.

Figure 3.4 White shark searching for food (Braik *et al.* 2022)

Also, Figure 3.5 shows the heuristic methods of a white shark to hunt prey based on different distances (Makhadmeh *et al.* 2022).

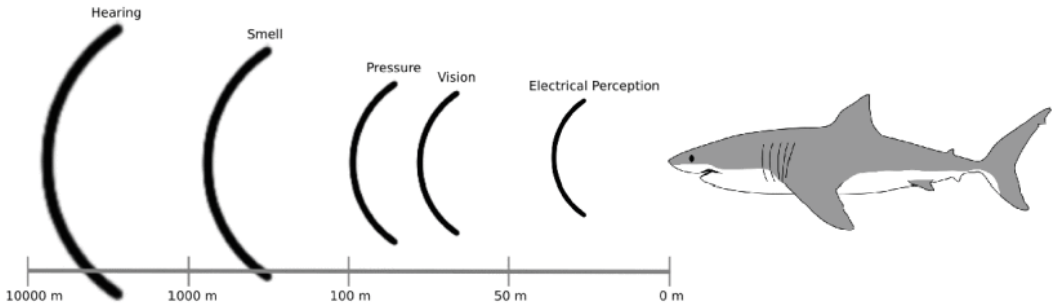

Figure 3.5 Heuristic methods of a white shark to hunt prey based on different distances (Makhadmeh *et al.* 2022).

Based on the distance, a shark can use different types of heuristic methods for hunting. Sharks detect the position of the bait based on electrical signals at distances of less than 50 meters. Sharks estimate the position of the prey at a distance between 50 and 100

meters, based on pressure, and between 100 and 1000 meters, based on smell. In the distance between 1000 and 10000, based on the sound of the prey, sharks recognize the location of the prey. The WSO algorithm is designed in such a way as to create a suitable balance between exploratory search behavior and productivity. The WSO algorithm has several steps explained and formulated in the following. In the proposed method for feature selection, a feature vector of web page URLs is coded as a member of the white shark optimization algorithm. Each feature vector is an array of 0 and 1, which respectively shows the non-selection of the feature and the selection of the feature in the detection of attacks. The proposed method randomly presents an initial population of feature vectors like Equation (3.7).

$$X = \begin{bmatrix} X_1^1 & X_1^2 & \cdots & X_1^d \\ X_2^1 & X_2^2 & \cdots & X_2^d \\ \vdots & \vdots & \vdots & \vdots \\ X_n^1 & X_n^2 & \dots & X_n^d \end{bmatrix} \tag{3.7}$$

In Equation (3.7), the number of feature vector elements equals d, and n is the number of feature vectors or the initial population of the WSO algorithm. In the proposed method, the feature vector No. i is displayed as x_i. The component j represents the dimension of a feature vector, and X is the initial population of feature vectors. One of the behaviors of the WSO algorithm is to update the motion feature vectors with the velocity vector towards a prey, as in Equation (3.8).

$$v_i^{t+1} = \mu[v_i^t + p_1(X_{gbest} - x_i^t) \times c_1 + p_2(X_{pbest}^i - x_i^t) \times c_2] \tag{3.8}$$

where v_i^t is the speed of shark number i in iteration t, and v_i^{t+1} is the new speed of shark or feature vector i. X_{gbest} is the most optimal feature vector or prey position, and X_{pbest}^i is the most optimal position that shark number i has obtained. Parameters c1 and c2 are two uniform random numbers between 0 and 1. In this equation, p_1 and p_2 are two coefficients for movement toward the prey and are calculated according to Equation (3.9) and Equation (3.10):

$$p_1 = p_{max} + (p_{max} - p_{min}) \times e^{-(4t/Maxt)^2} \quad (3.9)$$

$$p_2 = p_{min} + (p_{max} - p_{min}) \times e^{-(4t/Maxt)^2} \quad (3.10)$$

The p_{min} and p_{max} are set to 0.5 and 1.5, respectively. μ is the contraction coefficient to evaluate the convergence behavior of sharks, and it is calculated according to Equation (3.11):

$$\mu = \frac{2}{\left|2-\tau-\sqrt{\tau^2-\tau}\right|} \quad (3.11)$$

where, τ stands for the acceleration coefficient of the shark's movement toward the food and is equal to 4.125. The shark moves towards the prey with the calculated speed from the current position and moves according to Equation (3.12):

$$x_i^{t+1} = \begin{cases} x_i^t . \neg \oplus x_0 + u.a + lb & rand < m_v \\ x_i^t + \frac{v_i^t}{f} & rand \geq m_v \end{cases} \quad (3.12)$$

Values of a and b are defined as one-dimensional binary vectors. In this problem, the upper and lower boundaries of the search space are denoted by u and l, respectively. ω_0 is a rational vector defined in Equation (3.15). Equations (3.13) and (3.14) are used to calculate Equation (3.15).

$$a = sgn(x_i^t - u) > 0 \quad (3.13)$$

$$b = sgn(x_i^t - l) > 0 \quad (3.14)$$

$$x_0 = \oplus(a, b) \quad (3.15)$$

Values of f represent the frequency of the shark's wavy movement and are formulated according to Equation (3.16):

$$f = f_{min} + \frac{f_{max} - f_{min}}{f_{max} + f_{min}} \tag{3.16}$$

m_v is the symbol of the moving force, which increases with the number of rounds that the white shark reaches the prey, as in Equation (3.17):

$$m_v = \frac{1}{a_0 + e^{(\frac{Maxt}{2} - t)/a_1}} \tag{3.17}$$

where, a0 and a1 constants control exploratory search and exploitation. Sharks can move to a position near the prey and, in simpler terms, move to the most optimal shark in the population. For this purpose, Equation (3.18) is used.

$$x'^{t+1}_i = x_{gbest} + r_1 \times \vec{D} \times sgn(r_2 - 0.5) \qquad r_3 < S_s \tag{3.18}$$

The numbers r_1, r_2, and r_3 are random numbers between zero and one. $\vec{D}$ is the distance between the prey and the shark, formulated in Equation (3.19). $x'^{t+1}_i$is the new position of a shark in line with the optimal solution. S_s is the suggested coefficient to express the strength of the sharks' visual and olfactory senses after chasing other sharks close to the best prey and is formulated in Equation (3.20).

$$\vec{D} = \left| rand \times (x_{gbest} - x^t_i) \right| \tag{3.19}$$

$$S_s = \left| 1 - e^{(-a_2 \times t/Maxt)} \right| \tag{3.20}$$

Equation (3.20) is used to search for Fish School Behavior of white sharks.

$$x_i^{t+1} = \frac{x'^{t+1}_i + x_i^t}{2 \times rand} \tag{3.20}$$

By running the WSO algorithm, the feature vectors are updated in each iteration. S and V transfer functions are used to make the feature vectors binary, whose rules are formulated in Equation (3.21) and Equation (3.22).

$$T(x) = \frac{1}{1+e^{-x}} \tag{3.21}$$

$$T(x) = \left|\frac{2}{\pi}\arctan\left(\frac{\pi}{2}x\right)\right| \tag{3.22}$$

The feature vectors are re-normalized using S and V functions between zero and one. According to Equation (3.23), if the value of a feature is greater than or equal to 0.5, the feature is selected; otherwise, the feature is not selected.

$$x_i^t = \begin{cases} 1 & T(x_i^t) \geq 0.5 \\ 0 & T(x_i^t) < 0.5 \end{cases} \tag{3.23}$$

MLP neural network is used to evaluate each feature vector. Any feature vector that provides less error in the output of MLP and provides less number of features is more optimal. Equation (3.24) shows the feature selection objective function for evaluating the feature vectors.

$$Cost(x_i^t) = \alpha . E + \beta \frac{\|x_i^t\|}{d} \tag{3.24}$$

$\|x_i^t\|\|$ is the number of selected features in the feature vector x_i^t. d is the dimension of the feature vector. *E* is the detection error of phishing attacks by feature vector x_i^t. Any feature vector that minimizes the value of the objective function has more merit in the WSO algorithm.

3.5 Classification with LSTM

LSTM neural network has gates named forgetting gate, input gate, and output gate. Oblivion gate is for forgetting the unnecessary information of the past. The input gate is for storing information at time t. The output gate is so that all the information in Ct is not transferred to the output ht. Each gate has two inputs, which are xt and ht-1, and the two inputs are multiplied in two fully connected layers and then added together and finally passed through the sigmoid function. The LSTM network has four times the parameter and calculation cost of the RNN network. Bidirectional recurrent neural networks combine two independent neural networks. This structure allows networks to have forward and backward information about the sequence at each time step. Using the Bi-LSTM network makes the mode and status switch from the future to the past and from the past to the future. In a backward-running LSTM network, you retain future information. With the Bi-LSTM network, it is possible to preserve information from the past and the future at any time. Figure 3.6 shows the structure of the Bi-LSTM neural network and its cells.

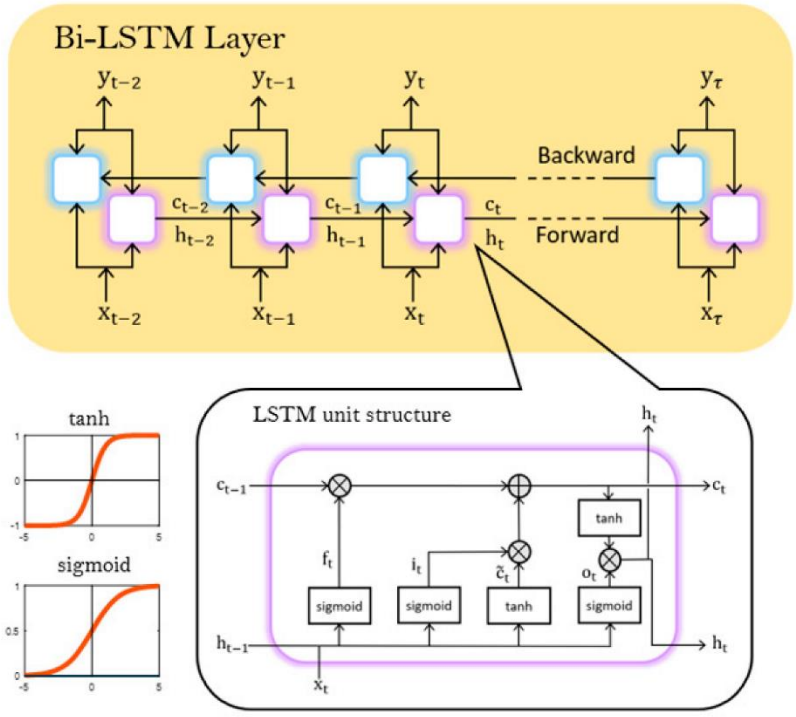

Figure 3.6 Bi-LSTM structure and LSTM neural network cell structure (Oh *et al.* 2022)

Equations (3.25), (3.26), (3.27), (3.28), (3.29), (3.30), (3.31), and (3.32), show the modeling of an LSTM cell is formulated.

$$W = \begin{bmatrix} W_f \\ W_i \\ W_c \\ W_o \end{bmatrix}, b = \begin{bmatrix} b_f \\ b_i \\ b_c \\ b_o \end{bmatrix} \tag{3.25}$$

$$\sigma(\alpha) = \frac{1}{1+e^{-\alpha}}, \tanh(\alpha) = \frac{e^{\alpha}-e^{-\alpha}}{e^{\alpha}+e^{-\alpha}} \tag{3.26}$$

$$f_t = \sigma\left(W_f \cdot [x_t, h_{t-1}] + b_f\right) \tag{3.27}$$

$$i_t = \sigma(W_i \cdot [x_t, h_{t-1}] + b_i) \tag{3.28}$$

$$\tilde{c}_t = \tanh(W_c \cdot [x_t, h_{t-1}] + b_c) \tag{3.29}$$

$$c_t = f_t \times c_{t-1} + i_t \times \tilde{c}_t \tag{3.30}$$

$$o_t = \sigma(W_o \cdot [x_t, h_{t-1}] + b_o) \tag{3.31}$$

$$h_t = o_t \times \tanh(c_t) \tag{3.32}$$

3.6 Pseudocode Proposed

The pseudocode of the proposed CNN-WSO-LSTM method is shown in Figure 3.7 to detect phishing attacks. In the proposed method, to detect phishing attacks at first, a set of URLs of fake and legal pages is considered input. Phishing datasets are often unbalanced because the number of phishing samples is far less than legal ones. Several artificial examples of fake URLs are created and added to the data set by the GAN deep learning method to solve this challenge.

In the next phase, balanced samples are used to train the CNN neural network. In the next step, the CNN neural network extracts the primary features, which are finally delivered to the feature selection phase. The essential features are selected and delivered to the LSTM neural network with the WSO binary algorithm in the feature selection stage. The role of the LSTM neural network is to classify URLs into two categories: phishing and regular. In the proposed code network, the following steps are provided to detect phishing attacks:

- Data set normalization with GAN deep learning technique
- Feature extraction with deep learning based on the CNN network
- Feature selection with a binary version of the WSO algorithm
- Reducing the dimensions of the samples with the optimal feature vector
- LSTM neural network training
- Evaluation of the proposed model in detecting phishing attacks with test samples

Table 3.1 shows the pseudocode of the proposed CNN-WSO-LSTM method

Table 3.1 Pseudocode of the proposed CNN-WSO-LSTM method

Setting parameters and t=1, generating artificial URL samples with **GAN** and balancing the dataset

Training CNN network on URLs for feature extraction

Coding feature vectors as population members of the **WSO** algorithm

Generate feature vectors as random population from **WSO** algorithm

Evaluation of feature vectors with the objective function of feature selection and selection of the most optimal feature vector

while (**t< Maxt**) **do**

Update the parameters **v, p1, p2, μ, a, b, w0, f, mv** and **Ss**

For i = 1 **to** n **do**

$$v_i^{t+1} = \mu[v_i^t + p_1(X_{gbest} - x_i^t) \times c_1 + p_2(X_{pbest}^i - x_i^t) \times c_2]$$

end for

for i = 1 **to** n **do**

if rand < **mv** then

$$x_i^{t+1} = x_i^t . \neg \oplus x_0 + u.a + lb$$

else

$$x_i^{t+1} = x_i^t + \frac{v_i^t}{f}$$

end if

end for

for i = 1 to n **do**

if rand ≤ Ss **then**

if i == 1 **then**

$$x_i^{t+1} = x_{gbest} + r_1 \times \vec{D} \times sgn(r_2 - 0.5)$$

else

$$x'^{t+1}_i = x_{gbest} + r_1 \times \vec{D} \times sgn(r_2 - 0.5)$$

$$x_i^{t+1} = \frac{x'^{t+1}_i + x_i^t}{2 \times rand}$$

end if

end if

end for

Evaluate and update the new feature vectors

t = t + 1

end while

LSTM training with optimal feature vector and evaluation of the proposed model

3.7 Dataset

In this paper, the set of URLs is collected from the sources of the ISCX-URL-2016 dataset and the Phishtank dataset (Prabakaran *et al.* 2023, Bu and Kim 2022). The number of data set samples has been balanced using the GAN neural network. The dataset has 20 thousand legal samples and 20 phishing samples. The proposed method has also produced 10,000 real phishing examples and 10,000 artificial phishing examples. In the proposed method, common URL parts, such as "http://", "https://" and "www" have been deleted.

3.8 Evaluation Metrics

To evaluate the proposed method, evaluation indices such as accuracy, sensitivity, and precision, which are formulated according to Equations (4.1), (4.2) and (4.3) are used.

$$Accuracy= (TP+TN)/ (TP+TN+FP+FN) \quad (4.1)$$

$$Sensitivity=Recall=TP/ (TP+FN) \quad (4.2)$$

$$Precision=TP/ (TP+FP) \quad (4.3)$$

TP, *TN*, *FP*, and *FN* parameters are defined as follows:

- True positive (TP): The URL example is of the phishing type and is classified in the phishing category.
- False positive (FP): The URL sample is of legitimate type and is wrongly classified in the phishing category.
- True negative (TN): The URL sample is of legal type and is classified in the legal category.
- False negative (FN): The URL sample is of phishing type and is wrongly classified in the legal category.

4. RESULTS AND DISCUSSION

In this section implements the proposed method for detecting phishing attacks in MATLAB and Python. The tests performed in this section are implemented and compared with similar methods.

MATLAB and Python software and libraries such as Keras and Tensorflow have been used to implement the proposed method. In the implementations, the training data size is set to 70% of the total data, 15% for test data, and 15% for validation data. The structure of the convolutional neural network is according to (Zhang *et al.* 2015). The normalization range of the data set is in the range [0,1], the number of feature vectors or population of the WSO algorithm is equal to 20, and the number of repetitions is equal to 100. Parameters c1 and c2 are random numbers in the interval [0,1]. The parameters pmin and pmax in the WSO algorithm have values of 0.5 and 1.5, respectively. The coefficient of τ in the WSO algorithm is set equal to 4.125. Table 4.1 and Table 4.2 show the proposed method's accuracy, precision, and sensitivity for detecting ISCX-URL-2016 and Phishtank phishing attacks.

Table 4.1 Evaluation metrics of the proposed method and deep learning on the ISCX-URL-2016 dataset

METHOD	ACCURACY	PRECISION	SENSITIVITY
LSTM	95.82	94.63	95.44
CNN	95.82	94.83	93.39
CNN-LSTM	96.14	95.54	94.21
CNN-WSO-LSTM(proposed Method)	97.94	97.82	97.76

Table 4.2 Evaluation metrics of the proposed method and deep learning on the Phishtank dataset

METHOD	ACCURACY	PRECISION	SENSITIVITY
LSTM	92.21	91.13	90.18
CNN	91.64	89.83	90.08
CNN-LSTM	92.31	91.27	91.14
CNN-WSO-LSTM(Proposed Method)	96.78	95.67	95.71

The proposed method has been compared with LSTM, CNN, and CNN-LSTM methods for comparison and evaluation. The CNN-LSTM network is also a model of the proposed method whose feature selection phase is removed. For a better analysis, the results of the proposed method have been compared with deep learning methods visually and in Figure 4.1 and Figure 4.2. Experiments show that in the ISCX-URL-2016 data set, LSTM deep learning method in detecting phishing attacks has accuracy, precision, and sensitivity of 95.82%, 94.63%, and 95.44%, respectively. CNN's deep learning method in detecting phishing attacks has accuracy, precision, and sensitivity equal to 95.82% and 94.83%, respectively. It is 93.39%.

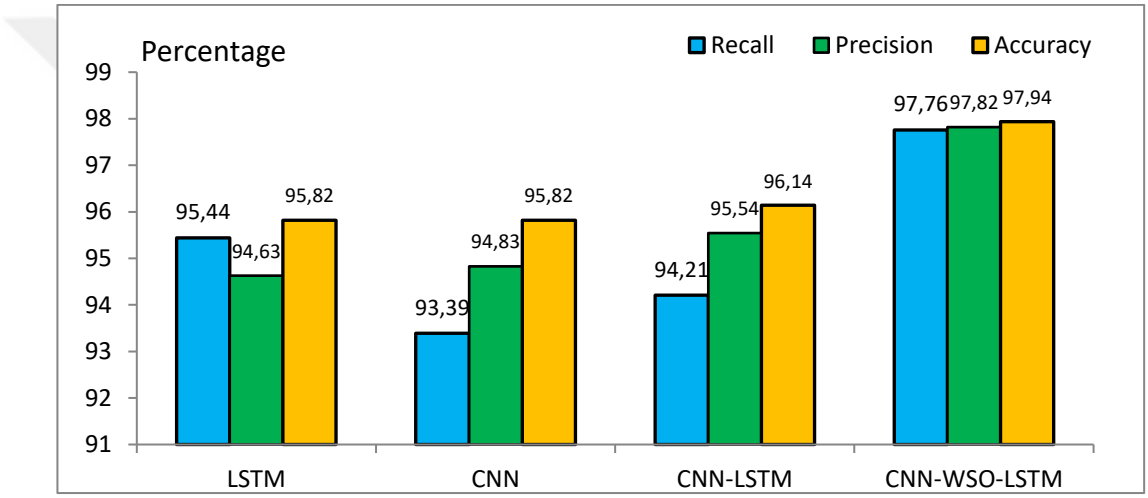

Figure 4.1 Comparison of the evaluation metrics of the proposed method with several deep learning methods in the ISCX-URL-2016 dataset

The accuracy, precision, and sensitivity of the CNN-LSTM method in the ISCX-URL-2016 dataset for detecting attacks are 96.12%, 95.84%, and 94.21%, respectively. The proposed method or CNN-WSO-LSTM in detecting phishing attacks has an accuracy of 97.94%, 97.82%, and 97.76%, respectively. Compared to the CNN-LSTM method, the proposed method has improved the accuracy, precision, and sensitivity index by 1.77%, 1.01%, and 3.55%, respectively, due to the intelligent selection of features by the WSO algorithm.

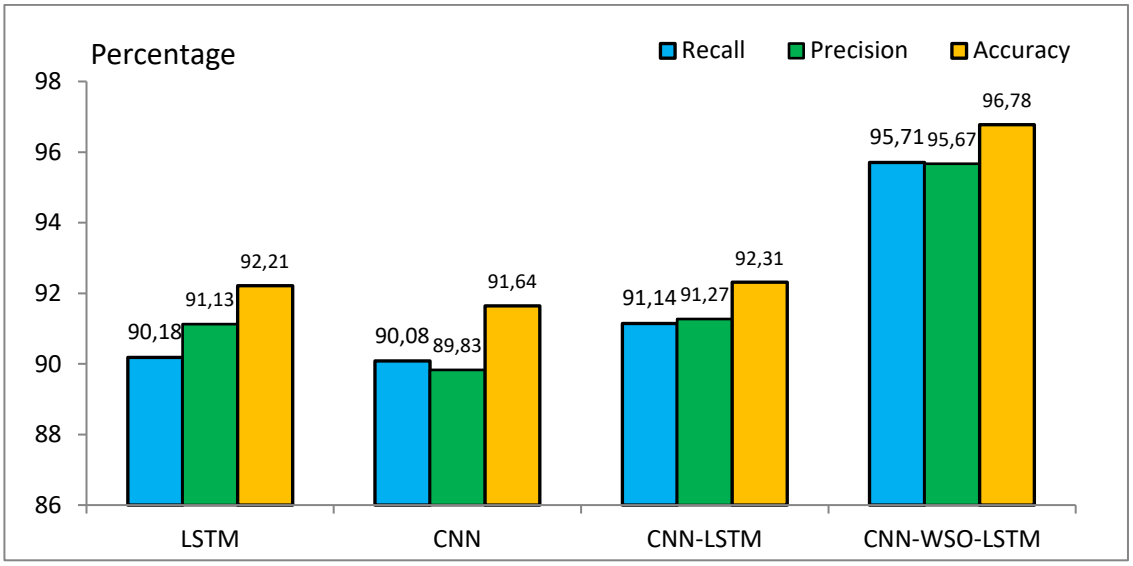

Figure 4.2 Comparing the evaluation metrics of the proposed method with several deep learning methods in the PhishTank dataset

In the Phishtank dataset, the accuracy, precision, and sensitivity of LSTM are 92.21%, 91.13%, and 90.18%, respectively. CNN's accuracy, precision, and sensitivity index in detecting phishing attacks are 91.64%, 89.83%, and 90.08%, respectively. The accuracy, precision, and sensitivity index of CNN-LSTM are 92.31%, 91.27%, and 91.14%, respectively. In the Phishtank dataset, the proposed method's accuracy, precision, and sensitivity in detecting attacks are 96.78%, 95.67%, and 95.71%, respectively. The proposed method for detecting phishing attacks is based on deep learning, machine learning, and meta-heuristic algorithms. For a more detailed evaluation of the proposed method, its efficiency has been evaluated with modern meta-heuristic methods in detecting phishing attacks in MATLAB. In Figure 4.3, Figure 4.4, and Figure 4.5, respectively, the index of accuracy, precision, and sensitivity of the proposed method is compared with several meta-heuristic algorithms for detecting phishing attacks. The implementation of the swarm intelligence methods of WOA (Riyahi *et al.* 2022), HHO (Peng *et al.* 2023)), and JSO (Chou *et al.* 2021) for feature selection in MATLAB shows that the proposed method has better indicators for detecting phishing attacks.

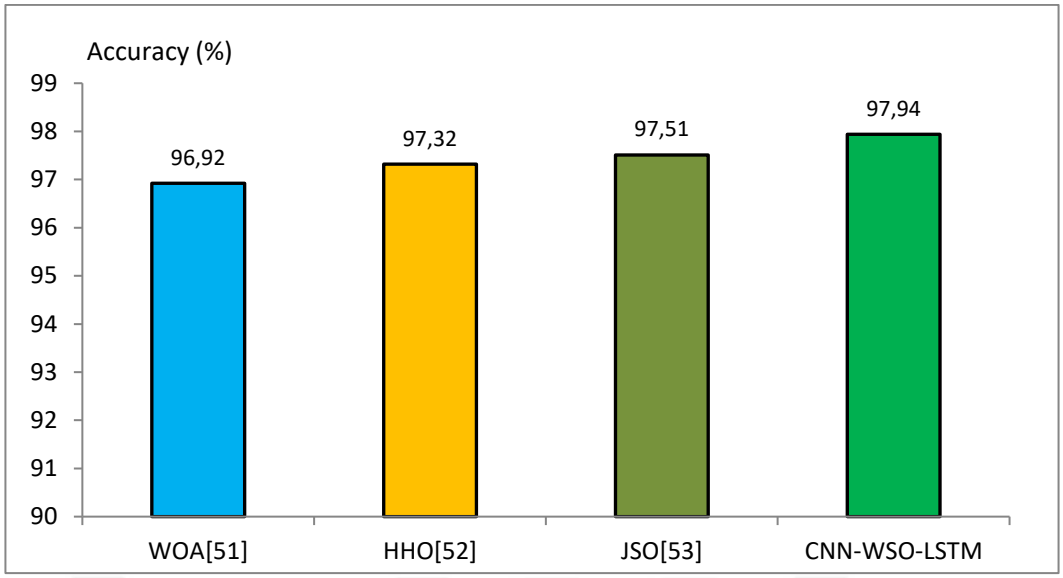

Figure 4.3 Comparison of the accuracy index of the proposed method and feature selection methods in the ISCX-URL-2016 dataset

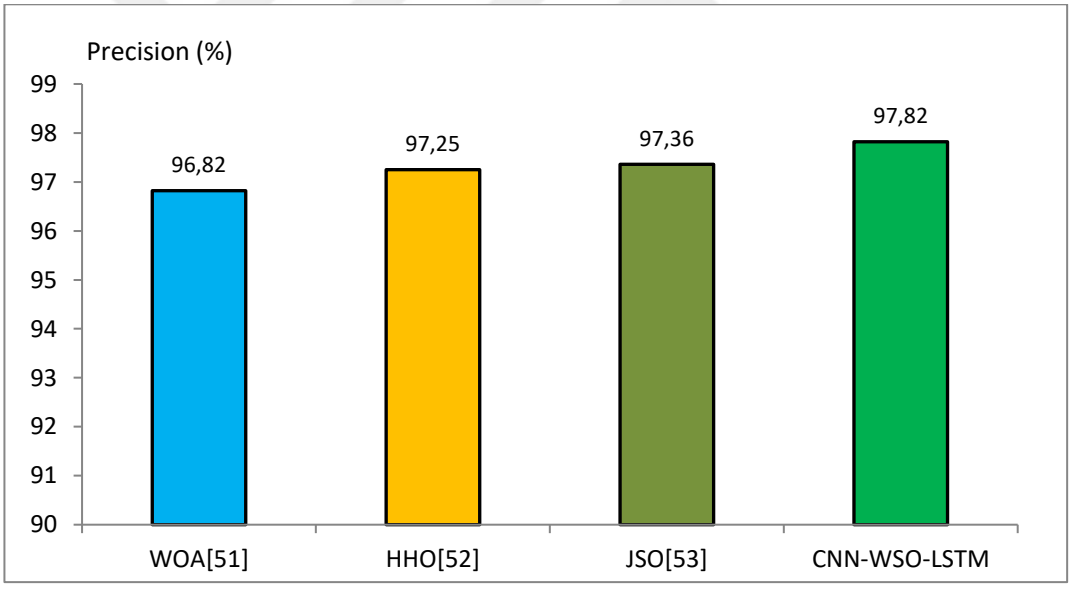

Figure 4.4 Comparison of the precision index of the proposed method and feature selection methods in the ISCX-URL-2016 dataset

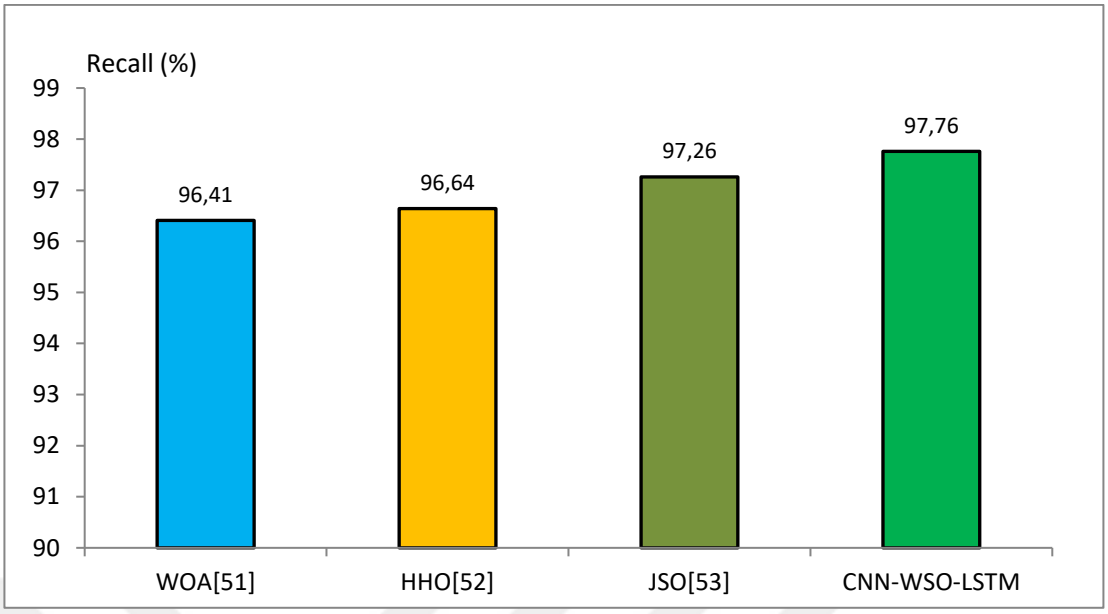

Figure 4.5 Comparison of the sensitivity index of the proposed method and feature selection methods in the ISCX-URL-2016 dataset

Experiments show that WOA, HHO, and JSO methods in detecting phishing attacks have an accuracy of 96.92%, 97.32%, and 97.51%, respectively, and the proposed method is more accurate than the compared methods and is around 97.94%. The precision index of the proposed method for detecting attacks in WOA, HHO, and JSO is 96.82%, 97.25%, and 97.36%, respectively, and the accuracy of the proposed method is 97.82%. The sensitivity index of the WOA, HHO, and JSO methods is 96.41%, 96.64%, and 97.26%, respectively, and the sensitivity of the proposed method is 97.76%. Experiments and evaluation show that the proposed method is more successful in detecting phishing attacks than WOA, HHO, and JSO feature selection and meta-heuristic algorithms regarding accuracy, sensitivity, and precision.

The proposed method has the lowest error for detecting phishing attacks among the feature selection methods. The worst performance in these tests is related to the WOA algorithm detecting phishing attacks. The reasons for the effectiveness of the proposed method in the feature selection phase for detecting phishing attacks are as follows:

- Unlike the WOA, HHO, and JSO algorithms, the WSO algorithm has a velocity vector and can change the direction of movement according to the problem conditions.

- The WSO algorithm initially has a global search mechanism, and then the search process is dynamically changed to a local type.
- Various search behaviors in the WSO algorithm make the feature space well-searched.

An important indicator for evaluating meta-heuristic algorithms is the measurement of the number of selected features in detecting phishing attacks. The number of features selected by the proposed method in different datasets (Mohammad *et al.* 2014) has been compared with meta-heuristic methods WOA, HHO, and JSO. Unlike the PishTank dataset, the UCI and Tan datasets do not require feature extraction because they each have 30 and 48 selected features, respectively. In the diagram of Figure 4.6, the average number of features selected in two datasets in the proposed method and WOA, HHO, and JSO algorithms are displayed.

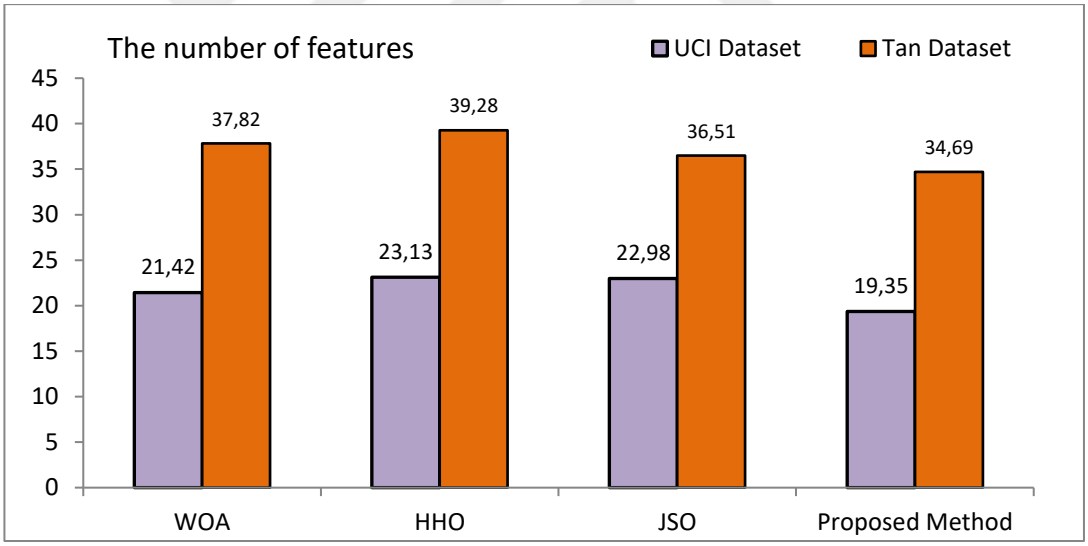

Figure 4.6 Comparison of the average number of features selected in the proposed method with feature selection methods

The analysis of the proposed method shows that the proposed method has succeeded in selecting 19.35 features from the 30 primary features in the UCI dataset. WOA, HHO, and JSO algorithms have selected 21.42, 23.13, and 22.98 features in the UCI dataset, respectively. The evaluations show that among the compared methods in the UCI data set, the proposed method has more dimensionality reduction than WOA, HHO, and JSO

algorithms. In the Tan data set, the number of features selected by WOA, HHO, and JSO algorithms and the proposed method has selected 37.82, 39.28, 36.51, and 34.69 features, respectively.

The dimensionality reduction in the proposed method in the UCI and Tan datasets is 35.5% and 27.72%, respectively. The classification input dimensions have been reduced more than the WOA, HHO, and JSO algorithms. In Table 4.3, the proposed method in the phase of feature extraction, feature selection, and classifier has been compared with several deep learning methods in two datasets (Bu and Kim 2022).

Table 4.3 Comparison of the proposed method with deep learning methods in ISCX-URL-2016 and phishtank

DATASET	**ISCX-URL-2016**		**PHISHTANK**	
Metrics	Acc**(%)**	Recall**(%)**	Acc**(%)**	Recall**(%)**
Character-CNN (Bu and Kim 2022)	0.9363	0.8909	0.8852	0.8034
LSTM (Iuga *et al.* 2016)	0.9175	0.8803	0.8544	0.7865
CNN-LSTM (Bu and Kim 2022)	0.9424	0.9015	0.9070	0.8374
URLNet (Le *et al.* 2018)	0.9450	0.9390	0.9226	0.8785
Texception Net (Tajaddodianfar *et al.* 2020)	0.9765	0.9462	0.9319	0.9075
CNN+GA (Bu and Kim 2022)	0.9685	0.9510	0.9483	0.9081
Proposed Method	97.94	97.76	96.78	95.71

The proposed method is also compared with (Prabakaran *et al.* 2023) methods presented in 2023 in the ISCX-URL-2016 data set according to Table 4.4.

Table 4.4 Comparison of the proposed method with deep learning methods on the ISCX-URL-2016 dataset

MODEL	**ACCURACY (%)**	**PRECICSION (%)**	**RECALL (%)**
AE-DNN (Prabakaran *et al.* 2023)	91.45	92.77	90
Deep AE-DNN (Prabakaran *et al.* 2023)	93.25	94.39	92.02
Denoising AE-DNN (Prabakaran *et al.* 2023)	95.15	96.04	94.22
Sparse AE-DNN(Prabakaran *et al.* 2023)	94.85	95.83	93.82
Convolutional AE-DNN (Prabakaran *et al.* 2023)	95.91	96.91	94.88
Contractive AE-DNN(Prabakaran *et al.* 2023)	96.55	97.02	96.08
VAE – DNN (Prabakaran *et al.* 2023)	97.45	97.89	97.20
Proposed Method	97.94	97.82	97.76

The proposed method has been compared with deep learning methods in the accuracy index in two datasets, ISCX-URL-2016 and PhishTank. The accuracy index of the proposed method is higher than Character-CNN, LSTM, CNN-LSTM, URLNet, TexceptionNet, and CNN+GA in detecting phishing attacks.

The proposed method in the ISCX-URL-2016 dataset has more accuracy, precision, and sensitivity than AE-DNN, Deep AE-DNN, Denoising AE-DNN, Sparse AE-DNN, Convolutional AE-DNN, Contractive AE-DNN is VAE – DNN. The proposed method is more successful than the VAE-DNN method in the accuracy and sensitivity index in detecting phishing attacks. The VAE-DNN method is more successful than the proposed method in the accuracy index.

5. CONCLUSIONS AND FUTURE WORKS

Phishing attacks are one of the main challenges for users on the Internet. Phishing attacks steal users' information, such as their usernames and passwords. Estimates show that phishing attacks cost millions of dollars annually to online payment services and internet users. Machine learning and deep learning methods are essential for detecting phishing attacks. Deep learning methods can detect zero-day attacks. Deep learning methods to detect phishing attacks face many challenges. One of the challenges of detecting phishing attacks is the imbalance between fake and legal samples. In most datasets, the number of fake or phishing samples is in the minority, which makes the dataset unbalanced. Deep learning on an unbalanced dataset increases the detection error of phishing attacks. Another challenge of machine learning and deep learning methods is feature engineering in the feature extraction and selection phase. Failure to extract basic features from URLs and failure to select intelligent features reduces the accuracy of deep learning methods in detecting phishing attacks.

This paper presents a new approach based on machine learning, deep learning, and swarm intelligence to solve the challenges of deep learning and machine learning in detecting phishing attacks. The proposed method for balancing fake and original samples uses GAN deep learning technique. The Character-CNN neural network is used for feature extraction. The proposed method introduces URLs as a new matrix and numerical coding as CNN input. The feature vector extracted by CNN is used as the input of the feature selection method. The binary version of the WSO algorithm for feature selection is presented in the proposed method. In the fully connected layer in CNN, the LSTM classifier is used to classify samples into normal and attack categories.

Experiments are performed on two data sets, UCI and Tan, which do not require feature extraction, and two sets, ISCX-URL-2016 and Phishtank, which require feature extraction.

Tests on the UCI and Tan datasets show that the proposed method has reduced the number of features by 35.5% and 27.72%, respectively. The proposed method has selected fewer features in phishing detection than WOA, HHO, and JSO algorithms.

The proposed method in the ISCX-URL-2016 dataset has accuracy, precision, and sensitivity of 97.94%, 97.82%, and 97.76%, respectively. The proposed method in the PhishTank dataset has accuracy, precision, and sensitivity of 96.78%, 95.67%, and 95.71%, respectively. The proposed method is more accurate than LSTM, CNN, and CNN-LSTM methods in ISCX-URL-2016 and Phishtank datasets. The proposed method is more accurate in detecting attacks than the combined deep learning methods with swarm intelligence, such as the CNN+GA method. The proposed method is more accurate in detecting phishing attacks than deep learning hybrid techniques such as DNN, VAE-DNN, and AE-DNN.

The proposed method for detecting phishing attacks has the following advantages:

- Data set balancing with GAN deep learning
- Coding of URLs strings in the form of a numerical matrix and according to CNN input structure
- Extracting the features of URLs with deep learning based on traversing URL characters
- Intelligent selection of selected CNN features with WSO swarm intelligence
- Optimizing CNN neural network output with WSO algorithm and optimal selection of features to reduce attack detection error
- High accuracy of the proposed model in detecting phishing attacks
- Ability to detect zero-day attacks
- Evaluation of the proposed method on four different datasets

The relatively long time to train the model and the complexity of the model in the training phase is one of the challenges of the proposed method. In future works, Apache Spark architecture will be used as a distributed architecture to accelerate the proposed method's

training and reduce the training time. In future works, embedded learning will be used in the fully connected CNN layer to improve the performance of the proposed method.

DDoS attacks can be discovered primarily using two techniques: in-line packet inspection of all messages, and out-of-band detection using traffic flow record analysis. Either strategy can be implemented on-site or through cloud services. In future we can use the LSTM deep learning to train the system and use the trained networ to test the data. Also, we can use the other methaheuristic method, to select the best features and use to train the LSTM deep learning. Also, we can use the IoT to obtaine the attached data to find the method to classificying it.

REFERENCES

Adane, K. and Beyene, B. 2023. Phishing website detection with and without proper feature selection techniques: Machine learning approach. In Advances in Intelligent Systems, Computer Science and Digital Economics IV, pp. 745-756, Switzerland.

Ahmed, D. S., Hussein, A. P. D. K. Q. and Abdulalah, H. A. 2022. Phishing websites detection model based on decision tree algorithm and best feature selection method. Turkish Journal of Computer and Mathematics Education, 13(1): 100-107.

Aljabri, M. and Mirza, S. 2022. Phishing attacks detection using machine learning and deep learning models. In 2022 7th International Conference on Data Science and Machine Learning Applications, pp. 175-180. IEEE.

Aljofey, A., Jiang, Q., Rasool, A., Chen, H., Liu, W., Qu, Q. and Wang, Y. 2022. An effective detection approach for phishing websites using URL and HTML features. Scientific Reports, 12(1): 8842.

Al-Qahtani, A. F. and Cresci, S. 2022. The covid-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. IET Information Security, 16(5): 324-345.

Alshehri, M., Abugabah, A., Algarni, A. and Almotairi, S. 2022. Character-level word encoding deep learning model for combating cyber threats in phishing URL detection. Computers and Electrical Engineering, 100: 107868.

Anuar, M. A. H., Redzuan, F., Wan Adnan, W. A., Vincent, R. J., Sagir, A., Abdul-Hamid, F. and Abbas, M. S. 2022. A Preliminary investigation on user factors of phishing e-mail. Central Asia and the Caucasus, 23(1).

Asiri, S., Xiao, Y., Alzahrani, S., Li, S. and Li, T. 2023. A Survey of intelligent detection designs of HTML URL phishing attacks. IEEE Access.

Balogun, A. O., Mojeed, H. A., Adewole, K. S., Akintola, A. G., Salihu, S. A., Bajeh, A. O. and Jimoh, R. G. 2021. Optimized decision forest for website phishing detection, In: Data Science and Intelligent Systems: Proceedings of 5th Computational Methods in Systems and Software, pp. 568-582, Cham.

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z. and Kifayat, K. 2021. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76: 139-154.

Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Rodriguez-Galan, G., Martínez-Cepeda, V. and Nuñez-Agurto, D. 2023. Comparative study of deep learning algorithms in the detection of phishing attacks based on HTML and text obtained from web pages. In Applied Technologies: 4th International Conference, ICAT 2022, pp. 386-398, Switzerland.

Bountakas, P. and Xenakis, C. 2023. Helphed: Hybrid Ensemble Learning Phishing Email Detection. Journal of Network and Computer Applications, 210: 103545.

Bozkir, A. S., Dalgic, F. C. and Aydos, M. 2023. GramBeddings: A new neural network for URL based identification of phishing web pages through n-gram embeddings. Computers & Security, 124: 102964.

Braik, M., Hammouri, A., Atwan, J., Al-Betar, M. A. and Awadallah, M. A. 2022. White shark optimizer: A novel bio-inspired meta-heuristic algorithm for global optimization problems. Knowledge-Based Systems, 243: 108457.

Bu, S. J. and Kim, H. J. 2022. Optimized URL feature selection based on genetic-algorithm-embedded deep learning for phishing website detection. Electronics, 11(7): 1090.

Buckley, J., Lottridge, D., Murphy, J. G. and Corballis, P. M. 2023. Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. International Journal of Human-Computer Studies, 102996.

Chou, J. S. and Truong, D. N. 2021. A novel metaheuristic optimizer inspired by behavior of jellyfish in ocean. Applied Mathematics and Computation, 389: 125535.

Da Silva, C. M. R., Feitosa, E. L. and Garcia, V. C. 2020. Heuristic-based strategy for Phishing prediction: A survey of URL-based approach. Computers & Security, 88: 101613.

Daengsi, T., Pornpongtechavanich, P. and Wuttidittachotti, P. 2021. Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Education and Information Technologies, 1-24.

Divakaran, D. M. and Oest, A. 2022. Phishing detection leveraging machine learning and deep learning: A review, IEEE, 20(5): 86 - 95.

Guo, B., Zhang, Y., Xu, C., Shi, F., Li, Y. and Zhang, M. 2021. HinPhish: An effective phishing detection approach based on heterogeneous information networks. Applied Sciences, 11(20): 9733.

Hijji, M. and Alam, G. 2021. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. IEEE Access, 9: 7152-7169.

Hota, H. S., Sharma, D. and Shrivas, A. 2022. An integrated approach of proposed pruning based feature selection technique (PBFST) for phishing e-mail detection. Recent Advances in Computer Science and Communications,15(5): 683-692.

Iuga, C., Nurse, J. R. and Erola, A. 2016. Baiting the hook: factors impacting susceptibility to phishing attacks. Human-centric Computing and Information Sciences, 6: 1-20.

Le, H., Pham, Q., Sahoo, D. and Hoi, S. C. 2018. URLNet: Learning a URL representation with deep learning for malicious URL detection, In: Conference 2017, pp. 1-13, Washington,

Lin, Z., Feng, M., Santos, C. N. D., Yu, M., Xiang, B., Zhou, B. and Bengio, Y. 2017. A structured self-attentive sentence embedding, In: 5th International Conference on Learning Representations, pp. 1-15, China.

Makhadmeh, S. N., Al-Betar, M. A., Assaleh, K. and Kassaymeh, S. 2022. A hybrid white shark equilibrium optimizer for power scheduling problem based IoT. IEEE Access, 10: 132212-132231.

Mohammad, R. M., Thabtah, F. and McCluskey, L. 2014. Intelligent rule-based phishing websites classification. IET Information Security, 8(3): 153-160.

Nepal, S., Gurung, H. and Nepal, R. 2022. Phishing URL Detection Using CNN-LSTM and Random Forest Classifier, pp. 1-15, USA.

Nordin, N. S. and Ismail, M. A. 2023. A hybridization of butterfly optimization algorithm and harmony search for fuzzy modelling in phishing attack detection. Neural Computing and Applications, 35(7): 5501-5512.

Oest, A., Safaei, Y., Zhang, P., Wardman, B., Tyers, K., Shoshitaishvili, Y., and Ahn, G. J. 2020. Phishtime: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. In Proceedings of the 29th USENIX Conference on Security Symposium, pp. 379-396.

Oh, S., Yu, M., Cho, S., Noh, S. and Chun, H. 2022. Bi-LSTM-augmented deep neural network for nulti-gbps VCSEL-based visible light communication link. Sensors, 22(11): 4145.

Paturi, R., Swathi, L., Pavithra, K. S., Mounika, R. and Alekhya, C. 2022. Detection of phishing attacks using visual similarity model. In 2022 International Conference on Applied Artificial Intelligence and Computing, pp. 1355-1361, IEEE.

Peng, L., Cai, Z., Heidari, A. A., Zhang, L. and Chen, H. 2023. Hierarchical harris hawks optimizer for feature selection. Journal of Advanced Research 12(1):552-560.

Prabakaran, M. K., Chandrasekar, A. D. and Meenakshi, P. 2023. An enhanced deep learning-based phishing detection mechanism to effectively identify malicious URLs using variational autoencoders. IET Information Security 54(5):787-790.

Priya, S., Selvakumar, S. and Velusamy, R. L. 2022. PaSOFuAC: Particle swarm optimization based fuzzy associative classifier for detecting phishing websites. Wireless Personal Communications, 125(1): 755-784.

Rahman, A. U., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S. and Halim, Z. 2022. Discovering the correlation between phishing susceptibility causing data biases and big five personality traits using C-GAN. IEEE Transactions on Computational Social Systems, 8(10):458-566.

Raja, A. S., Pradeepa, G. and Arulkumar, N. 2022. Mudhr: Malicious URL detection using heuristic rules based approach. In AIP Conference Proceedings 2393(1): 020176.

Rambabu, V., Malathi, K. and Mahaveerakannan, R. 2022. An innovative method to predict the accuracy of phishing websites by comparing logistic regression algorithm with support vector machine algorithm, In: 2022 6th International Conference on Electronics, Communication and Aerospace Technology. pp 646-650, India.

Riyahi, M., Rafsanjani, M. K., Gupta, B. B. and Alhalabi, W. 2022. Multiobjective whale optimization algorithm-based feature selection for intelligent systems. International Journal of Intelligent Systems, 37(11): 9037-9054.

Roy, S. S., Awad, A. I., Amare, L. A., Erkihun, M. T. and Anas, M. 2022. Multimodel Phishing URL Detection Using LSTM, Bidirectional LSTM, and GRU Models. Future Internet, 14(11): 340.

Sabahno, M. and Safara, F. 2022. ISHO: improved spotted hyena optimization algorithm for phishing website detection. Multimedia Tools and Applications, 81(24): 34677-34696.

Shieh, C. S., Nguyen, T. T., Lin, W. W., Huang, Y. L., Horng, M. F., Lee, T. F. and Miu, D. 2022. Detection of adversarial DDoS attacks using generative adversarial networks with dual discriminators. Symmetry, 14(1): 66.

Shirazi, H., Muramudalige, S. R., Ray, I., Jayasumana, A. P. and Wang, H. 2023. Adversarial autoencoder data synthesis for enhancing machine learning-based phishing detection algorithms. IEEE Transactions on Services Computing, 16(4).

Shuaib, M., Abdulhamid, S. I. M., Adebayo, O. S., Osho, O., Idris, I., Alhassan, J. K. and Rana, N. 2019. Whale optimization algorithm-based email spam feature selection method using rotation forest algorithm for classification. SN Applied Sciences, 1: 1-17.

Siddiqi, M. A., Pak, W. and Siddiqi, M. A. 2022. A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12): 6042.

Tajaddodianfar, F., Stokes, J. W. and Gururajan, A. 2020. Texception: a character/word-level deep learning model for phishing URL detection. In ICASSP 2020-2020 IEEE International Conference on Acoustics Speech and Signal Processing, pp. 2857-2861, Spain.

Tan, C. C. L., Chiew, K. L., Yong, K. S., Sebastian, Y., Than, J. C. M. and Tiong, W. K. 2023. Hybrid phishing detection using joint visual and textual identity. Expert Systems with Applications, 119723.

Van D., B., Burda, P., Allodi, L. and Zannone, N. 2021. Combining text and visual features to improve the identification of cloned webpages for early phishing detection. In Proceedings of the 16th International Conference on Availability, Reliability and Security, page 1-10.

Wang, J. 2022. An improved genetic algorithm for web phishing detection feature selection. In 2022 Asia Conference on Algorithms, Computing and Machine Learning pp. 130-134. IEEE.

Wei, Y. and Sekiya, Y. 2022. Sufficiency of ensemble machine learning methods for phishing websites detection. IEEE, 10: 124103-124113.

Wen, T., Xiao, Y., Wang, A. and Wang, H. 2023. A novel hybrid feature fusion model for detecting phishing scam on Ethereum using deep neural network. Expert Systems with Applications, 211: 118463.

Xiao, X., Zhang, D., Hu, G., Jiang, Y. and Xia, S. 2020. CNN–MHSA: A convolutional neural network and multi-head self-attention combined approach for detecting phishing websites. Neural Networks, 125: 303-312.

Zahra, S. R., Chishti, M. A., Baba, A. I. and Wu, F. 2022. Detecting covid-19 chaos driven phishing/malicious URL attacks by a fuzzy logic and data mining based intelligence system. Egyptian Informatics Journal, 23(2): 197-214.

Zhang, X., Zhao, J. and LeCun, Y. 2015. Character-level convolutional networks for text classification. Advances in neural information processing systems, 28.

Zhu, E., Ju, Y., Chen, Z., Liu, F. and Fang, X. 2020. DTOF-ANN: an artificial neural network phishing detection model based on decision tree and optimal features. Applied Soft Computing, 95: 106505.

Zhu, E., Yuan, Q., Chen, Z., Li, X. and Fang, X. 2022. CCBLA: A lightweight phishing detection model based on CNN, biLSTM, and attention mechanism. Cognitive Computation, 1-14.

Zieni, R., Massari, L. and Calzarossa, M. C. 2023. Phishing or not phishing? A survey on the detection of phishing websites, IEEE Access, 11: 18499 - 18519.

CURRICULUM VITAE

Personal Information

Name and Surname : Abbas Jabr Saleh ALBAHADILI

Education

MSc	Çankırı Karatekin University Graduate School of Natural and Applied Sciences Department of Electronics and Computer Engineering	2021-2023
Undergraduate	Al- Qalam University College Faculty of Computer Engineering Department of Computer Engineering Techniques	2014-2017