

Phishing detection using grey wolf and particle swarm optimizer

Adel Hamdan¹, Muhannad Tahboush², Mohammad Adawy², Tariq Alwada'n³, Sameh Ghwanmeh⁴, Moath Husni⁵

¹Computer Science Department, The World Islamic Sciences and Education University, Amman, Jordan

²Information and Network Security, The World Islamic Sciences and Education University, Amman, Jordan

³Network and Cybersecurity Department, Teesside University, Middlesbrough, United Kingdom

⁴Computer Science Department, American University in the Emirates, Dubai, United Arab Emirates

⁵Software Engineering, The World Islamic Sciences and Education University, Amman, Jordan

Article Info

Article history:

Received Mar 12, 2024

Revised Jul 8, 2024

Accepted Jul 16, 2024

Keywords:

Feature selection

Grey wolf optimizer

Machine learning

Particle swarm optimizer

Phishing detection

ABSTRACT

Phishing could be considered a worldwide problem; undoubtedly, the number of illegal websites has increased quickly. Besides that, phishing is a security attack that has several purposes, such as personal information, credit card numbers, and other information. Phishing websites look like legitimate ones, which makes it difficult to differentiate between them. There are several techniques and methods for phishing detection. The authors present two machine-learning algorithms for phishing detection. Besides that, the algorithms employed are XGBoost and random forest. Also, this study uses particle swarm optimization (PSO) and grey wolf optimizer (GWO), which are considered metaheuristic algorithms. This research used the Mendeley dataset. Precision, recall, and accuracy are used as the evaluation criteria. Experiments are done with all features (111) and with features selected by PSO and GWO. Finally, experiments are done with the most common features selected by both PSO and GWO ($PSO \cap GWO$). The result demonstrates that system performance is highly acceptable, with an F-measure of 91.4%.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Adel Hamdan

Computer Science Department, The World Islamic Sciences and Education University

Amman, Jordan

Email: adel.hamdan@wise.edu.jo

1. INTRODUCTION

Phishing is a type of cybercrime, a serious attack, and an online crime in which an attacker sends several messages that seem and look to come from a trusted source. Usually, a uniform resource locator (URL) or a malicious attachment will be included in the email. Phishing tries to get and steal sensitive and valuable information such as usernames, credit card numbers, passwords, and credentials. If the operator clicks on the file, the phishing email will steal personal information, misuse user information, harm, or infect the computer with a virus [1]. In the last decades, the number of email advertisements has significantly increased. This growth leads to unauthorized access to users' sensitive information. Also, phishing emails have increased the damage to enterprise resources [2]. Also, the process of defending against phishing is recognized as cybersecurity, and defending internet-connected sources is cybersecurity's main objective [3]–[5].

Most organizations have improved their resources to combat potential damage from phishing and security breaches. However, effective phishing challenges have had an increased impact on international finance. Also, the risk for users and organizations still needs more protection and investigation [6].

Uniform resource locator (URL) is an address that represents the location of a website. We connect to the database stored on the server by accessing any URL. URLs are divided into two categories: malicious and benign. Malicious URLs are used for phishing and other harmful purposes, but benign URLs are harmless [7].

Cybersecurity has become more complicated since cyber-attacks have become more complicated and repeated. This complexity makes assessing, recognizing, and handling such events more complex. The anti-phishing working group (APWG) has detected more than 51,000 different phishing URLs. Also, based on the Rivest–Shamir–Adleman (RSA) examination, phishing hit the price of worldwide enterprises by \$9 billion in 2016 [8]. Figure 1 illustrates the phishing report by APWG in the first quarter of 2023 [9].

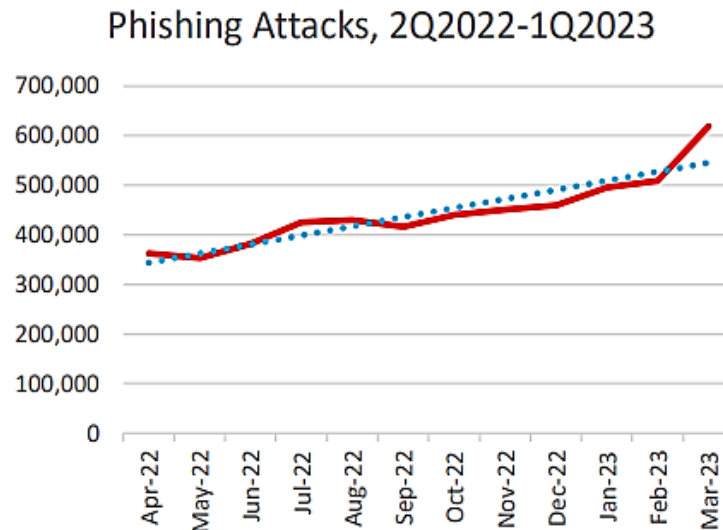


Figure 1. APWG phishing activity report first quarter 2023

There are several strategies to fight phishing. The authors mainly categorize phishing detection into two categories: Awareness of users and software detection. Software detection has several methods and strategies, and one of these strategies is machine learning techniques [10]. Machine learning algorithms can be used for email classification, intrusion detection, phishing and spear phishing detection, and other cyber-attacks. Also, no doubt machine learning has a massive impact on almost every business, including phishing [11]–[13].

The rest of this study is ordered as follows: section 2 presents the author’s suggested model. Section 3 discusses the methods used in this research, such as literature review, feature selection methods, dataset, and machine learning algorithms. Section 4 presents experiments and results. The last section, section 5, presents this research conclusion and future work.

2. THE PROPOSED MODEL

The authors of this investigation will use particle swarm optimization (PSO) and grey wolf optimizer (GWO) to select features. PSO and GWO will be used to reduce the number of features to reduce complexity and time consumption. Then, two machine learning classifiers will be used. Machine learning classifiers used in this work are XGBoost and random forest (RF). The dataset used in this study consists of 111 features, and this number of features is huge and can be reduced using such metaheuristic algorithms. PSO and GWO reduced the number of features from 111 to 55 and 59, respectively. Also, in this study, authors use the most common features selected by both PSO and GWO ($PSO \cap GWO$). Figure 2 presents the proposed model.

The contribution of this paper can be summarized into the following points: using particle swarm optimization and grey wolf optimizer for feature selection with the Mendeley dataset for phishing detection, using features intersection of PSO and GWO ($PSO \cap GWO$) for phishing detection, and applying XGBoost and RF for phishing detection.

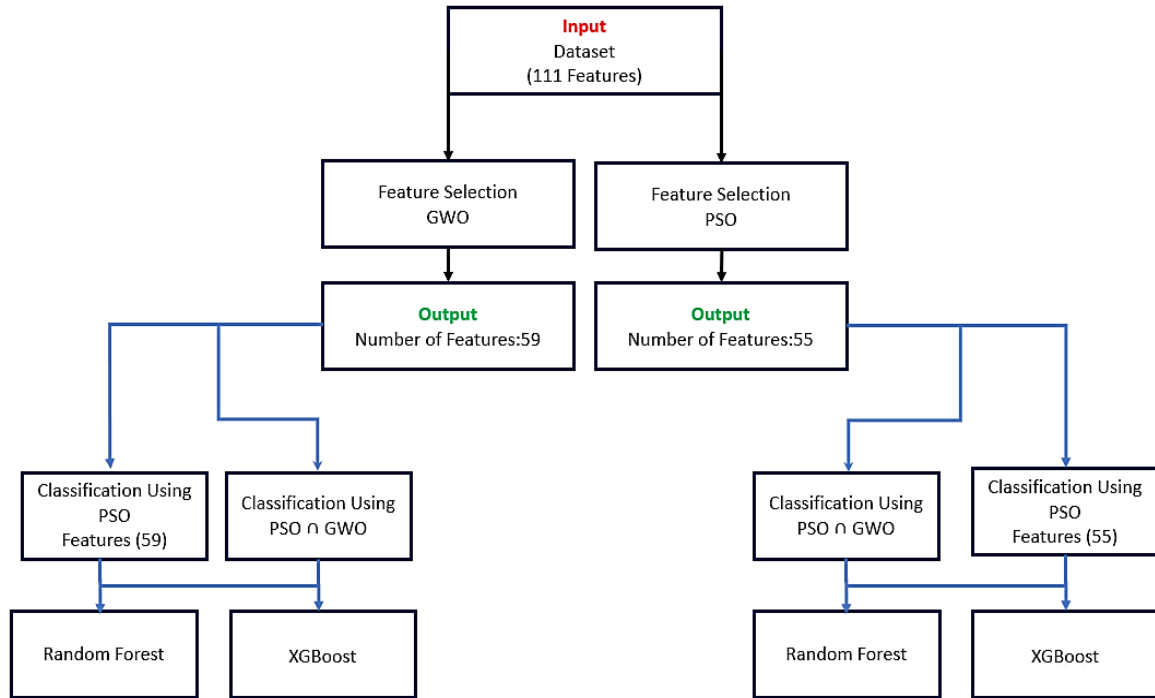


Figure 2. The proposed model

3. METHOD

In this section, the literature review for this research will be presented. Also, different methods for intrusion detection use different types of datasets. Besides that, feature selection methods such as PSO and GWO will be shown. In addition, machine learning algorithms used in this research will be presented. Finally, the dataset used in this research will be presented.

3.1. Literature review

Sahingoz *et al.* [14] presented a real-time anti-phishing approach. Also, seven classifications and natural language processing algorithms are implemented. Besides that, a new dataset is assembled in this work. The constructed dataset contains 37,375 URLs. The dataset contains 36,400 legitimate websites and 37,175 illegitimate. Also, the random forest algorithm with only one natural language processing shows the best results with a 97.98% correctness rate.

Yi *et al.* [15] focus on employing a deep learning frame to detect phishing. Two types of features for web phishing are used. Besides, a recognition type based on deep belief networks (DBN) is introduced. A big dataset to test DBN is used, and the true positive rate (TPR) is approximately 90%.

Alshingiti *et al.* [16] propose three different deep-learning methods to identify phishing. Also, convolutional neural network (CNN), long short-term memory (LSTM), and LSTM-CNN are proposed to detect URL websites. This research shows that CNN is better than LSTM-CNN and LSTM in terms of correctness. The dataset used in this research contains 20,000 records and 80 features.

Mahajan and Siddavatam [17] use machine learning equipment for phishing detection by extracting different features of legitimate and illegitimate URLs. Several algorithms are used in this work, such as decision trees, random forests, and support vector machines. The dataset used in this research was composed of *www.alexacom*, and the URLs of phishing data were assembled from *www.phishtank.com*. Results in this research show a 97.14 accuracy rate using random forest.

Alshahrani *et al.* [18] suggested a detection model that uses data mining with PSO to increase the method of phishing detection. Feature selection is conducted based on various techniques. The dataset in this research consists of 10,000 URLs. 6,000 genuine connections and 4,000 phishing URLs. Finally, all the classifiers have given more than 91% accuracy.

Sakunthala and Shankar [19], in this research, probabilistic latent semantic and greedy levy gradient boosting (PLS-GLGB) is suggested for detecting illegitimate websites using MapReduce. The dataset used was acquired from a phishing tank [20]. Results show meaningful amounts of phishing detection time and errors.

Adu-Manu *et al.* [21] examine tactics, procedures, and countermeasures of social engineering and phishing. They also displayed a comprehensive study of up-to-date social engineering methods used for phishing. Besides, necessary human attributes that put workers at risk of phishing attacks are presented.

Mosa *et al.* [22] present a survey of diverse machine learning techniques that conduct phishing challenges. The dataset set used consists of more than 11,000 websites from the Kaggle dataset. The algorithms used in this study are neural network (NN), naïve Bayes (NB), and adaptive boosting (AdaBoost). Accuracy achieved was 90.23%, 92.97%, and 95.43%, respectively.

Brindha *et al.* [23] present an intelligent Cuckoo Search (CS) algorithm with a deep learning-based phishing email recognition and categorization framework. The suggested model aims to classify the emails as either legitimate or illegitimate effectively. The implementation of the recommended model was evaluated using a standard dataset. The proposed model achieved 99.72% accuracy.

Aldakheel *et al.* [24] introduce an approach for finding phishing sites with acceptable accuracy. Authors utilize the convolution neural network (CNN) for accurate categorization that efficiently recognizes legitimate sites from phishing sites. The dataset used in this research is PhishTank. Also, the authors demonstrate that binary categorical loss and Adam optimizer are used, and the correctness of k-nearest neighbours (KNN), natural language processing (NLP), recurrent neural network (RNN), and random forest (RF) models are 87%, 97.98%, 97.4%, and 94.26%, respectively.

Ali and Malebary [25] propose PSO to successfully weigh diverse website features to achieve greater exactness. Experimental results show that PSO achieved good results. Several machine learning algorithms were used, such as back propagation neural network, support vector machine, k-nearest neighbour, decision tree, random forest, and naïve Bayes. The dataset used in this study is from the UCI machine learning repository, which contains 4,898 phishing and 6,157 legitimate. The number of features in this dataset is 30.

Jaber *et al.* [26] used a grey wolf optimizer to select the proper features for phishing classification. Results show a classification rate of 97.49%. The dataset used in this study is based on PhishTank, which has 112 features. and 100,000 URLs.

Gualberto *et al.* [27] suggested an attempt based on machine learning for phishing detection. The proposed model reaches an F1-measure 99.95% success rate using the XGBoost algorithm. The dataset used in this work was obtained from two collections of email Phishing Corpus. This research proposes two models. The first model uses all the features acquired from the document-term matrix (DTM), and the second model uses latent Dirichlet allocation (LDA).

3.2. Feature selection

Feature selection algorithms can be classified into three groups: wrapper-based, filter-based, and embedded. This research will employ PSO and GWO [28]–[30]. The aim of using feature selection is to reduce the number of features used for phishing detection.

3.2.1. Particle swarm optimization

Particle swarm optimization (PSO) algorithm can be used for optimization. PSO is motivated by the behaviour of united animals like birds or fish. PSO cannot guarantee a good solution. In PSO, particles move according to some simple formula [30]. Also, swarms travel in the search space to find the best result. If a better position or solution is found, the movement is done. This process is repeated until the optimal solution is found [31]–[33].

3.2.2. Gray wolf optimizer

Gray wolf optimizer (GWO) algorithm is a swarm intelligence algorithm. GWO obtained by Mirjalili *et al.* [34], emulated hierarchy and the chasing of grey wolves. In GWO, the types of wolves are alpha, beta, delta, and omega. Alpha is the dominant and the decision maker. Beta is the second-top group of individuals and helps alpha in making decisions. The third valuable group of entities is the delta. Finally, omega is the lowest level in the group. Alpha, beta, and delta lead the rest of the groups to find the best solution [34], [35].

3.3. Dataset

The Mendeley dataset is used for the Phishing websites dataset, consisting of a group of legitimate and phishing URLs. Each website is characterized by a set of features that donate. The dataset has two variants (full variant and small variant). In the full variant, the total number of instances is 88,647, the number of legitimate websites is 58,000, and the number of phishing URLs is 30,647. The entire number of features is 111. In the small variant, the total number of instances is 58,645, the number of legitimate websites is 27,998, and the number of illegitimate URLs is 60,647. Finally, the total number of features is 111 [36].

3.4. Machine learning algorithms

Machine learning is one of the most accepted techniques for malicious websites. Finding phishing is a simple classification problem. There are several machine learning classification algorithms such as XGBoost, RF, support vector machine (SVM), decision tree (DT), and naïve Bayes (NB); in this research, authors will use XGBoost and RF. RF are ensemble machine learning techniques that can be used for regression or grouping. XGBoost is an optimized algorithm designed to be highly effective, elastic, and portable. XGBoost is one of the most prevalent machine learning algorithms, and it can be used for regression and classification [5], [11], [17], [24], [25].

4. EXPERIMENTS AND RESULTS

In the following section, the authors will demonstrate the experiments' evaluation metrics, important features, and results. This study also uses Anaconda and Weka open-source machine learning. Finally, experiments were done using a Dell Machine, 11th Gen -1165G7 @ 2.80GHz, RAM 32 GB, Windows 11.

4.1. Experiments phases and metrics

In phase 1, PSO and GWO are used separately for ten iterations, and the number of features is documented each time. In phase 2, the most repeated features from each algorithm are selected for the classification stage using RF and XGBoost. After 10 iterations using both GWO and PSO, the authors select 55 features for PSO and 58 for GWO, as shown in Table 1.

Several criteria could be used to verify the accuracy of our experiments. Those criteria are accuracy, recall (R), precision (P), F-measure, false negative rate (FNR), true positive rate (TPR), and false positive rate (FPR). This can be seen in Table 2 and (1) to (6).

Table 1. Feature selected

Iterations	PSO	GWO
1	55	58
2	58	59
3	57	60
4	56	58
5	58	59
6	59	57
7	57	56
8	53	60
9	52	57
10	51	60
Average	55.6	58.4

Table 2. Matrix of confusion

		Prediction	
		Normal	Phishing
Act.	Normal	x (TP)	y (FN)
	Phishing	z (FP)	w (TN)

$$TPR = x/(x + y) \quad (1)$$

$$FPR = z/(z + w) \quad (2)$$

$$FNR = y/(x + y) \quad (3)$$

$$P = TP/(TP + FP) \quad (4)$$

$$R = TP/(TP + FN) \quad (5)$$

$$F - Measure = 2 * P * R/(P + R) \quad (6)$$

Here,

TPR: Amount of normal data found to be normal.

FPR: Amount of attack found to be normal.

FNR: Amount of normal found as a strike.
 P: Proportion of the number of choices that are accurate.
 R: Proportion of total related results accurately organized.
 F- Measure: Examining of correctness.

4.2. Experiments results

This section will demonstrate the results of PSO and GWO experiments using RF and XGBoost. The number of features in the dataset is 111. Also, the number of features selected by PSO is 55, and the number of most common features selected by both PSO and GWO is 44. Table 3 and Figure 3 demonstrates the results using the RF classification algorithm.

Table 3. PSO and GWO using RF

Random Forest	TP	FP	FN	P	R.	F-Measure
All Features (111)	0.81	0.21	0.15	0.794	0.844	0.818
PSO (55)	0.91	0.17	0.16	0.843	0.850	0.847
GWO (59)	0.89	0.16	0.15	0.848	0.856	0.852
PSO∩GWO (44)	0.92	0.18	0.16	0.836	0.852	0.844

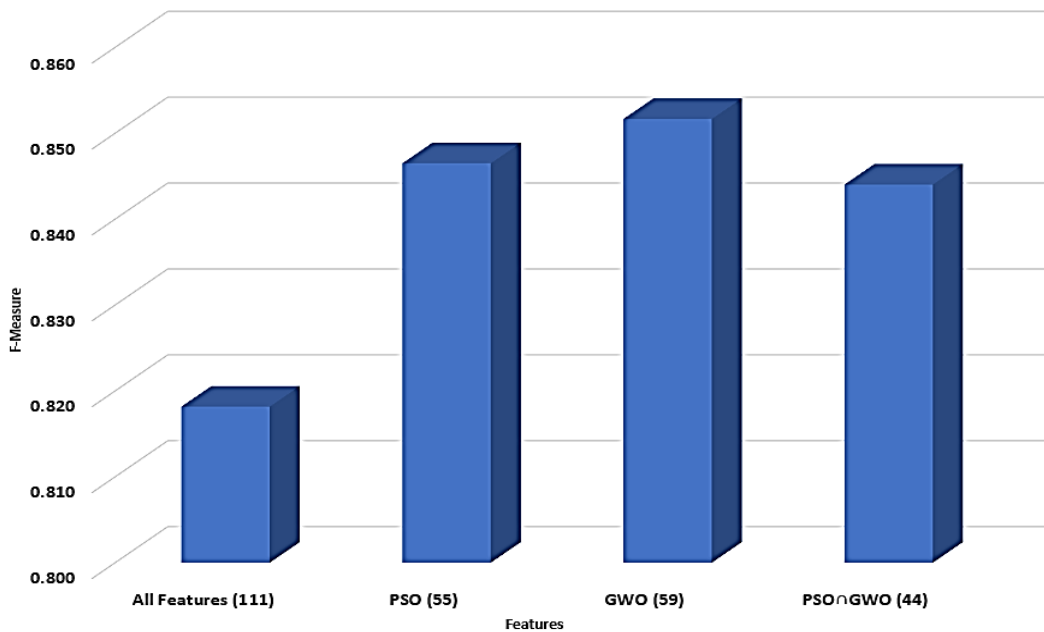


Figure 3. F-measure (RF)

The TPR range for RF is between 81% and 91%, while the precision range is between 79.4% and 84.8%. Also, the Recall is between 84.4% and 85.6%. Finally, the F-measure range is between 81.8% and 85.2%. Table 4 and Figure 4 demonstrate the results using the XGBoost classification algorithm.

The TPR range for XGBoost is between 87% and 96%, while the Precision range is between 79.1% and 96%. Also, the recall is between 85.6% and 87.3%. Finally, the F-measure range is between 82.5% and 91.4%. Figure 3 presents the F-measure range for RF experiments, while Figure 4 presents the F-measure range for XGBoost experiments.

Table 4. PSO and GWO using XGBoost

XGBoost	TP	FP	FN	P.	R.	F-Measure.
All Features (111)	0.87	0.23	0.14	0.791	0.861	0.825
PSO (55)	0.88	0.22	0.13	0.800	0.871	0.834
GWO (59)	0.96	0.04	0.14	0.960	0.873	0.914
PSO∩GWO (44)	0.89	0.22	0.15	0.802	0.856	0.828

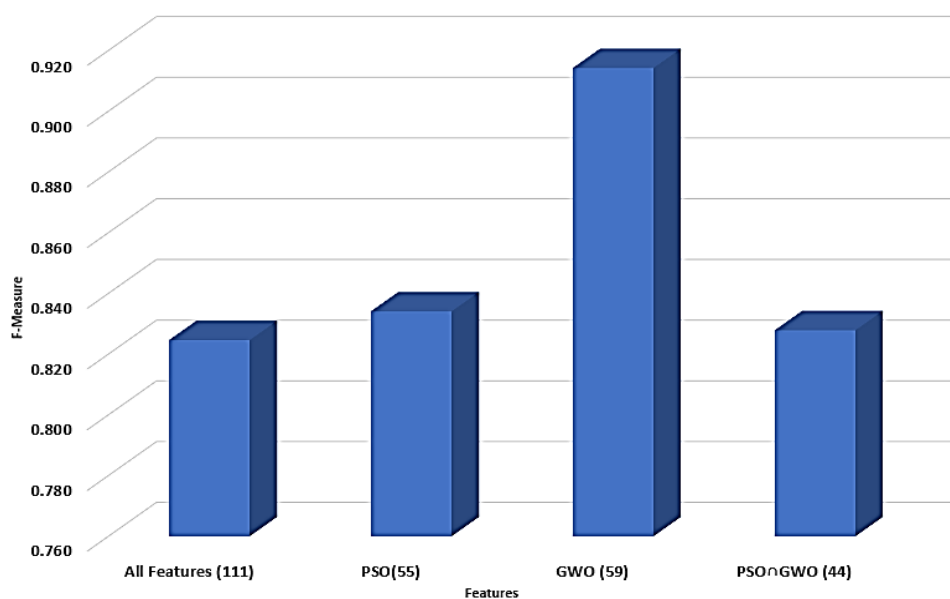


Figure 4. F-measure (XGBoost)

5. CONCLUSION

No doubt, phishing is a universal problem, and the number of phishing websites is increasing quickly. Several techniques and algorithms are used to fight phishing. This paper uses two well-known machine-learning algorithms for phishing detection: RF and XGBoost. Also, this paper presents PSO and GWO metaheuristic procedures for feature reduction. Besides, the number of features is lowered from 111 to 55 and 59, respectively. Reducing the number of features can reduce the complexity and processing time. Also, in this study, the researcher tries to use the best common features that are selected by both PSO and GWO ($PSO \cap GWO$) and the number of these features is 44. Numerous assessment criteria are used, such as precision, recall, TPR, FPR, FNR, and F-measure. Finally, the investigation demonstrates that the proposed model performance is highly acceptable. The RF best F-Measure is 85.2 % and occurs with GWO (59 Features). Also, XGBoost best F-measure is 85.2% and occurs with GWO (59). Future work could be an evaluation of other metaheuristic algorithms and using other machine learning classifications such as naïve Bayes, SVM, and NN.

ACKNOWLEDGMENT

The researchers want to thank editor and reviewers for the time they were granted to review the manuscript. Further, I am very thankful to WISE University.





REFERENCES

- [1] A. Mandadi, S. Boppana, V. Ravella, and R. Kavitha, "Phishing website detection using machine learning," *2022 IEEE 7th International conference for Convergence in Technology (I2CT)*, Mumbai, India, 2022, pp. 1-4, Apr. 2022, doi: 10.1109/i2ct54291.2022.9824801.
- [2] S. Alrefaai, G. Ozdemir, and A. Mohamed, "Detecting phishing websites using machine learning," *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2022, pp. 1-6, doi: 10.1109/hora55278.2022.9799917.
- [3] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respicio, "Cybersecurity education: Evolution of the discipline and analysis of master programs," *Computers and Security*, vol. 75, pp. 24–35, Jun. 2018, doi: 10.1016/j.cose.2018.01.015.
- [4] C. Iwendi *et al.*, "KeySplitWatermark: zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020, doi: 10.1109/access.2020.2988160.
- [5] A. Rehman Javed, Z. Jalil, S. Atif Moqurrah, S. Abbas, and X. Liu, "Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 10, Aug. 2020, doi: 10.1002/ett.4088.
- [6] S. Alnemari and M. Alshammari, "Detecting phishing domains using machine learning," *Applied Sciences*, vol. 13, no. 8, p. 4649, Apr. 2023, doi: 10.3390/app13084649.
- [7] S. K. H. Ahammad *et al.*, "Phishing URL detection using machine learning methods," *Advances in Engineering Software*, vol. 173, Nov. 2022, doi: 10.1016/j.advengsoft.2022.103288.
- [8] H. Bleau and G. Fraud, "Cybercrime forecast: retrieved RSA 2017," *rsa.com*, 2017. <https://www.rsa.com/en-us/resources/2017-global-fraud> (accessed Nov. 01, 2021).




- [9] APWG, "Phishing activity trends reports," *apwg.org*, <https://apwg.org/trendsreports/> (accessed Nov. 01, 2023).
- [10] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Computing and Applications*, vol. 28, no. 12, pp. 3629–3654, Mar. 2016, doi: 10.1007/s00521-016-2275-y.
- [11] A. Hamdan Mohammad, "Intrusion detection using a new hybrid feature selection model," *Intelligent Automation & Soft Computing*, vol. 29, no. 3, pp. 65–80, 2021, doi: 10.32604/iasc.2021.016140.
- [12] A. Hamdan Mohammad, T. Alwada'n, O. Almomani, S. Smadi, and N. ElOmari, "Bio-inspired hybrid feature selection model for intrusion detection," *Computers, Materials & Continua*, vol. 73, no. 1, pp. 133–150, 2022, doi: 10.32604/cmc.2022.027475.
- [13] A. Hamdan Mohammad, S. Smadi, and T. Alwada'n, "Email filtering using hybrid feature selection model," *Computer Modeling in Engineering & Sciences*, vol. 132, no. 2, pp. 435–450, 2022, doi: 10.32604/cmcs.2022.020088.
- [14] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, pp. 345–357, Mar. 2019, doi: 10.1016/j.eswa.2018.09.029.
- [15] P. Yi, Y. Guan, F. Zou, Y. Yao, W. Wang, and T. Zhu, "Web phishing detection using a deep learning framework," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–9, Sep. 2018, doi: 10.1155/2018/4678746.
- [16] 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, p. 232, Jan. 2023, doi: 10.3390/electronics12010232.
- [17] R. Mahajan and I. Siddavatam, "Phishing website detection using machine learning algorithms," *International Journal of Computer Applications*, vol. 181, no. 23, pp. 45–47, Oct. 2018, doi: 10.5120/ijca2018918026.
- [18] S. M. Alshahrani, "URL phishing detection using particle swarm optimization and data mining," *Computers, Materials & Continua*, vol. 73, no. 3, pp. 5625–5640, 2022, doi: 10.32604/cmc.2022.030982.
- [19] R. Sakunthala Jenni and S. Shankar, "Semantic based greedy levy gradient boosting algorithm for phishing detection," *Computer Systems Science and Engineering*, vol. 41, no. 2, pp. 525–538, 2022, doi: 10.32604/csse.2022.019300.
- [20] "Phishtank dataset," *PhishTank*. <http://data.phishtank.com/data/online-valid.csv> (accessed Nov. 01, 2023).
- [21] K. Sarpong Adu-Manu, R. Kwasi Ahiabile, J. Kwame Appati, and E. Essel Mensah, "Phishing attacks in social engineering: a review," *Journal of Cyber Security*, vol. 4, no. 4, pp. 239–267, 2022, doi: 10.32604/jcs.2023.041095.
- [22] D. T. Mosa, M. Y. Shams, A. A. Abohany, E.-S. M. El-kenawy, and M. Thabet, "Machine learning techniques for detecting phishing URL attacks," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 1271–1290, 2023, doi: 10.32604/cmc.2023.036422.
- [23] R. Brindha, S. Nandagopal, H. Azath, V. Sathana, G. Prasad Joshi, and S. Won Kim, "Intelligent deep learning based cybersecurity phishing email detection and classification," *Computers, Materials & Continua*, vol. 74, no. 3, pp. 5901–5914, 2023, doi: 10.32604/cmc.2023.030784.
- [24] E. A. Aldakheel, M. Zakariah, G. A. Gashgari, F. A. Almarshad, and A. I. A. Alzahrani, "A deep learning-based innovative technique for phishing detection in modern security with uniform resource locators," *Sensors*, vol. 23, no. 9, Apr. 2023, doi: 10.3390/s23094403.
- [25] W. Ali and S. Malebary, "Particle swarm optimization-based feature weighting for improving intelligent phishing website detection," *IEEE Access*, vol. 8, pp. 116766–116780, 2020, doi: 10.1109/access.2020.3003569.
- [26] A. N. Jaber, L. Fritsch, and H. Haugerud, "Improving phishing detection with the grey wolf optimizer," *2022 International Conference on Electronics, Information, and Communication (ICEIC)*, Jeju, Korea, Republic of, 2022, pp. 1–6, doi: 10.1109/iceic54506.2022.9748592.
- [27] E. S. Gualberto, R. T. De Sousa, T. P. De B. Vieira, J. P. C. L. Da Costa, and C. G. Duque, "From feature engineering and topics models to enhanced prediction rates in phishing detection," *IEEE Access*, vol. 8, pp. 76368–76385, 2020, doi: 10.1109/access.2020.2989126.
- [28] E. Emary, H. M. Zawbaa, and A. E. Hassanien, "Binary grey wolf optimization approaches for feature selection," *Neurocomputing*, vol. 172, pp. 371–381, Jan. 2016, doi: 10.1016/j.neucom.2015.06.083.
- [29] Q. Al-Tashi, S. J. Abdul Kadir, H. M. Rais, S. Mirjalili, and H. Alhussian, "Binary optimization using hybrid grey wolf optimization for feature selection," *IEEE Access*, vol. 7, pp. 39496–39508, 2019, doi: 10.1109/ACCESS.2019.2906757.
- [30] A. Sahoo and S. Chandra, "Multi-objective grey wolf optimizer for improved cervix lesion classification," *Applied Soft Computing*, vol. 52, pp. 64–80, Mar. 2017, doi: 10.1016/j.asoc.2016.12.022.
- [31] F. Marini and B. Walczak, "Particle swarm optimization (PSO). a tutorial," *Chemometrics and Intelligent Laboratory Systems*, vol. 149, pp. 153–165, Dec. 2015, doi: 10.1016/j.chemolab.2015.08.020.
- [32] J. Kennedy and R. Eberhart, "Particle swarm optimization," in *Proceedings of ICNN'95-International Conference on Neural Networks*, 1995, vol. 4, pp. 1942–1948, doi: 10.1109/ICNN.1995.488968.
- [33] K. Ishaque, Z. Salam, M. Amjad, and S. Mekhilef, "An improved particle swarm optimization (PSO)-based MPPT for PV with reduced steady-state oscillation," *IEEE Transactions on Power Electronics*, vol. 27, no. 8, pp. 3627–3638, Aug. 2012, doi: 10.1109/TPEL.2012.2185713.
- [34] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey wolf optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, Mar. 2014, doi: 10.1016/j.advengsoft.2013.12.007.
- [35] J.-S. Wang and S.-X. Li, "An improved grey wolf optimizer based on differential evolution and elimination mechanism," *Scientific Reports*, vol. 9, no. 1, May 2019, doi: 10.1038/s41598-019-43546-3.
- [36] G. Vrbančić, "Phishing websites dataset," *Phishing Websites Dataset*, vol. 1, 2020, doi: 10.17632/72ptz43s9v.1.

BIOGRAPHIES OF AUTHORS






Adel Hamdan     is a professor in the Computer Science Department at the World Islamic Sciences and Education University, Amman-Jordan. Born in Jordan in 1973. He received his B.Sc. from Philadelphia University in 1998. Then, he earned a master's degree in computer information systems from the Arab Academy for Banking and Financial Science in 2005 and a Ph.D. in computer information systems in 2009 from the Arab Academy for Banking and Financial Science. He works at the Applied Science Private University and The World Islamic Sciences and Education University. His research interests are machine learning, artificial intelligence, and cybersecurity. Certified CCNA, CEH. Also certified and licensed to teach and issue certificates in the following courses from cisco network academy: Cybersecurity Essentials, IoT, NDG Linux, introduction to Cybersecurity, and others. He can be contacted at adel.hamdan@wise.edu.jo.






Muhannad Tahboush    received a Ph.D. degree in cybersecurity from Cyprus International University. He is a at the Department of Information Systems and Networks, The World Islamic Sciences and Education University, Amman, Jordan. His research interests include network security, cryptography, and information security. He can be contacted at muhannad.tahboush@wise.edu.jo.






Mohammad Adawy    received a Ph.D. degree in computer networks and network security. He is currently Dr at the Department of Information Systems and Networks, The World Islamic Sciences and Education University, Amman, Jordan. His research interests include computer networks, wireless networks, wireless sensor networks, and network security. He can be contacted at mohammad.adawi@wise.edu.jo.






Tariq Alwada'n    has been a senior lecturer in computer networks/cybersecurity at the School of Computing, Engineering and Digital Technologies at Teesside University, United Kingdom since July 2020. He holds a Ph.D. in computer science from De Montfort University, UK since 2012. His master's degree was in computer and information networks from the University of Essex, UK, in 2007. His BS was in computer engineering from Al Balqa Applied University, Jordan, in 2005. His main research interests are cloud computing, fog computing, grid computing, IoT, big data mobility in distributed systems, and security. He is certified and licensed as a CCNA instructor from Cisco Network Academy before joining Teesside University. He worked as a lecturer at the Higher Colleges of Technology, UAE, between 2019 and 2020. He also worked as an associate professor of Computer Science at WISE University, Jordan, between 2012 and 2019. He can be contacted at t.alwadan@tees.ac.uk.



Sameh Ghwanmeh    is a full professor of computer science and engineering. Obtained his Ph.D. and M.S. from the UK, in 1996 and 1993 respectively, and his BS degree in computer engineering from Jordan, in 1985. The published work exceeds sixty international journal papers in different research fields, including information retrieval and natural languages processing, data science and big data and its industrial applications, image processing, applications of fuzzy logic techniques, knowledge management, e-business, e-learning, neural networks, computer networks, and wireless networks. Was involved in curriculum development for many undergraduate and graduate programs. Managed and coordinated several research projects funded by regional and international agencies such as the European Commission. A referee for several regional and international conferences. Member of editorship and reviewing activities of several international research journals. He can be contacted at sameh.ghwanmeh@aue.ae.



Moath Husni    was born in Alkarak, Jordan, in 1980. He received a B.E. degree in computer science from the Mutah University, Al Karak, Jordan, in 2002, a master's degree in computer information systems from the Arab Academy for Banking and Financial Sciences in Amman Jordan in 2005, and a Ph.D. degree in software engineering from the university of Utara Malaysia 2016. Moath is an assistant professor at The World Islamic Sciences and Education University (WISE) software engineering department. His research interests cover Agile development methods, software quality assurance, web application development, software process improvement, and software quality metrics with many technical publications. He can be contacted at moath.tarawneh@wise.edu.jo.