ISSN 2278-3091
Volume 9, No.1.5, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse5091.52020.pdf
https://doi.org/10.30534/ijatcse/2020/5091.52020

Fuzzy Modelling using Butterfly Optimization Algorithm for Phishing Detection

Noor Syahirah Nordin[1], MohdArfian Ismail[2], NurulAswa Omar[3]
[1]Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang,Malaysia, syahirahnd21@gmail.com
[2]Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, Malaysia, arfian@ump.edu.my
[3]Faculty of Computer Science and Information Technology, UniversitiTun Hussein Onn Malaysia (UTHM), Malaysia nurulaswa@uthm.edu.my

ABSTRACT

Fuzzy system is a rule-based system by using human experts which hold the truth values or membership values to make a particular decision while fuzzy modelling is a process of identifying the fuzzy parameter. However, it is difficult to generate fuzzy parameter manually when applied on complex problem. To generate the fuzzy parameter automatically, an optimization method is required and Butterfly Optimization Algorithm (BOA) is one of the good methods to be applied. The proposed method will be utilized to produce the optimal solution in finding fuzzy parameter before implementing the fuzzy technique in the dataset chosen. Two datasets were used, namely Website Phishing Dataset (WPD) and Phishing Websites Dataset (PWD). As the result, average accuracy for WPD and PWD is 96.80% and 94.65% respectively. To be conclude, BOA shows promising results to be applied to measure the accuracy of the fuzzy modelling in phishing detection.

Key words: Fuzzy, Butterfly Optimization Algorithm, phishing detection.

1. INTRODUCTION

At the age of the fast-growing technologies and billion users of the internet, there is always danger and threat in its use. One of the threat is phishing attack where it is among the easiest attack to be done by the attacker. This attack is evolving day by day as the phisher getting more creative in planning and launching the attack for malicious intention. Phishing is a simple, easy but dangerous type of cyber-attack. The purpose is to deceive the victims by stealing their personal information. Another motives for performing phishing attacks are financial benefit, selling stolen identities to the black market, defame, ransom, attack's propagation, exploiting security gaps and to gain popularity among the phisher or their peer groups [1]. According to [2], there are two types of phishing attack. The first type is spear phishing which means the attacker attack on victims' private information in order to increase the attacks' probability. The second type of phishing is clone phishing where the attacker mails the link that contained phishing site to fraud victims.

Phishing works when the attacker using malware to remotely control the victim device as the victims falls into their trick. One of the trick is by perceiving the victims through bogus email that is being sent to the victims' email. The email that were sent looked trustworthy to the victim as the email's content usually similar to the legitimate email even though it is phishing email exactly. Another trick is by faking the website clicked by the victims through unknown source or any untrusted popup window that appear on the victim's screen while opening another website. Without deeper concern about the website, the victims tend to fill in their personal information as being asked to do so in the fake website. Spamming user's mobile phone by sending malicious messages through short messaging services (SMS) also another medium used by the phisher to trick victims. The flow of the phishing attack where preparation is needed before performing the attack is shown in Figure 1. It includes the victim selection, fake webpages creation and methods to launch the attack.

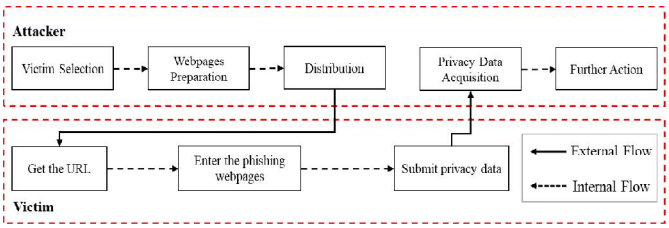

Figure 1: Flow chart of the phishing attack [3]

Phishing attack may lead to the bad consequences where the victim could give all their private information to the phisher without concerning that they will be the victims and it will affecting their life. Therefore, an effective method is needed to detect phishing attack that poses a major threat in network security [4]. Fuzzy technique can be considered as a great method to be implemented to increase the effectiveness of the phishing detection[5]. Fuzzy is one of the most effective technique used in the classification problem. It is near to the way human reasoning as people can make rational decisions based on the combination of multiple parameters. The parameters involved in the system are fuzzy rules and membership function. However, human expert play an

important role in identifying the fuzzy parameter thus problem will arise when there is no human available to do so. Therefore, there is no guarantee in the accurateness produced in the result of fuzzy modelling when there is no optimization method applied. To cater this issue, the optimization method ought to be implemented in the fuzzy system to automatically tune the fuzzy parameters.Hence, this study proposes a method by the application of the BOA in the fuzzy modelling to detect phishing. BOA is one of the recent method that is nature inspired in the metaheuristic algorithm.

The remainder of the paper is structured as follows. The next section describes the Materials and Methods where it discuss the related works on classification method in phishing detection area, fuzzy system, BOA, fuzzy modelling using BOA then followed by model and experiment data. Section 3 shows the experimental result of the proposed method and the last section which is Section 4 will concluded this paper.

2. MATERIALS AND METHODS

2.1 Related Work on Phishing Detection

In recent years, numerous existing phishing detection methodshave been proposed.In classification method, there exist various kind of method that have been tested efficiently by the researchers to classify data. Nowadays, it is a crucial technique or tool because it is used to make all kinds of decision in any aspects which helps the decision maker to make sense of data and find pattern. Authors in [2] has proposed a machine learning method for URL based on fuzzy logic as a classifier. The aim of their study is to propose a framework to detect phishing by using URL based feature in the extraction process and fuzzy logic as the classifier. 1000 URLs from PhishTank and Open phish site was used to train the data and the result from the study 91.46% in terms of the accuracy of the proposed approach. Other than that, researchers in [6] has proposed a study on a content-based phishing detection method in email medium. The purpose was to adopt a new way of detecting phishing by integrating the principles of computing with social engineering. A semantic web database was utilized to store data whereas fuzzy system was used for allocating email categories. The result produced was high in accuracy thus outperformed other method that has been compared in the study. Besides that, authors in [7] has introduced an efficient neural network model based on optimized phishing detection function named OFS-NN. To solve the over-fitting problem in neural network, the optimal feature selection algorithm has been utilized. This approach producesgreat results, as it can enhance the machine learning efficiency. As indicated by Moghimi and Varjani, they identify phishing in internet banking using SVM method. SVM has been used to classify the web pages by determining the relationship between the content of the page and the URL of the page so that the identity of the webpage can be identified in [8]. As the result, the proposed method shows 99.17% accuracy in internet banking and to imply it on mobile devices in the future. Orunsolu et al. has utilized Naïve Bayes and SVM as classifier to distinguish phishing website to improve the efficacy of the anti-phishing schemes. 2541phishing pages and 25000 legitimate pages were used as their dataset in the training model. The runtime of Naïve Bayes was better than SVM while their accuracy rate were similar for both classifier which is 99.96% accuracy [9]. In addition, the previous method done was by using Firefly Algorithm in fuzzy modelling to detect phishing detection. The result achieved was 98.86% accuracy for phishing website detection and 97.49% for phishing detection in SMS [10].

Overall, it can be said that there are a lot of methods used in detecting phishing attack in classification problems. However, all of the methods mentioned has its own advantages and disadvantages in solving the problems arise. To be conclude, the application of classification method approach in detecting phishing attack is technically an effective method to be applied since it is proven to produce the good results in solving problems.

2.2 Fuzzy System

Fuzzy system is a rule-based system that consists of a set of if-then rules that was developed by Lofti A. Zadeh in 1965. It is a method that different from the traditional logic where everything was classified between Yes and No. Unlike traditional logic, this system uses fuzzy logic concept where it can take value between 0 and 1 and involves all the possibilities between Yes and No. Hence, fuzzy logic imitates the way of human thinking as it can handle the imprecise situation and models human cognitive decision making. In fuzzy system, it is characterized by two parameters in order to make sure that the system work properly. Fuzzy rules and membership function are the two important parameters in the system [11]. Fuzzy rules were applied based on its attribute values, and each rule has a weight that determines the degree to which the available number is limited between 0 and 1. This is called membership function that also known as membership value or degree of membership. There are different forms or shape of membership function which are Triangular, Trapezoidal, Generalized Bell, Gaussion and Sigmoidal membership function [12].

The basic structure of the fuzzy logic technique includes four main components to reason data; (i) fuzzification, (ii) fuzzy inference engine, (iii) defuzzification, and (iv) fuzzy knowledge base. The fuzzy system elements are described in Figure 2 and Table 2 lists the components in fuzzy system and its description [13].

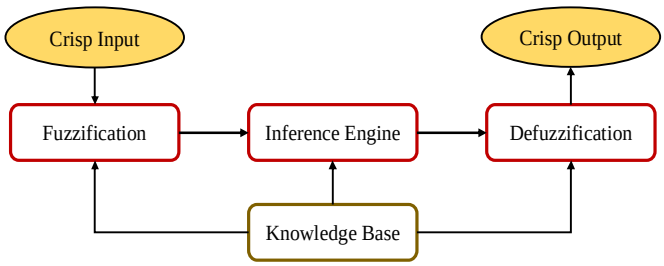

Figure 2: Fuzzy system elements[14]

Table 2: Description of the fuzzy system elements

Component	Description
Fuzzification	Translates crisp data into fuzzy values
Inference Engine	Perform fuzzy operation to obtain output in fuzzy value
Defuzzification	Translates fuzzy output into crisp data
Knowledge Base	Contains a set of fuzzy rules (rule base) and membership function (database)

2.3 Butterfly Optimization Algorithm

The BOA is one of the Arora's recently introduced, nature-inspired algorithm [15]. It is an algorithm that mirrors the behaviour of butterflies foraging food. Each butterfly has its own fragrance that distinguishes them from another butterflies within the gather. The scent of each butterfly is dependent on three major components (i) modality of the sensor, (ii) stimulus intensity and (iii) power exponent. The butterflies sense the scent in the air to detect food source position or mating partner. To demonstrate the characteristic of the butterflies, summarization of it are as follows:

i. All butterflies are able to attract each other by emitting their fragrance.

ii. Every butterfly moves towards the other butterflies that emit more fragrance or just travelin random direction.

iii. The fragrance intensity emitted by the butterflies are decided by the setting of the objective function to be optimized.

In order to perform optimization, butterflies act as the search agent in BOA. There are three stages in the algorithm; (i) initialization stage, (ii) iteration stage and (iii) last stage. Firstly, the step began by defining the objection function, generating initial population and initializing the algorithm's parameter. Then, in the iteration stage, a number of iterations are performed. All butterflies will be assessedin each iteration by evaluating their fitness function before producing the fragrance at their position using (1) as follows:

$$f = cI^a \tag{1}$$

where f is the fitness function where it supposed to attract other butterflies with their fragrance. Meanwhile c is the sensory modality, $I$is the variation of butterfly and a is the power exponent parameter depends on the sensory modality. The global and local search processes are implemented after generating the random number $rand$, where $rand \in [0,1]$. In global search phase, the butterfly will move towards another butterflies who emits more fragrance which can be represented in (2)

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i \tag{2}$$

where x_i^t is the solution vector x_i for ith butterfly in iteration number t, f_i defined the fragrance of ith butterfly while g^* represents current best solution in current iteration. Meanwhile, the local search process can be described in (3)

$$x_i^{t+1} = x_i^t + (r^2 \times x_j^t - x_k^t) \times f_i \tag{3}$$

where x_j^t and $x_k^t$are two vectors representing two different butterflies from the solution space. The iteration will continue until the termination criteria satisfied. The last phase is the final phase where the best solution found after the value of the parameter is updated. Figure 3 presents the steps of BOA in pseudo code.

```
Objective function f(x), x = (x_1, x_2, ..., x_dim), dim = no. of dimensions
Generate initial population of n butterflies x_i = (i = 1, 2, ..., n)
Stimulus Intensity I, at x_i is determined by f(x_i)
Define sensor modality c, power exponent a and switch probability p
while stopping criteria not met do
    for each butterfly in population do
        Calculate fragrance of the butterfly using Eq. (1)
    end for
    Find the best butterfly
    for each butterfly in population do
        Generate a random number rand from [0, 1]
        if rand < p then
            Move towards best butterfly solution using Eq. (2)
        else
            Move randomly using Eq. (3)
        end if
    end for
    Update the value of a
end while
Output the best solution found
```

Figure 3: Pseudocode of BOA [15]

2.4Fuzzy Modelling using BOA

When the optimal solution in BOA is found, the fuzzy logic techniques are embedded in the algorithm by updating the fuzzy parameter that will produce the best fitness value. Then, the fuzzy logic techniques that will be implemented in the algorithm including the process of fuzzification, inference engine and defuzzification to find a new solutions in fuzzy modelling [16]. To be more easily understood, the steps are being summarizes as below:

Step 1 : Begin the algorithm by initializing the BOA's parameters which including objective function and initial population.

Step 2 : Calculate the butterflies' fragrance in the population.

Step 3 : After butterflies moving towards the best butterflies or move randomly in the population, update the position of butterflies.

Step 4 : If the updated solution is better than the previous one, accept and replace the previous one with the new value. Otherwise, keep the previous solution.

Step 5 : After reaching the stopping criteria, find the optimal solution in the BOA. The step will goes back to evaluating objective function as long as the iteration has not reached the stopping criteria.

Step 6 : Update the fuzzy parameter; membership function and fuzzy rules based on the chosen dataset.

Step 7 : Implement fuzzy logic techniques where the process including fuzzification, inference engine and defuzzification. The input before fuzzification process is crisp input and the fuzzy value will be convert into crisp output after the process of defuzzification. Inference engine is where all of the operation of combining the membership function and fuzzy rules work.

Step 8 : Returning the final fuzzy model as the new solution before ending the process. The process will goes back to Step 4 if still wants to continue the process.

2.5 Model and Experimental Data

In this study, two datasets from University of California, Irvine (UCI) machine learning repository will be used. The reason to use the datasets from this source because the database provides trusted and high quality data. All data in this database can be freely accessed from the Internet in their official website linked http://archive.ics.uci.edu/ml/. Thereby, the datasets used for experiment in this study are Website Phishing Dataset (WPD) and Phishing Websites Dataset (PWD).

WPD is a set of phishing and legitimate websites collected by Neda Abdelhamid. This dataset contains 1353 number of websites where 702 of them are phishing URLs, 548 are legitimate websites and the remaining of them are suspicious websites. All websites were collected from different sources such as PhishTank and Yahoo. This dataset has 9 number of attributes and three classes which are phishing, legitimate and suspicious. The attributes are SFH, pop up window, SSL final state, request URL, URL anchor, web traffic, URL length, domain age and having IP. The second dataset is PWD. This dataset has 2456 instances and 30 attributes including the class attribute. According to Mohammad et al., the dataset collected are mainly from trusted sources; PhishTank archive, MillerSmiles archive and Google searching operators. The attributes are IP, URL length, shortening service, at symbol, double slash, prefix, sub domain, SSL, domain registration length, favicon, port, https, request URL, URL anchor, links in tags, SFH, submit to email, abnormal URL, redirect, on mouse over, right click, pop up, iframe, domain age, DNS, web traffic, page rank, google index, links pointing to page and statistical report. Meanwhile, the class attribute is the result of the website either phishing or legitimate website.

Moreover, a good method to evaluate the results produced are needed in every experiment. Therefore, the technique of k-fold cross validation will be utilized to foresee the execution of the proposed method. By using this technique, it helps the researcher to better use of the data and predict the pattern of the results produced when running the experiment. K-fold cross validation technique is easy to understand since it is very simple and has been use by many researchers make it among one of the popular technique to validate data. This technique works by dividing the datasets into k fold with equal or approximately equal sizes and each fold will be run repeatedly for k times on every fold of the data. Next, the result produces in each fold will be calculate averagely to find the single estimation value. For the last step, k accuracies will be produced as the final result to evaluate the proposed method's performance. In this study, 10-fold cross validation will be applied since it is very common used among the researchers to evaluate data. To assess the outcome of the experiments performed, its fitness value will be calculated which will reflect the model's accuracy.

3. EXPERIMENTAL RESULTS

In this part, the analyzation of the results from the algorithm will be described in details. Firstly, the parameters of the BOA were tested with different value to identify which value produce the best result when implementing the fuzzy modelling using BOA. There are four parameters from BOA that were taken into account which are population size, sensor modality, power exponent and switch probability. Table 2 shows the range value of each parameter that mentioned in most research papers.

Table 2: Parameters setting

Parameter	Value
Population size	[10, 50]
Sensor modality	[0.01, 0.03]
Power exponent	[0.1, 0.3]
Switch probability	[0.5, 0.8]

After each parameter has perform the sensitivity analysis, the best value of every parameter can be found. This process has been done in order to produce the better result in fuzzy modelling in the purpose to achieve higher result in the accuracy level. The best value of each kind of parameter setting can be shown in the Table 3.

Table 3: The best parameters setting

Parameter	Value
Population size	50
Sensor modality	0.01
Power exponent	0.1
Switch probability	0.8

For the last analyzation is the accuracy of the result for every dataset taken after applying the best parameter value of BOA in the fuzzy modelling. The result from both datasets were different because of the characteristics of each dataset is not same thus it will affect the performance level of the experiment. Three categories from the result will be analyse; best solution, worst solution and the solution's average value. The highest accuracy from the 10-fold cross validation will be considered as the best solution while the lowest accuracy will be the worst solution. The best and worst accuracy result

will be measured in a single run from the experiment. These analyses of the experiment's best and worst value aims to determine the quality of the fuzzy modelling. In the meantime, the solution's average value is the mean value of all the accuracy value generated in single run. Table 4 summarizes the results obtained for every dataset applied in terms of best, worst and average value of the accuracy value in the fuzzy modelling. In addition, the value of standard deviation was also being calculated to measure the consistency of the method in producing the result. The calculation was made after the accuracy value of every fold in the 10-fold cross validation is obtained.

To prove the performance of the proposed study, the results for both datasets were compared with other algorithms which are the best performing that has been mentioned at the first part of the paper. Six algorithms have been chosen which are GA, DE, PSO, TLBO, HS and GSA. As the result, it has been proven that this method is better than the other methods to be applied in the fuzzy modelling where the result produced was the highest in both datasets. Table 5summarizes the comparison of the results obtained with other algorithms in dataset 1, WPD and dataset 2, PWD respectively. In addition, the results obtained on both datasets were also being compared with another works in order to show the effectiveness of the proposed method. The proposed method has outperformed the methods that has been proposed in the previous works in both datasets. Although it does not show a significant differences in the result, but it still produces better result that will increase the performance value of the experiment. Thus, Table 6 summarizes the comparison of dataset 1 and Table 7 compared the results of the works that utilized dataset 2.

Table 4: The summary result using BOA in fuzzy modelling

Dataset	Accuracy (%)			Standard Deviation
	Best	Worst	Average	
WPD	97.43	95.56	96.80	0.61
PWD	95.10	90.32	94.65	1.65

Table 5: The comparison of results with other algorithms

Algorithm	Dataset 1 – WPD (%)	Dataset 2 – PWD (%)
GA	95.19	90.10
DE	67.80	67.80
PSO	54.29	54.29
TLBO	54.30	56.30
HS	80.56	87.89
GSA	90.29	86.25
This study	**96.80**	**94.65**

Table 6: The result comparison with other works for dataset 1

Work By	Result (%)
Amir Latif et al.[17]	89.87
Zubair Hasan, Hasan, andZahan[18]	91.90
This study	**96.80**

Table 7: The result comparison with other works for dataset 2

Work By	Result (%)
Zabihimayvan and Doran[19]	93.00
Roopak, Vijayaraghavanand Thomas[20]	92.00
Vrbančič, Fister andPodgorelec[21]	94.40
This study	**94.65**

4. CONCLUSION

The research finding shows that the phishing detection can bedone by usingoptimization method for fuzzy modelling. In this study, a method by using fuzzy system and BOA was proposed to detect phishing. The presentation of the BOA in fuzzy modelling has been described clearly in this paper. BOA was being picked to generate the fuzzy parameter in fuzzy system thus it can tackle the problem in fuzzy system which is hard to determine the parameter. To evaluate the results produced in each experiment, k-fold cross validation technique was used since this technique proved that it is such a good choice to be used. For the experimental result, research finding shows that the proposed method produce the highest accuracy value for both datasets when compared to other algorithms. The proposed method were compared with another six methods in the metaheuristic algorithm and shows better performance. In addition, this study has proven that it has better performance and can outperform the proposed method in another works where it can achieved very competitive results in the accuracy value. In the future, BOA can be combine with another algorithm as the optimization method to produce better result in fuzzy modelling.

ACKNOWLEDGMENT

This study was supported by Fundamental Research Grant Scheme (FRGS) with Vot No. FRGS/1/2018/ICT02/UMP/02/2: RDU190113 from Ministry of Higher Education (MOHE) and managed by Universiti Malaysia Pahang and Geran TIER-1 H107 from Research Management Centre (RMC), UniversitiTun Hussein Onn Malaysia (UTHM).

REFERENCES

1. D. Goel and A. K. Jain. **Mobile phishing attacks and defence mechanisms : State of art and open research**,*Comput. Secur.*, vol. 73, pp. 519–544, 2018.
2. H. Chapla, R. Kotak, and M. Joiser.**A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier**, *Proc. Fourth Int. Conf. Commun. Electron. Syst. (ICCES 2019)*, no. Icces, pp. 383–388, 2019.
3. Y. Ding, N. Luktarhan, K. Li, and W. Slamu.**A keyword-based combination approach for detecting phishing webpages**, Vol. 84, pp. 256–275, 2019.
4. A. Aleroud and L. Zhou. **Phishing environments,techniques,and countermeasures : A survey**, *Comput. Secur.*, vol. 68, pp. 160–196, 2017.
5. P. Barraclough and G. Sexton.**Phishing Website Detection Fuzzy System Modelling**, *2015 Sci. Inf. Conf.*, pp. 1384–1386, 2015.

6. H. Che, Q. Liu, L. Zou, H. Yang, D. Zhou, and F. Yu.**A Content-Based Phishing Email Detection Method**, *2017 IEEE Int. Conf. Softw. Qual. Reliab. Secur.*, 2017.
7. E. Zhu, C. Ye, D. Liu, F. Liu, F. Wang, and X. Li.**An Effective Neural Network Phishing Detection Model Based on Optimal Feature Selection**,*2018 IEEE Intl Conf Parallel Distrib. Process. with Appl. Ubiquitous Comput. Commun. Big Data Cloud Comput. Soc. Comput. Networking, Sustain. Comput. Commun.*, pp. 781–787, 2018.
8. M. Moghimi and A. Y. Varjani. **New rule-based phishing detection method,***Expert Syst. Appl.*, vol. 53, pp. 231–242, 2016.
9. A. A. Orunsolu, A. S. Sodiya, and A. T. Akinwale. **A predictive model for phishing detection**,*J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2019.
10. N. S. Nordin, M. A. Ismail, V. Mezhuyev, S. Kasim, M. S. Mohamad, and A. Osman. **Fuzzy Modelling using Firefly Algorithm for Phishing Detection**, *Adv. Sci. Technol. Eng. Syst. J.*, vol. 4, no. 6, pp. 291–296, 2019.
11. C. Bergmeir and M. Ben. **frbs : Fuzzy Rule-Based Systems for Classification**,*J. Stat. Softw.*, vol. 65, no. 6, pp. 1–30, 2015.
12. C. Wang. **A Study of Membership Functions on Mamdani-Type Fuzzy Inference S**,*Theses Diss.*, vol. Paper 1665, 2015.
13. R. Jain and A. Abraham.**A Comparative Study of Fuzzy Classification Methods on Breast Cancer Data**, *7th Int. Work Conf. Artif. Nat. Neural Networks, IWANN'03*, pp. 1–6, 2003.
14. C. Paper. **Fuzzy logic based design of classical behaviors for mobile robots in ROS middleware Fuzzy Logic Based Design of Classical Behaviors for Mobile Robots in ROS Middleware**, no. May 2016, 2014.
15. S. Arora and S. Singh. **Butterfly optimization algorithm : a novel approach for global optimization**, *Soft Comput.*, vol. 23, no. 3, pp. 715–734, 2019.
16. L. Vanschoren, Joaquin and van Rijn, Jan N. and Bischl, Bernd and Torgo. **OpenML: Networked Science in Machine Learning**, *SIGKDD Explor.*, vol. 15, pp. 49–60, 2013.
17. R. M. Amir Latif, M. Umer, T. Tariq, M. Farhan, O. Rizwan, and G. Ali.**A Smart Methodology for Analyzing Secure E-Banking and E-Commerce Websites**, *Proc. 2019 16th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2019*, no. February 2020, pp. 589–596, 2019.
18. K. M. Zubair Hasan, M. Z. Hasan, and N. Zahan. **Automated Prediction of Phishing Websites Using Deep Convolutional Neural Network**,*5th Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2019*, pp. 11–12, 2019.
19. M. Zabihimayvan and D. Doran. **Fuzzy Rough Set Feature Selection to Enhance Phishing Attack Detection**,*IEEE Int. Conf. Fuzzy Syst.*, vol. 2019-June, pp. 5–10, 2019.
20. S. Roopak, A. P. Vijayaraghavan, and T. Thomas. **On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection**, *1st Int. Conf. Adv. Technol. Intell. Control. Environ. Comput. Commun. Eng. ICATIECE 2019*, pp. 172–175, 2019.
21. G. Vrbančič, I. Fister, and V. Podgorelec. **Swarm Intelligence Approaches for Parameter Setting of Deep Learning Neural Network**, in *Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics - WIMS '18*, 2018, pp. 1–8.