Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 6, 291-296 (2019)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Fuzzy Modelling using Firefly Algorithm for Phishing Detection

Noor Syahirah Nordin[1], Mohd Arfian Ismail[1,*], Vitaliy Mezhuyev[2], Shahreen Kasim[3], Mohd Saberi Mohamad[4,5], Ashraf Osman Ibrahim[6]

[1] *Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang, 26300, Malaysia.*

[2] *FH JOANNEUM University of Applied Sciences, Institute of Industrial Management, Austria.*

[3] *Soft Computing and Data Mining Centre, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn, Johor, Malaysia.*

[4] *Institute for Artificial Intelligence and Big Data, Universiti Malaysia Kelantan, City Campus, Pengkalan Chepa, 16100 Kota Bharu, Kelantan, Malaysia.*

[5] *Faculty of Bioengineering and Technology, Universiti Malaysia Kelantan, Jeli Campus, Lock Bag 100, 17600 Jeli, Kelantan, Malaysia.*

[6] *Faculty of computer Science and Information Technology, Alzaiem Alazhari University, Khartoum North 13311, Sudan.*

ARTICLE INFO

Article history:
Received: 30 August, 2019
Accepted: 16 November, 2019
Online: 12 December, 2019

Keywords:
Fuzzy modeling
Firefly algorithm
Phishing detection

ABSTRACT

A fuzzy system is a rule-based system that uses human experts' knowledge to make a particular decision, while fuzzy modeling refers to the identification process of the fuzzy parameters. To generate the fuzzy parameters automatically, an optimization method is needed. One of the suitable methods provides the Firefly Algorithm (FA). FA is a nature-inspired algorithm that uses fireflies' behavior to interpret data. This study explains in detail how fuzzy modeling works by using FA for detecting phishing. Phishing is an unsettled security problem that occurs in the world of internet connected computers. In order to experiment with the proposed method for the security threats, a database of phishing websites and SMS from different sources were used. As a result, the average accuracy for the phishing websites dataset achieved 98.86%, while the average value for the SMS dataset is 97.49%. In conclusion, both datasets show the best result in terms of the accuracy value for fuzzy modeling by using FA.

1. Introduction

Phishing is a cyber-attack criminal activity that is intended to steal sensitive information such as credit card information or account login credential from users by using bogus websites [1], [2]. There are three components in phishing techniques; medium of phishing, vector to transmit the attack, and technical approaches used during the attack. The first component, the medium of phishing is the base means of conveying the phishing attacks to the victims which involve three bases; internet, voice, and short messaging service (SMS). The second component, the vector that defines the vehicle in place for launching the attack such as Email, eFax, websites, and social networks that are accessible through the Internet. The last component is the technical approaches which are used to improve the phishing effectiveness during an attack.

Nowadays, many approaches are being used by the phishers to steal personal information such as browser vulnerabilities, mobile phone or man-in-them-middle. A phishing attack is the simplest kind of security threat, but at the same time is the most effective and dangerous violence. This is due to the fact that attackers use malware to remotely control a victim's device for their particular intention such as spying or stealing personal information. While not many people are aware that they may be a victim of a phishing attack, it is poses a major threat in network security. Therefore, many researchers are focused on the methods to detect phishing efficiently and produce better results than the previous methods.

*Corresponding Author: Mohd Arfian Ismail, arfian@ump.edu.my

https://dx.doi.org/10.25046/aj040637

One way to improve the efficiency to detect the phishing attack is by using the fuzzy techniques. With the fuzzy system, people can make an intelligent decision that works based on the combination of several factors. However, this method is a time consuming and does not guarantee an optimum solution because a fuzzy system requires the identification of the fuzzy parameters; fuzzy rules and the membership function. Hence, the optimization method needs to be applied in the system in order to tune the parameters of the fuzzy system automatically. This paper proposes a novel method by application of the Firefly Algorithm (FA). FA can be considered as a recent optimization method that is being used in artificial intelligence [3].

2. Materials and Methods

2.1. Related Works

There are many existing phishing detection techniques proposed in recent years. Researchers [4] proposed a software named anti-phishing simulator that collects phishing and spam messages where the users can examine the link addresses in the mail. It prescribes whether the messages can be classified as a phishing attack by using the Bayesian classification algorithm. Authors [5] have given a phishing site detection approach via URL analyses. Their work uses a URL detection method to discover phishing websites using a random forest algorithm. They have limited the feature set of URL detection to eight out of thirty-one features. The parameters considered to measure the accuracy level include f-measure, ROC Curve, precision, and sensitivity for analysis purposes. As a result, the accuracy level of this method was 95% [5]. By using the machine learning, researchers [6] proposes a hybrid solution that combines three approaches; blacklist and whitelist, heuristics, and visual similarity. The hybrid solution will be fed to the machine learning algorithm to calculate the accuracy results. By using different approaches , it will produce better accuracy and provide more efficient protection system [6]. According to [7], PhishBox is a new approach for phishing validation and detection that collects phishing data in real-time. The modules in this method include extract-transform-load, modelling, voting, monitoring, and visualization. The results [7] show that the proposed method has achieved high performance compared to the other works. Authors [8] used the C4.5 decision tree algorithm to analyse phishing sites. The data contain URL heuristics and the sites ranked to decide on a phishing attack. The proposed method extracts URL features and calculates their heuristic value. Then, the C4.5 decision tree algorithm was used to generate rules and identify the probability of phishing. There are 9 features of the URL used in the proposed method to detect phishing sites. The results showed that the method is more robust and precise compared to previous methods. Researchers [9] proposed a secured methodology for anti-phishing. The algorithm and techniques used were balanced block replacement, advanced encryption standard, and code generation. There are two phases in the proposed techniques which are user registration phase and user login phase. The method [9] is not flexible to accommodate the increasing number of consumers, therefore it will be difficult to provide a unique code to each user. Authors [10] proposed phishing emails detection using Cuckoo Search SVM (CS-SVM). Cuckoo Search algorithm was used for parameter selection. It extracts 23 features that are used to construct the hybrid classifier. This method uses the measures of a true positive rate, a false positive rate, and an accuracy as evaluation metric to evaluate the performance. CS-SVM shows a 91 percent higher result in terms of phishing email detection accuracy at different training sets when compared with traditional SVM classifier [10].

Overall, a lot of methods have been proposed by other researchers and have their advantages and disadvantages in producing the results. For detecting phishing in real-time, the researchers create new software that uses specific tools and algorithms to collect phishing data. On the other hand, the machine learning approach was recognised by researchers as the most effective method.

2.2. Fuzzy System

The fuzzy system is a rule-based system which works by using the fuzzy logic to reason data. Most of the fuzzy concepts come from the human language. It is an approach based on the "degrees of truth" and it imitates the way humans make decisions that involve the possibilities between YES and NO.

To ensure that the fuzzy system works properly, fuzzy parameters are needed. The parameters are the fuzzy rules and membership functions [11]. Fuzzy rules were originally obtained from human experts through the knowledge engineering processes. However, this approach cannot be applied when there are no human experts or if the data are too complex. Besides, membership function is a function that defines the degree to which a given input belongs, where the output is between 0 and 1. To implement a fuzzy logic technique , four elements are required which are fuzzification, fuzzy inference engine, fuzzy rule base, and defuzzification. The elements of the fuzzy system are shown in Figure 1 while the list and description of the components in a fuzzy system are described in Table 1.

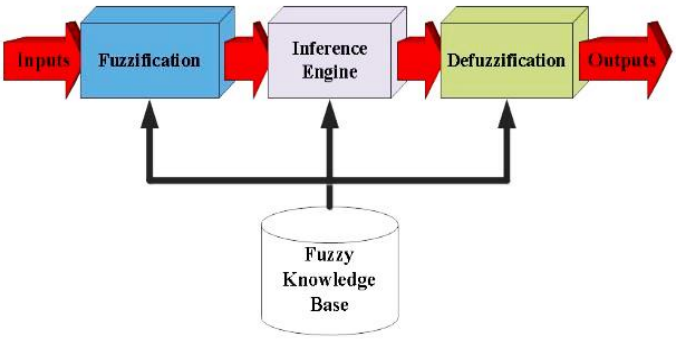


Figure 1: Elements of the fuzzy system

Table 1: Description of the fuzzy system elements

Component	Description
Fuzzy knowledge base	It contains a set of fuzzy sets and fuzzy rules
Fuzzification	Convert crisp data into the membership function
Inference Engine	Perform fuzzy operation by combining membership functions with the fuzzy rules to obtain the fuzzy output
Defuzzification	Convert fuzzy output into crisp data

Meanwhile, fuzzy modelling is a task of finding or identifying the fuzzy parameters to achieve the desired behaviour. An effective method should be used to generate the fuzzy parameters automatically from data. Regarding that, using an optimization method is the best choice by automatically generating the fuzzy parameters from available data [12].

2.3. Representation of Fuzzy Parameter

In the study, the fuzzy rule is defined by using numerical form where it is responsible for representing the fuzzy sets in the model. The fuzzy rules use the IF-THEN form as shown in Figure 2.

IF (A_1^j **IS** R_1^j) **AND** (A_2^j **IS** R_2^j) **AND** ….. (A_j^j **IS** R_j^j) **THEN** (**CL IS** C^j)

Where,

A = linguistic variable (attribute of the data)
R = linguistic value (value of the data)
CL = class attribute of the data
C = output of the linguistic value
j = number of attribute in the data
i = number of rules that is used

Figure 2: IF-THEN rule form description

The A in the IF-THEN form represents the input of the linguistic value while the output is the value of C for the class variable. The value of the attribute (A) is set in a range of 0 until 3, where the values of 1 and 2 are represented as phishing and legitimate respectively while the values of 0 and 3 do not apply. It gives meaning where if the fuzzy rule produces the value of 0 or 3 in the attribute's value, the attribute will not be included as the fuzzy set. Meanwhile, the value of class (CL) is set to 0 and 1, where it represents the result of the attribute.

The example of the process of encoding the fuzzy rules in the case study shown in Figure 3. The sample was taken from the Phishing Websites Dataset. In this example, almost all 30 attributes were included in the fuzzy rule in which 8 produced the value of 0, which is not included in the fuzzy sets. This is because the attribute has a value of 1; "*phishing*". If the fuzzy set stated "*legitimate*", the value will be 2. At the end of the fuzzy rules that represent a membership function, the results will be shown.

The schematic shape of the membership function used in this study is trapezoidal. The encoding process of the membership function is demonstrated in Figure 4, where it applied on the first dataset (the phishing websites dataset). The value of every parameter represented the starting point of the overlap in the membership functions. Since the number of attributes in the dataset is 31, the length of the membership function is equal to 31 as well.

2.4. Firefly Algorithm

The FA is an algorithm that was developed by Xin-She Yang at Cambridge University in 2007 [13]. The FA is a swarm intelligence-based metaheuristic approach inspired by the behaviour of fireflies. The flashing light of fireflies acts as a signal system or communication to attract other fireflies. It can also function as a protective warning mechanism. The flashing characteristics of the fireflies are as follows: i) All fireflies are unisex, therefore they become attracted to other fireflies without being concerned about their sex; ii) The less bright fireflies will move to the other fireflies who has the brighter flash as the attractiveness is proportional to their brightness. The attractiveness and brightness of the firefly are reduced as the distance increase. If no firefly is brighter than them, the fireflies will move randomly without the right direction; iii) The brightness of a firefly is determined by the setting of the objective function to be optimized.

Rule 1: IF (*have IP* IS *phishing*) AND (*URL length* IS *phishing*) AND (*shortening service* IS *phishing*) AND (*at symbol* IS *phishing*) AND (*double slash* IS *phishing*) AND (*prefix suffix* IS *phishing*) AND (*sub domain* IS *phishing*) AND (*SSL final* IS *phishing*) AND (*domain registration length* IS *phishing*) AND (*favicon* IS *phishing*) AND (*port* IS *phishing*) AND (*https* IS *phishing*) AND (*request URL* IS *phishing*) AND (*anchor* IS *phishing*) AND (*link in tags* IS *phishing*) AND (*SFH* IS *phishing*) AND (*redirect* IS *phishing*) AND (*on mouse over* IS *phishing*) AND (*right click* IS *phishing*) AND (*pop up window* IS *phishing*) AND (*iframe* IS *phishing*) then (*website* IS *phishing*)

A_1^1	A_2^1	A_3^1	A_4^1	A_5^1	A_6^1	A_7^1	A_8^1	A_9^1	A_{10}^1	A_{11}^1	A_{12}^1	A_{13}^1	A_{14}^1	A_{15}^1	A_{16}^1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

A_{17}^1	A_{18}^1	A_{19}^1	A_{20}^1	A_{21}^1	A_{22}^1	A_{23}^1	A_{24}^1	A_{25}^1	A_{26}^1	A_{27}^1	A_{28}^1	A_{29}^1	A_{30}^1	CL
0	0	1	1	1	1	1	0	0	0	0	0	0	0	1

Where,

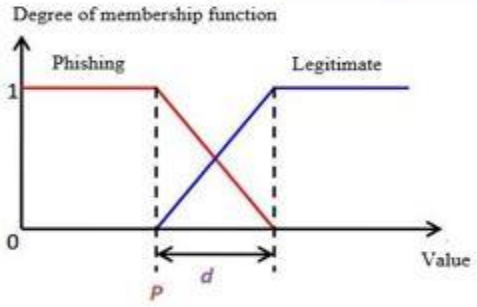
A_1^1	:	Have IP	A_{11}^1	:	Port	A_{21}^1	:	Right click
A_2^1	:	URL length	A_{12}^1	:	Https	A_{21}^1	:	Pop up window
A_3^1	:	Shortening service	A_{13}^1	:	Request URL	A_{23}^1	:	Iframe
A_4^1	:	At symbol	A_{14}^1	:	URL of anchor	A_{24}^1	:	Age of domain
A_5^1	:	Double slash	A_{15}^1	:	Links in tags	A_{25}^1	:	DNS record
A_6^1	:	Prefix	A_{16}^1	:	SFH	A_{26}^1	:	Web traffic
A_7^1	:	Sub domain	A_{17}^1	:	Submit to email	A_{27}^1	:	Page rank
A_8^1	:	SSL	A_{18}^1	:	Abnormal URL	A_{28}^1	:	Google index
A_9^1	:	Domain registration length	A_{19}^1	:	Redirect	A_{29}^1	:	Links pointing to page
A_{10}^1	:	Favicon	A_{20}^1	:	On mouse over	A_{30}^1	:	Statistical report

CL : Phishing / Legitimate

Figure 3: The example of process encodes for fuzzy rules

Parameter	Attribute
A_1^1	Have IP
A_2^1	URL length
A_3^1	Shortening service
A_4^1	At symbol
A_5^1	Double slash
A_6^1	Prefix
A_7^1	Sub domain
A_8^1	SSL
A_9^1	Domain registration length
A_{10}^1	Favicon
A_{11}^1	Port
A_{12}^1	Https
A_{13}^1	Request URL
A_{14}^1	URL of anchor
A_{15}^1	Links in tags
A_{16}^1	SFH

Parameter	Attribute
A_{17}^1	Submit to email
A_{18}^1	Abnormal URL
A_{19}^1	Redirect
A_{20}^1	On mouse over
A_{21}^1	Right click
A_{22}^1	Pop up window
A_{23}^1	Iframe
A_{24}^1	Age of domain
A_{25}^1	DNS record
A_{26}^1	Web traffic
A_{27}^1	Page rank
A_{28}^1	Google index
A_{29}^1	Links pointing to page
A_{30}^1	Statistical report
CL	Phishing / Legitimate



	A_1^1	A_2^1	A_3^1	A_4^1	A_5^1	A_6^1	A_7^1	A_8^1	A_9^1	A_{10}^1	A_{11}^1	A_{12}^1	A_{13}^1	A_{14}^1	A_{15}^1	A_{16}^1
p	1	0	1	0	0	2	1	0	0	0	2	2	1	1	0	1
d	0	0	1	0	1	1	1	0	0	1	2	1	1	1	0	2

	A_{17}^1	A_{18}^1	A_{19}^1	A_{20}^1	A_{21}^1	A_{22}^1	A_{23}^1	A_{24}^1	A_{25}^1	A_{26}^1	A_{27}^1	A_{28}^1	A_{29}^1	A_{30}^1	CL
p	1	1	0	2	2	1	0	1	0	0	2	0	1	1	0
d	0	0	1	1	1	1	1	2	2	1	2	2	1	0	0

Figure 4: Value of membership function and the length of overlap

The work of FA is started by initializing the objective function, followed by generating the initial population of fireflies. Then continued with determining the light intensity and ranking the fireflies before updating the fireflies' position in the population. Figure 5 shows the flowchart of the FA.

2.5. Model and Experimental Data

In order to test the efficiency of the proposed method in detecting phishing, two benchmarks datasets were used. The first dataset is taken from the University of California, Irvine (UCI) machine learning repository. This database is the trusted and most widely used dataset for detecting phishing attacks, which can be accessed at http://archive.ics.uci.edu/ml/. The dataset involved is a phishing website dataset that contains 2456 instances and 30 attributes. The dataset collected is mainly from trusted sources; PhishTank archive, MillerSmiles archive, Google searching operators.

Meanwhile, the second dataset that was used contains SMS messages that were obtained from the Unicamp website at http://www.dt.fee.unicamp.br/~tiago/smsspamcollection/. The dataset contains 5574 instances and 2 attributes that were collected from various sources such as Grumbletext Web, NUS SMS Corpus, and SMS Spam Corpus v.0.1 Big.

The experiments were conducted by using 10-fold cross-validation for both datasets. The cross-validation was performed by partitioning the data into 10 partitions where every partition consists of equal number of data in it. The process was then repeated 10 times. In evaluating these experiments, the results were measured by their fitness value which is equivalent to the accuracy of the model. There are three categories considered in the model, which are the best solution, worst solution, and average value. The best solution is the highest accuracy in each experiment amongst the 10-fold cross-validation in a single run while the worst solution indicates the lowest accuracy value in a single run. The purpose of determining the best and worst result in every experiment is to show the potential of fuzzy modelling by using FA. Meanwhile, the average solution is the mean value of all the fitness value results in the experiments.

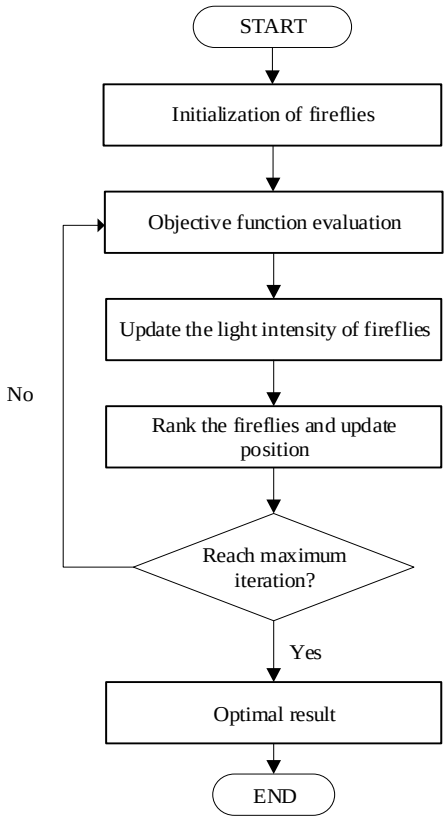


Figure 5: Flowchart of the Firefly Algorithm

In this study, the fuzzy system is used to generate fuzzy rule and membership function by using the FA. For the classification process, the fuzzy engine used was Sazonov Fuzzy Engine. It is a freely available fuzzy engine which is fully implemented in Java. It can be downloaded at http://people.clarkson.edu/~esazonov/.

3. Experimental Results

This section presents the analysis of the results obtained. Fuzzy modelling by using FA was tested with many parameters affecting the performance of the system . The effects of five parameter's performance which are population size, gamma probability, alpha0 probability, alphan probability, and the number of generations are shown in Table 2.

Table 2: Parameters setting

Parameter	Value
Population size	[10,40]
Gamma probability	[0.5,2.0]
Alpha0 probability	[0.1,0.4]
Alphan probability	[0.001,0.004]
Number of generations	[50,200]

As mentioned in most of the research papers, FA needs a small number of populations e.g. from 10 to 40 [14]. This is to make sure that the solution can be gained in a short time. For the gamma probability value, the current study stated that the ideal value for the gamma is 1.0 [15]. Next, the papers stated that 0.2 is the ideal value for the alpha0 parameter and 0.001 is the ideal value to be used for alphan probability [15]. Meanwhile, the number of generations tested was in a range of 50 to 100.

Table 3: The best parameters setting

Parameter	Value
Population size	20
Gamma probability	1.0
Alpha0 probability	0.2
Alphan probability	0.001
Number of generations	100

After the sensitivity analysis of every parameter in the algorithm has been performed, the best parameter setting can be found. The best parameter generated can be used to find the highest fitness value and is able to produce higher interpretability of the fuzzy model. Table 3 shows the best results for every parameter setting when being applied to both datasets.

Lastly, the accuracy of the results for every dataset was recorded and analyzed. The results were obtained after applying the best parameter value shown in Table 3. The first dataset shows that the highest accuracy, which is the best result, manages to reach up to 100% accuracy while the worst value is 97.72% and the average accuracy is 98.86%. Meanwhile, the second dataset indicates the value of 99.46% as the best accuracy value, 95.52% as the worst value, and 97.49% as average accuracy. To access the performance of the proposed study, the accuracy results for both datasets obtained were compared with other works. Table 4 gives the comparison of dataset 1 while Table 5 compared the results of dataset 2 with other works. Table 4 and Table 5 clearly show that the proposed method produces the best results compare to others.

Table 4: The comparison of results with other works for dataset 1

Work By	Result
Kaytan and Hanbay [16]	95.05%
Ubing et al.[17]	92.5%
Vrbančič, Fister, and Podgorelec [18]	94.4%
Mohd Foozy [19]	95.53%
This study	**98.86%**

Table 5: The comparison of results with other works for second dataset

Work By	Result
Mathew and Issac [20]	98.22%
Kawade[21]	98.34%
Raj et al. [22]	96.17%
Safie et al. [23]	97.13%
This study	**99.46%**

4. Conclusion

In this study, an improved method for fuzzy modelling was proposed and presented in detail. The method used FA for generating the fuzzy rule and membership function automatically for identifying the fuzzy parameter. To test the performance of the proposed method, two benchmark datasets were used. The results of the implementation of the method have been analyzed and it showed that the proposed method performed well compared to other works in terms of accuracy. To conclude, the implementation of FA for fuzzy modelling was able to produce good results.

Conflict of Interest

There is no conflict of interest declared by the authors.

Acknowledgment

Special appreciation to Universiti Malaysia Pahang for the sponsorship of this study by approve the Ministry of Higher Education (MOHE) for Fundamental Research Grant Scheme (FRGS) with Vot No. RDU190113.

References

[1] K. Leng, C. Lin, K. Wong, K. S. C. Yong, and W. King, "A new hybrid ensemble feature selection framework for machine learning-based phishing detection system," *Inf. Sci. (Ny).*, vol. 484, pp. 153–166, 2019. https://doi.org/10.1016/j.ins.2019.01.064

[2] M. M. Moreno-Fernández, F. Blanco, P. Garaizar, and H. Matute, "Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud," *Comput. Human Behav.*, vol. 69, pp. 421–436, Apr. 2017. https://doi.org/10.1007/978-3-319-09129-7_17

[3] R. B. Francisco, M. F. P. Costa, and A. M. A. C. Rocha, "Experiments with Firefly Algorithm," in *Computational Science and Its Applications -- ICCSA 2014*, 2014, pp. 227–236. https://doi.org/10.1007/978-3-319-09129-7_17

[4] M. Baykara and Z. Z. Gurel, "Detection of phishing attacks," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, 2018, pp. 1–5. https://doi.org/10.1109/ISDFS.2018.8355389

[5] S. Parekh, D. Parikh, S. Kotak, and S. Sankhe, "A New Method for Detection of Phishing Websites: URL Detection," in *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018*, 2018, no. Icicct, pp. 949–952. https://doi.org/10.1109/ICICCT.2018.8473085

[6] V. Patil, P. Thakkar, C. Shah, T. Bhat, and S. P. Godse, "Detection and Prevention of Phishing Websites Using Machine Learning Approach," in *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*, 2019, pp. 1–5. https://doi.org/10.1109/ICCUBEA.2018.8697412

[7] J. H. Li and S. De Wang, "PhishBox: An approach for phishing validation and detection," in *Proceedings - 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 2017 IEEE 15th International Conference on Pervasive Intelligence and Computing, 2017 IEEE 3rd International Conference on Big Data Intelligence and Compu*, 2018, vol. 2018-Janua, pp. 557–564. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.10

[8] L. MacHado and J. Gadge, "Phishing Sites Detection Based on C4.5 Decision Tree Algorithm," in *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*, 2018, pp. 1–5. https://doi.org/10.1109/ICCUBEA.2017.8463818

[9] T. Churi, P. Sawardekar, A. Pardeshi, and P. Vartak, "A Secured Methodology for Anti-Phishing," in *International Conference on Innovations in Information, Embedded and Communication Systems*, 2017, pp. 1–4. https://doi.org/10.1109/ICIIECS.2017.8276081

[10] W. Niu, X. Zhang, G. Yang, Z. Ma, and Z. Zhuo, "Phishing emails detection using CS-SVM," in *Proceedings - 15th IEEE International Symposium on Parallel and Distributed Processing with Applications and 16th IEEE International Conference on Ubiquitous Computing and Communications, ISPA/IUCC 2017*, 2018, pp. 1054–1059.

[11] L. S. Riza, C. Bergmeir, F. Herrera, and J. M. Benítez, "frbs : Fuzzy Rule-Based Systems for Classification and Regression in R," *J. Stat. Softw.*, vol. 65, no. 6, pp. 1–30, Jun. 2015. https://doi.org/10.18637/jss.v065.i06

[12] S. K. Rawat, "A Review on Spam Classification of Twitter Data Using Text Mining and Content Filtering," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 6, pp. 485–488, 2015.

[13] A. J. Umbarkar, U. T. Balande, and P. D. Seth, "Performance evaluation of firefly algorithm with variation in sorting for non-linear benchmark problems," in *AIP Conference Proceedings*, 2017, vol. 1836. https://doi.org/10.1063/1.4981972

[14] X.-S. Yang, "Firefly algorithms for multimodal optimization," in *Stochastic Algorithms: Foundations And Applications*, 2009, p. 178. https://doi.org/10.1007/978-3-642-04944-6_14

[15] J. Kwiecień and B. Filipowicz, "Firefly algorithm in optimization of queueing systems," *Bull. Polish Acad. Sci. Tech. Sci.*, vol. 60, no. 2, pp. 363–368, 2012. https://doi.org/10.2478/v10175-012-0049-y

[16] M. Kaytan and D. Hanbay, "Effective Classification of Phishing Web Pages Based on New Rules by Using Extreme Learning Machines," *Anatol. J. Comput. Sci.*, vol. 2, no. 1, pp. 15–36, 2017.

[17] A. A. Ubing, S. Kamilia, A. Abdullah, N. Jhanjhi, and M. Supramaniam, "Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 252–257, 2019. http://dx.doi.org/10.14569/IJACSA.2019.0100133

[18] 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. http://doi.acm.org/10.1145/3227609.3227655

[19] C. F. Mohd Foozy, R. Ahmad, M. A. Faizal Abdollah, and C. C. Wen, "A Comparative Study with RapidMiner and WEKA Tools over some Classification Techniques for SMS Spam," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 226, no. 1, 2017. https://doi.org/10.1088%2F1757-899x%2F226%2F1%2F012100

[20] K. Mathew and B. Issac, "Intelligent spam classification for mobile text message," *Proc. 2011 Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2011*, vol. 1, no. December, pp. 101–105, 2011.

[21] D. R. Kawade, "SMS Spam Classification using WEKA," *Int. J. Electron. Commun. Comput. Technol.*, vol. 5, no. ICICC, pp. 43–47, 2015. https://doi.org/10.1109/ICCSNT.2011.6181918

[22] H. Raj, Y. Weihong, S. K. Banbhrani, and S. P. Dino, "LSTM Based Short Message Service (SMS) Modeling for Spam Classification," in *Proceedings of the 2018 International Conference on Machine Learning Technologies*, 2018, pp. 76–80. http://doi.acm.org/10.1145/3231884.3231895

[23] W. N. H. W. Safie, N. N. A. Sjarif, N. F. M. Azmi, S. S. Yuhaniz, R. C. M. Yusof, and S. Yaacob, "SMS spam classification using Vector Space Model and Artificial Neural Network," *Int. J. Adv. Soft Comput. its Appl.*, vol. 10, no. 3, pp. 130–142, 2018.