Efficient Detection of Phishing Websites Using Multilayer Perceptron

https://doi.org/10.3991/ijim.v14i11.13903

Ammar Odeh (✉)
Princess Sumaya University for Technology Amman, Jordan
a.odeh@psut.edu.jo

Ismail Keshta
AlMaarefa University Riyadh, KSA

Eman Abdelfattah
Ramapo College of New Jersey, New Jersey, USA

Abstract—Phishing is a type of Internet fraud that aims to acquire the credential of users via scamming websites. In this paper, a novel approach is utilized that uses a Neural Network with a multilayer perceptron to detect the scam URL. The proposed system improves the accuracy of the scam detection system as it achieves a high accuracy percentage of 98.5%.

Keywords—Multilayer Perceptron (MLP), Activation function, Semantic attack, Phishing.

1 Introduction

In recent years, cyber-attacks are becoming increasingly common. The attackers use the computer as a tool or as a target and sometimes both. A cyber-attack is an intrusion by computer hackers utilizing one or more computers against single or multiple computers or against the infrastructure. A cyber-attack deliberately destroys computers, steals information, or use a compromised computer as a starting point for other threats [1, 2].

The cyber-attacks are classified mainly into two categories. The first category is the syntactic attack that are grouped under the name "malicious software" or "malware" and this type of attacks include viruses, Trojan horses, and worms. As soon as the malicious software is inserted into a computer, the computer system starts doing undesired functions [3]. The second category is semantic attacks, where the attackers collect the victim information through some websites or links that looks like trusted websites or to acquire his/her username, password, and credit card information [4]. Table 1 shows some types of semantic attacks and a brief description for them [5].

Table 1. Types of Semantic Attacks

Types of Semantic Attacks	Description
Brute-Force Attack	An end-all method to crack a difficult password.
Dictionary Attack	The attacker uses a dictionary in an attempt to guess the password.
Denial-of-Service Attack	The attack focuses on the interruption of a network service.
Backdoor	Any secret method of bypassing normal authentication or security controls.
Eavesdropping	Listening to a private conversation.
Spoofing	Falsifying data.
Privilege Escalation	An attacker is able to fool the system into giving him/her access to restricted data.
Phishing	The attacker uses Email, Website, URL to crack usernames, passwords and credit card details directly from users.

Nowadays, most of the internet users are facing website phishing daily through different tools, such as email, SMS, or instant message from unsuspecting users by employing social engineering techniques. Phishing emails are designed to sound as if they were sent from a lawful corporation or a recognized individual. Such emails also aim to get the victim to visit a website that leads the victim to a fake website that claims to be legitimate. The victim may then be requested to enter confidential information, such as usernames and passwords for the credit card [6, 7].

Phishing websites are now a significant issue, not only because of the rise in the number of such websites but also because of clever tactics used to develop these websites, so that even users with good experience with cybersecurity and the Web could be fooled [8].

The rest of this paper is organized as follows. Section II discusses previous anti-phishing techniques. Preliminaries are discussed in Section III. The novelty of the proposed approach is discussed in Section IV, Section V describes the simulation results regarding the proposed work. Finally, concluding remarks and future works are offered in Section VI.

2 Prior Works

Phishing protection methods are classified into two main categories; denunciation platforms and heuristics-based solutions. denunciation platforms are built by developers and periodically provide the web browser with the updated blacklist [9]. Google developed SafeBrowsing and operates in the Safari, Chrome, Firefox browsers. Microsoft maintained SmartScreen and operates in the Internet Explorer and Edge. The main drawback of the blacklist model is the period of time needed to recognize the phishing sites; sometimes it takes zero-day (0_day) and sometimes takes months which is enough time to fraud for multiple victims. The second solution is heuristics-based solutions, where the heuristics algorithms study the URL features and predict if the URL is trusted or malicious [10].

Dhamija et al. introduced Dynamic Security Skins, by employing a shared secret image that enables the server to verify its identity to the user [11].

Beatson et al. proposed a Trusted Credentials Area (TCA) which is any third-party certification against phishing [12].

Other authentication techniques are used to protect the user against the phishing problem. These techniques deploy user authentication, email authentication, and server authentication. AOL introduced Passcode as a one of user authentication against password phishing where the authentication Passcode expired every 60 seconds [11]. Other techniques employed by Microsoft by sending Sender ID to cover the domain spoofing problem [12]. Another model called Phishing graph introduced by Jakobsson to visualize the flow of information of phishing attack, by using the phishing graph system enables him to understand and analyze the phishing attack [13].

Silva et al. used logistic regression classifier to analyze the features of URLs and identify the phishing URLs. Jain and Gupta employed the K-mean algorithm to predict the similarity of suspicious pages. Other prediction algorithms employed the content or information on the suspicious page [14]. Aburrous implemented hashing to identify malicious sites by verifying the CSS formatting as well as JavaScript or HTML [15].

Afroz et al. Integrate the potential of whitelisting strategies to prevent new or planned phishing scams with the ability of blacklisting and heuristic approaches to alert clients of harmful sites [16][26].

3 Preliminaries

In this research, the proposed model is evaluated using the selected dataset. This section describes the dataset and the Neural Network used in the proposed model.

3.1 Dataset

The dataset used in this article collected from Phish Tank, Miller, Smiles, Google search (26/0/2015). The dataset contains 2456 instances and 30 attributes. The 30 attributes distributed over four features categories; Address bar, abnormal, HTML and JavaScript, and Domain [17][27][28].

3.2 Multilayer perceptron (MLP)

A Multilayer perceptron is a class of feed-forward artificial neural network (FFNN) that consists of more than two layers; the first layer is the input layer and the last one is the output layer and there are some layer(s) between them called hidden layer(s). As the number of layers is increased, the time complexity is increased. Each neuron receives an input (x1, x2,..xn) and bias (b). Each of the input is multiplied with the weight (w) and then the output (y) is processed based on the activation function (φ).

$$y = \varphi(\sum_{i=1}^{n} w_i x_i + b) \quad (1)$$

4 Proposed Model

Fig 1 shows the system flow diagram to recognize the URL. The proposed system reads the URL, then the URL is classified into features according to the dataset components. Then, the model applies the single attribute evaluator and ranks the link's features. Based on a single attribute evaluator, the proposed model eliminates irrelevant attributes. The next step is to combine attributes and apply the search strategy to remove the redundant data and keep the high correlated attributes. Finally, the system decides if the link is harmful or not.

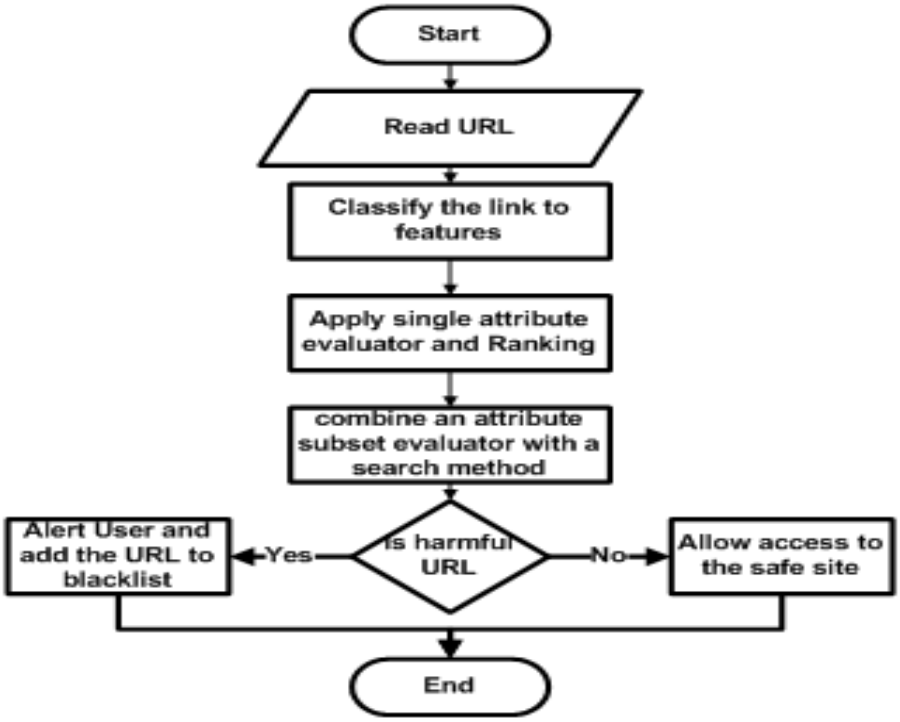

Fig. 1. The Proposed System Flow Diagram

5 Experimental Work

The proposed model uses Weka 3.6 and Python to evaluate the performance of the model. Table 2 shows the experimental parameters such as the learning rate, the number of epochs (number of passes through data), and the number of hidden layers, the batch size, and the momentum.

Table 2. Experimental Parameters

Parameter	Value
Learning rate for MLP	0.3
Number of epochs for MLP	500
Number of hidden layers for MLP	1
Number of hidden neurons for MLP	1
Batch Size	100
Momentum	0.2

6 Discussion of Results

This section describes the results. The confusion matrix is demonstrated in Table 3. The accuracy and F measure of the proposed model is evaluated.

Table 3. Confusion matrix

		Predicted class	
		Positive	**Negative**
Actual class	**Positive**	**TP**	**FP**
	Negative	**FN**	**TN**

After applying the single attribute evaluator, the system generated only 10 attributes (class is included). These attributes are as follows: Prefix_Suffix, having_ Sub_Domain, SSLfinal_State, Request_URL URL_of_Anchor, Links_in_tags SFH,web_traffic, and Google_Index. Fig 2 and Fig 3 describe the structure of the MLP network and the heat map to describe the correlation factor with the result (Safe, Unsafe).

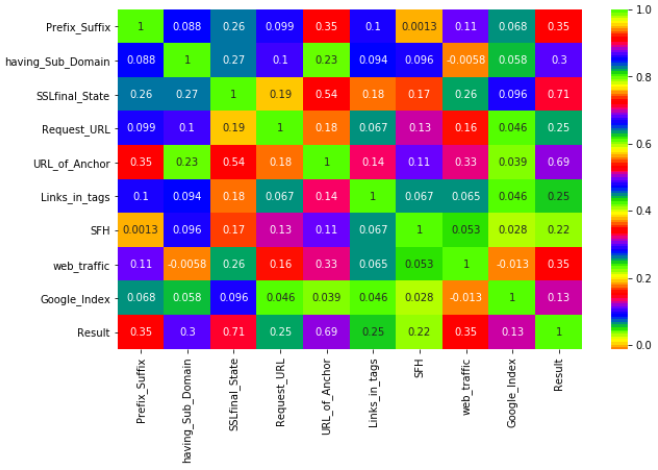

Fig. 2. Heat Map After Applying Single Attribute Evaluator

The proposed model applies attributes combine to minimize the number of highly correlated attributes so that the accuracy of the system is increased as shown in Fig 3 and Fig 4.

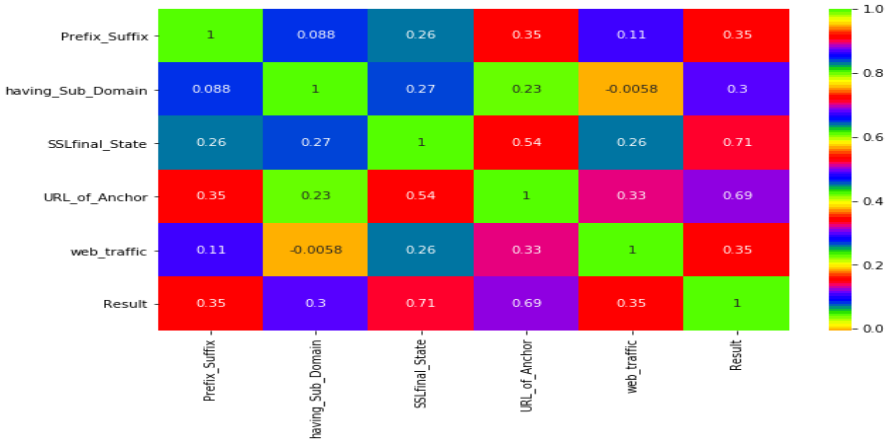

Fig. 3. Heat Map After Applying Attribute Combine

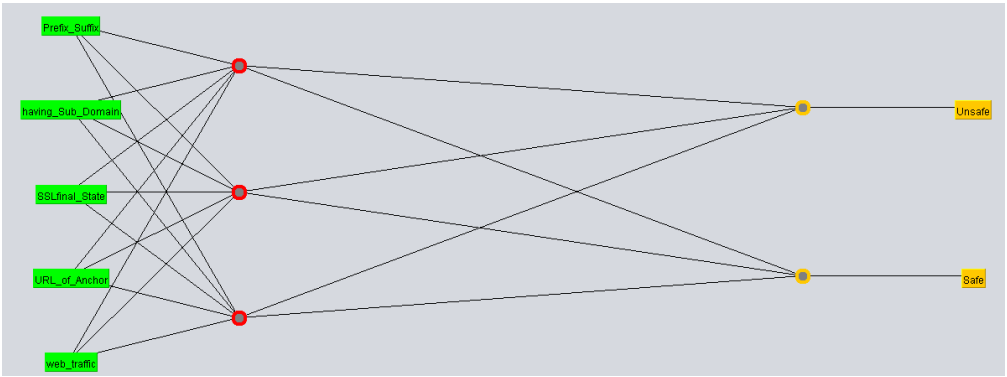

Fig. 4. MLP Structure

Based on the proposed model, the system uses a confusion matrix to evaluate its performance according to accuracy and F-measure.

$$\boldsymbol{Precision} = \boldsymbol{TruePositives} / (\boldsymbol{TruePositives} + \boldsymbol{FalsePositives}) \quad (2)$$

$$\boldsymbol{Recall} = \boldsymbol{TruePositives} / (\boldsymbol{TruePositives} + \boldsymbol{FalseNegatives}) \quad (3)$$

$$\boldsymbol{Accuracy} = \boldsymbol{TruePositives} + \boldsymbol{TrueNegatives} / (\boldsymbol{Total\ Nimber\ of\ Instances}) \quad (4)$$

$$\boldsymbol{F-Measure} = (2 * \boldsymbol{Precision} * \boldsymbol{Recall}) / (\boldsymbol{Precision} + \boldsymbol{Recall}) \quad (5)$$

Where

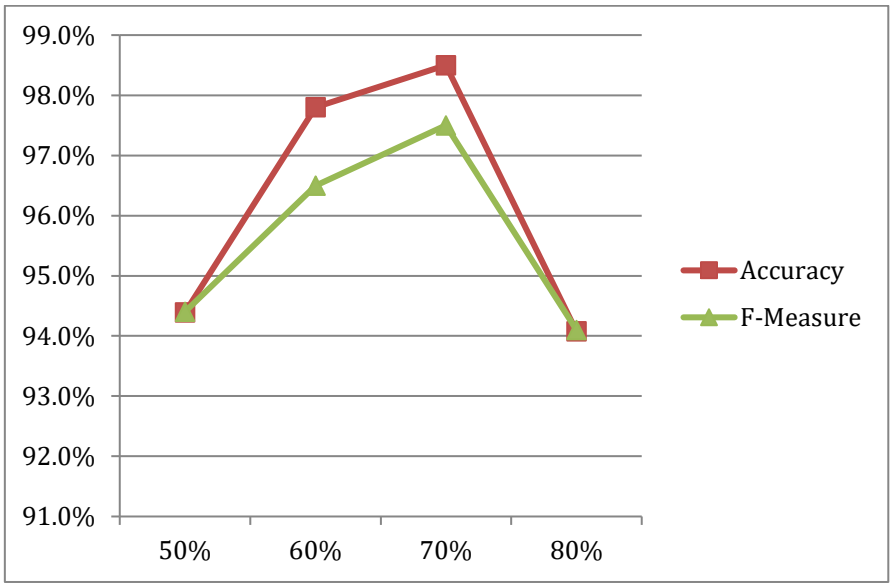

Fig. 5. Accuracy and F-Measure

Table 4 shows a comparison between different machine learning algorithms to detect the phishing URL and the corresponding accuracy for each one. Our proposed algorithm enhances the accuracy to achieve 98.5%.

Table 4. The accuracy of different algorithms to detect phishing URL

Paper	Machine Learning Algorithm	Accuracy
[18]	NN	94.07%
[19]	multi-label rule-based	94.8%
[20]	NN	84%
[21]	FFNN	87%
[22]	feed forward NN	97.40%
[23]	logistic regression classifier	98.40%
[24]	Naïve Bayesian classifier	90%
[25]	HNB and J48	96.25%

7 Conclusion

The proposed model introduces a new phishing detection approach by using a Multilayer perceptron Neural Network. The model applies the processing steps; single attribute evaluator and attribute combine to achieve high accuracy of 98.5% where the

training ratio is 70%. In future work, a comparison of different machine learning algorithms and analyzing them to evaluate which approach achieves the highest accuracy with minimum time complexity.

8 References

[1] Paul Francis, Sebastian Probst-Eide, Pawel Obrok, Cristian Berneanu, Sasa Juric, and Reinhard Munz, "Extended Diffix," arXiv preprint arXiv:1806.02075, 2018.

[2] Payam Karisani and Eugene Agichtein, "Did You Really Just Have a Heart At-tack? Towards Robust Detection of Personal Health Mentions in Social Media," in Proceedings of the 2018 World Wide Web Conference, 2018, pp. 137-146. https://doi.org/10.1145/3178876.3186055

[3] Najah Ben Said, Fabrizio Biondi, Vesselin Bontchev, Olivier Decourbe, Thomas Given-Wilson, Axel Legay, and Jean Quilbeuf, "Detection of mirai by syntactic and semantic analysis," 2017. https://doi.org/10.1109/issre.2018.00032

[4] Yousif, Huda, Karim Hashim Al-saedi, and Mustafa Dhiaa Al-Hassani. "Mobile Phishing Websites Detection and Prevention Using Data Mining Techniques." International Journal of Interactive Mobile Technologies 13.10 (2019). https://doi.org/10.3991/ijim.v13i10.10797

[5] Kaiyuan Kuang, Zhanyong Tang, Xiaoqing Gong, Dingyi Fang, Xiaojiang Chen, Heng Zhang, Jie Liu, and Zheng Wang, "Exploit dynamic data flows to protect software against semantic attacks," in 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (Smart World/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2017, pp. 1-6. https://doi.org/10.1109/uic-atc.2017.8397540

[6] Almseidin, Mohammad, et al. "Phishing Detection Based on Machine Learning and Feature Selection Methods." International Journal of Interactive Mobile Technologies (iJIM) 13.12 (2019): 171-183. https://doi.org/10.3991/ijim.v13i12.11411

[7] Ryan Heartfield, George Loukas, and Diane Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social en-gineering attacks," IEEE Access, vol. 4, pp. 6910-6928, 2016. https://doi.org/10.1109/access.2016.2616285

[8] Ahmed Aleroud and Lina Zhou, "Phishing environments, techniques, and countermeasures: A survey," Computers & Security, vol. 68, pp. 160-196, 2017. https://doi.org/10.1016/j.cose.2017.04.006

[9] Yuvaraj, D., et al. "Some Investigation on DDOS Attack Models in Mobile Net-works." International Journal of Interactive Mobile Technologies (iJIM) 13.10 (2019): 71-88. https://doi.org/10.3991/ijim.v13i10.11304

[10] Abdul Abiodun Orunsolu, Misturah Adunni Alaran, Adeleke Amos Adebayo, Sa-kiru Oluyemi Kareem, and Ayobami Oke, "A Lightweight Anti-Phishing Technique for Mobile Phone," Acta Informatica Pragensia, vol. 6, pp. 114-123, 2017. https://doi.org/10.18267/j.aip.104

[11] Saad Tayyab and Asad Masood, "A Review: Phishing Detection using URLs and Hyperlinks Information by Machine Learning Approach," 2019.

[12] Carlo Marcelo Revoredo da Silva, Eduardo Luzeiro Feitosa, and Vinicius Cardoso Garcia, "Heuristic-based strategy for Phishing prediction: A survey of URL-based approach," Computers & Security, vol. 88, p. 101613, 2020. https://doi.org/10.1016/j.cose.2019.101613

[13] Amine Ait-Ouahmed, Didier Josselin, and Fen Zhou, "Relocation optimization of electric cars in one-way car-sharing systems: modeling, exact solving and heuristics algorithms," International journal of geographical information science, vol. 32, pp. 367-398, 2018. https://doi.org/10.1080/13658816.2017.1372762
[14] Burton S Kaliski and Magnus Nyström, "Password-protection module," ed: Google Patents, 2011.
[15] Veena K Katankar and VM Thakare, "Short message service using SMS gateway," International Journal on Computer Science and Engineering, vol. 2, pp. 1487-1491, 2010.
[16] Markus Jakobsson, "Modeling and preventing phishing attacks," in Financial Cryptography, 2005.
[17] Pete Burnap, Amir Javed, Omer F Rana, and Malik S Awan, "Real-time classification of malicious URLs on Twitter using machine activity data," in Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, 2015, pp. 970-977. https://doi.org/10.1145/2808797.2809281
[18] Tayyabah Hassan and Fahad Ahmed, "Transaction and Identity Authentication Security Model for E-Banking: Confluence of Quantum Cryptography and AI," in International Conference on Intelligent Technologies and Applications, 2018, pp. 338-347. https://doi.org/10.1007/978-981-13-6052-7_29
[19] Sadia Afroz and Rachel Greenstadt, "Phishzoo: Detecting phishing websites by looking at them," in 2011 IEEE fifth international conference on semantic computing, 2011, pp. 368-375. https://doi.org/10.1109/icsc.2011.52
[20] D. and Graff Dua, C. (2019). UCI Machine Learning Repository.
[21] Rami M Mohammad, Fadi Thabtah, and Lee McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, pp. 443-458, 2014. https://doi.org/10.1007/s00521-013-1490-z
[22] Neda Abdelhamid, "Multi-label rules for phishing classification," Applied Compu-ting and Informatics, vol. 11, pp. 29-46, 2015. https://doi.org/10.1016/j.aci.2014.07.002
[23] Rami Mohammad, TL McCluskey, and Fadi Abdeljaber Thabtah, "Predicting phishing websites using neural network trained with back-propagation," 2013.
[24] Fadi Thabtah, Rami M Mohammad, and Lee McCluskey, "A dynamic self-structuring neural network model to combat phishing," in 2016 International Joint Conference on Neural Networks (IJCNN), 2016, pp. 4221-4226. https://doi.org/10.1109/ijcnn.2016.7727750
[25] Ammara Zamir, Hikmat Ullah Khan, Tassawar Iqbal, Nazish Yousaf, Farah Aslam, Almas Anjum, and Maryam Hamdani, "Phishing web site detection using diverse machine learning algorithms," The Electronic Library, 2020. https://doi.org/10.1108/el-05-2019-0118
[26] Ankit Kumar Jain and Brij B Gupta, "A machine learning based approach for phishing detection using hyperlinks information," Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 2015-2028, 2019. https://doi.org/10.1007/s12652-018-0798-z
[27] Arun Kulkarni, "Phishing Websites Detection using Machine Learning," 2019.
[28] Andre Bergholz, Jeong Ho Chang, Gerhard Paass, Frank Reichartz, and Siehyun Strobel, "Improved Phishing Detection using Model-Based Features," in CEAS, 2008

9 Authors

Ammar Odeh received his Ph.D. Degree in Computer science and Engineering with a concentration in Computer Security (Steganography) from University of Bridgeport. He received M.S. degree in Computer Science with a concentration in Reverse software Engineering and Computer Security from the University of Jordan, College of King

Abdullah II School for Information Technology (KASIT). In 2002, he finished B.Sc. Degree in Computer Science and applications, from the Hashemite University, Prince Al-Hussein Bin Abdullah II for Information Technology. During the Ph.D. period, he worked as research Assistant, Teaching Assistant, and Instructor. He is currently an assistant professor in the computer science at Princess Sumaya University for Technology.

Ismail Keshta received his B.Sc. and the M.Sc. degrees in computer engineering and his Ph.D. in computer science and engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2009, 2011, and 2016, respectively. He was a lecturer in the Computer Engineering Department of KFUPM from 2012 to 2016. Prior to that, in 2011, he was a lecturer in Princess Nourah bint Abdulrahman University and Imam Muhammad ibn Saud Islamic University, Riyadh, Saudi Arabia. He is currently an assistant professor in the computer science and information systems department of AlMaarefa University, Riyadh, Saudi Arabia. His research interests include software process improvement, modeling, and intelligent systems.

Eman Abdelfattah received her Ph.D. degree in Computer Science and Engineering from University of Bridgeport in Fall 2011. She received master's degree in Computer Science from University of Bridgeport in 2002. She is currently an Assistant Professor of Computer Science at Ramapo College of New Jersey. Her research interests are in the areas of Network Security, Machine Learning, Data Analytics, Mobile, and Wireless Communications.

Article submitted 2020-02-24. Resubmitted 2020-03-27. Final acceptance 2020-03-29. Final version published as submitted by the authors.