Received: 11 July 2020 | Revised: 30 July 2020 | Accepted: 2 August 2020

DOI: 10.1002/spy2.132

RESEARCH ARTICLE

WILEY

An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method

Shweta Sankhwar[1] | **Dhirendra Pandey**[1] | **Raees Ahmad Khan**[1] | **Sachi Nandan Mohanty**[2]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India

[2]Department of Computer Science and Engineering, IcfaiTech, ICFAI Foundation for Higher Education, Hyderabad, India

Correspondence
Sachi Nandan Mohanty, Department of Computer Science and Engineering, IcfaiTech, ICFAI Foundation For Higher Education, Hyderabad, India.
Email: sachinandan09@gmail.com

Abstract

Phishing in an enterprise is serious issue rising in wide scale and complexity, as phishers use email phishing via obfuscated, malicious or phished URLs and continuously adapt or innovate their strategies to lure victims for identity theft for financial benefits. To gain victim's trust and confidence phishers have started using visceral factors and familiarity cues. Phishing is not always money centric; phisher defame the user's goodwill and character. Defamation in enterprise could be much more traumatic than being embarrassed at a social networking site. It is a challenging task to address this issue. It is evident through literature review that single phishing detection filter approaches are insufficient to detect phishing in enterprise environ. Therefore, a novel anti-phishing model for enterprise using artificial neural network is proposed. In addition, this model effectively identifies whether the phishing email is known phishing or unknown phishing to reduce the trust and familiarity-based email phishing enterprise environ. The feed-forward backpropagation and Levenberg-Marquart methods of ANN are adopted to enhance the URL classification process and with Fuzzy Inference System to get result with imprecise data of social features. The proposed model can accurately classify the known and unknown email phishing via URLs.

KEYWORDS

authentication, E-mail phishing, enterprise cyber threat, machine learning techniques, privacy models for communication systems communication security, security and privacy in mobile communication services, social engineering

1 | INTRODUCTION

In digital era, email phishing is a critical issue causing loss of finance during online transactions. At present, different anti-phishing approaches are being proposed to detect email phishing attacks. Despite the various developed anti-phishing approaches are profoundly incompetent to tackle the real-time hassles. In literature review, a group of researchers argued upon about URLs blacklisting, which are mostly used in industry or organizations but not well off to

detect email phishing attacks with accuracy. The main reason, why still phishing attacks prevails is due to lack of computer operational knowledge and unawareness of cyber threats among internet users.[1] Many internet users still remain unacquainted of recognizing phishing emails.[2-4]

Therefore, this article is focused on email phishing detection in an enterprise. There are a number of possible research findings present with email phishing detection systems or models with sophisticated machine learning techniques to meet out the challenges. Currently, the security mechanism broadly classifies into two categories. One is list-based approach and other is heuristic-based approach. List-based approach assesses the existence of the legitimate website and accordingly stores in the predefined list which includes blacklist or white list or both.[5] On the other hand, heuristic-based approach is based on some distinctive features of phishing website or malicious URLs to facilitate the detection and identification of phishing website.[6] Heuristic-based model is designed to detect email phishing via URLs (obfuscated, malicious or phished URLs) using Naïve Bayes and Support Vector Machine classifiers. This model includes a URL detection algorithm which efficiently detects phishing and legitimate URLs. Research evidences suggest that the use of rule base phishing detection method has application in industry for identifying phishing attacks to analyze website information. As of now, many different phishing filtering approaches are existing with ML techniques such as logistic regression, Support Vector Machine, Markov Model, decision tree, and random forest for detecting phished URLs/links.[7,8] In this chapter, a novel approach for email phishing detection in enterprise environ is proposed with ANN.

The paper is organized in total nine sections: Section 1 introduces the paper, Section 2 is literature review, Section 3 propose novel anti-phishing approach consequently with URLs feature set and social feature set in Sections 4 and 5. Section 6 gives basic description of techniques used for email phishing classification and alert which is employed in implementation of proposed approach phase I in Section 7. Sections 7 and 8 result and discussion followed by performance evaluation of phase I and phase II of proposed approach, respectively. At last, the Section 9 concludes the paper.

2 | LITERATURE REVIEW

Since the last decade, social networking has come into lime light and has drawn users' remarkable standard of attention towards it. Social Networking refers to web-based services which allow users to connect with other users within their specific arena. Creation of profiles which could be public or protected are both meant to socially link with others in acquaintance or randomly. Social networking has emerged as a significant mode of online conferencing and sharing and exchanging contents or personal data, approaches, sentiments, opinion expression and feelings, and so on. The reliance and inclination of more and more users towards e-communication and social networking for information, news, opinions and other diverse matters has caught the eyes of phishers and has lured them towards the same.[6,9]

In enterprises environ, phishers gather internal information about the enterprise, names of collogues, relevant post to craft tailor-made emails which would contain a phished/malicious URLs/links. Looking at the reference/source of this email the victim automatically believes the authenticity and falls prey. This type of attack crafted by phishers and called as in insider attack in the enterprise environ. The attackers often disguise as a trustworthy and genuine entity and build contacts with their targets (naive user/employee) through email and social media. Often, they tend to attack a random individual or enterprise itself.[10] The individual attacks may pose specific spurious emails or post of an individual's concern or interest like using the posted official details of travel plans or reimbursement sanction, awards and promotion related with enterprise protocols and others, asking confirmation of debit/credit card details, username, password, desk number, date of birth, and so on.[11]

When it comes to the phishing attack in an enterprise, the boomerang thrown by attackers is usually the business email or familiarity cues. The targeted emails in this concern are sent to employees appearing to have sent from enterprise executives or IT staff ordering them to make wire transfers. The sly attackers already do their homework about gathering user data and acquiring information details of the working structure of enterprise with foreign associates or firms with which their instruction and actions are unquestioned or undoubted by the enterprise personnel.[12] This states that the phishing attacks executed through social engineering comprises four steps:

- Collating information and fake pretenses.
- Developing relationship or nexus.
- Exploitation of identified vulnerabilities.
- Execution of phishing attack.

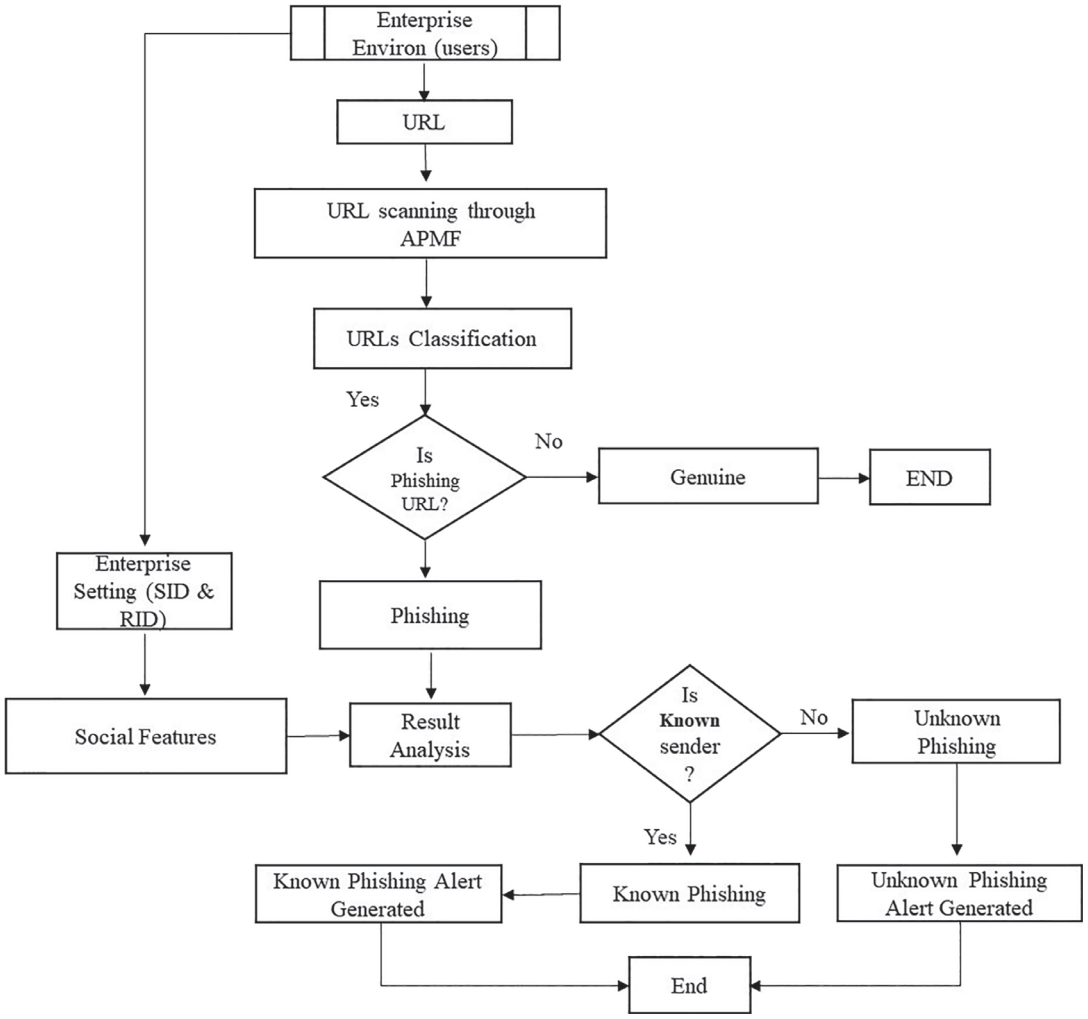

FIGURE 1 Architecture of anti-PhiEE model

3 | PROPOSED APPROACH FOR E-MAIL PHISHING DETECTION

An Anti-Phishing in Enterprise Environ (Anti-PhiEE) is integrated Approach to Detect Email-Phishing through malicious URLs in Enterprise Environ. Anti-PhiEE is an email phishing detection model as shown in Figure 1. Anti-Phishing Multi-Filter (APMF) is developed with 25 heuristics that work as multi-layer filters.[7] APMF consists of five layers which are used to discriminate between the legitimate and phished URLs. APMF is consist of five layers, that is, Page Ranking, URL Property Values, Suspicious URL Forms or Patterns, Google suggestion for URL Authenticity and Social Feature Set (social human factor scanner) to identify the known and unknown phishing.

Pertinent 25 heuristics is identified through the exhaustive literature review, statistical investigations and analysis on phished and legitimate URLs/websites.[7,13] The implementation of this model is done in two phases. In phase I, Backpropagation learning algorithm and TRAINLIM (ie, Levenberg-Marquardt [LM] backpropagation) algorithm is employed. The Artificial neural network methods feed-forward backpropagation neural network (FFNN) and LM neural network basically used for URLs classification. In phase II, Fuzzy rule-based system (FRBS) is used for Social facet filter with Mamdani FIS method to determine the known and unknown phishing.

4 | URL FEATURE SET

Heuristics approach is used to discriminate phishing URL/websites and legitimate URLs/webpage/links. Based on Advanced pertinent threats the phishing heuristics is identified; through the exhaustive literature review, statistical

TABLE 1 Suspicious URL forms or patterns

Heuristics	Description
IP Address, hexadecimal or ASCII code in URL	If URL in the form of IP Address, If URL in the form hexadecimal or Unicode.
Abnormal URL	URL—phishing page redirection
No. of subdomain	Length of sub domain
No of Dot "." In URL	More than 5 dots in URL
URL of length	Length of URL
Special characters	Whether URL has "-", "@" symbol or "//"
Phishing keyword	Phishing words as a hyperlink like verify, click here, submit, login, sign-in, and so on
Age of domain (in days)	Domain is less than 43 days
Port number matching	Whether explicit port number and protocol port no. are equal.
Number of TLDs	More than one TLD in a URL
Primary domain spelling mistakes	Whether primary domain is
Number of Slash "/"	Number of "/" slash
Login form	Login Form in Fake webpage

TABLE 2 URL property values

Heuristics	Description
Country matching	TLD country and domain country-code are equal.
HTTPS protocol	Whether URL use HTTPS or not.
DNS record	Whether URL has DNS record or not.
Reverse DNS look-up	Query of DNS to determine the domain associated with an IP Address.
WHOIS record	WHOIS record (Domain name, Registration, Expiry details etc.)
Value of TTL	TTL value of domain.
PTR record	Whether domain has PTR record or not.

investigations and analysis on phishing and legitimate websites or URLs.[5,8,14-22] Total 25 Heuristics are defined here to effectively determine the legitimate and phished URL listed as follows.

4.1 | Suspicious URL forms or patterns

These Heuristic are associated with Suspicious URL forms or patterns and symbols, The Characters such as "@" and more than one time "//" rarely appear in a URL.[23,24] The legitimate sites have one TLD so if URL containing more than one considered as phishing site. Phishing sites have very less life-time as get block listed. Fake Login form in a phishing page is a dangerous sign of loss money or sensitive information as listed in Table 1.[13,14,16,23-36]

4.2 | URL property values

These heuristics are based on URL Property Values for identification of phishing URL/website.[5,13] The fake or temporary phishing a site does not contains required properties as listed in Table 2.[37,38]

TABLE 3 Page ranking

Heuristics	Description
Google page rank (Indexing)	Domain's PageRank value
Alexa rank	Alexa rank value of domain
Alexa reputation	Alexa reputation value of domain

TABLE 4 Google suggestion for URL authenticity

Heuristics	Description
Similarity of primary Domain and Google suggestion	Levenshtein distance between primary domain and Google Suggestion
Similarity of Subdomain and Google suggestion (subdomain)	Levenshtein distance between primary domain and Google Suggestion
Safety of Google Suggestion for Primary domain	To check Google Suggestion result of Primary domain is present in the whitelist or not
Safety of Google Suggestion for Subdomain	Google Suggestion result of Subdomain is present in the whitelist or not

4.3 | Page ranking

These heuristics are based on page ranking, it is a numerical value calculated by the number of visitors and degree of popularity.[39,40] It is seen that the phishing site has very low page rank value as rarely visited by bulk users and these sites are exist for less time. Therefore, domain page rank value is very low as mentioned in Table 3.

4.4 | Google suggestion for URL authenticity

These heuristics are made on the idea of Google suggestion with existing algorithms to match or compare the String.[41] String matching algorithms are used to detect phishing URLs as listed in Table 4. When a user enters a single term in Google suggested word is returned. Using this idea of entering the URLs of phishing sites and legitimates sites for Google suggestion the result analysis done.[42,43]

If URL of phishing sites is searched and is similar to suggested result, the input URL is considered as suspicious as the site could be emulating an existing site. The URL as a string is considered in APMF and two well-known string-matching algorithms (source: Damerau-Levenshtein edit distance and Longest Common Subsequence) are employed to assess the similarity between two strings on the ground of different acts.[42,44]

5 | SOCIAL FEATURE SET

It is featured and demonstrated that the behavioral aspects are taken from the information of email header. The proposed heuristic has been used in this regard to identify and discriminate between the known and unknown phishing attacks in Enterprise Environ as follows.

5.1 | Social media contacts (X_1)

In this heuristic, friendship on social media account of Sender (S_id) and Receiver (R_id) with help of their email's IDs can be identified. It has been observed through the trend of fraudulent activities and the brainstorming discussion with experts and professionals that mostly Primary ID is used for both Email Service Provider as well as on Social Media. There is always a possibility that someone who is a rightful worker associated of the relevant is an enterprise insider threat, fraudster or phisher and, in this case, they can easily send the phishing email from within the arena.

5.2 | Social media common contact (X_2)

In this heuristic, targeting the common friend that means friends of friend's social media account is identified. Adversary or insider threat do social engineering, for instance, peering into the social media friend list of targets. Adversary tries to gain trust from targets or naive user. They gather information from friends of the target via social media through scraps, post, pages to launch the attack on email. Illustration, if the Boss is friend of naïve user and Boss's Personal Secretory is common friend. He does social engineering and launches the email phishing attack with the content and URL showing his/her Boss instruction.

5.3 | Social media common activities (X_3)

To catch the eyes of user the phisher involve and caste themselves into the same swing of user which may grab user's attention. For instance, liking the same post, pages and stuff on social media which user likes or declaring to visiting an event on social media site in which the user has shown interest. Further, volunteering or participating in specific professional project or a social task or cause like becoming a blood donor in which the user has also applied for. So, it simply means the phishers try to make an analysis of target's behavior in depth and grabbing their attention by literally chasing them on social media but not approaching them straight away however, at the same time being visible in the sight of users constantly by their parallel activities in order to make the user feel that they both are on the same boat or likely to be in the same swing.

5.4 | Frequency of email communication (X_4)

Suppose, an employee in enterprise has not registered himself on social media so it becomes difficult to identify known and unknown phishing. Thereby, this heuristic is coined to check the Frequency of email communication so as to identify known phishing or unknown phishing through the means of Email Service Provider (ESP Contact list) as well as frequency of email communication between sender and receiver through the threshold value 1 (T_t).

6 | BASIC DESCRIPTION OF TECHNIQUES USED FOR EMAIL PHISHING CLASSIFICATION AND PHISHING ALERT

6.1 | Basic principle of artificial neural network

An artificial neural network (ANN) is based on mimicry of human brain having basically three parts receiving the input from the surrounding called input layers and number of nodes (processing element) connected each other for transforming signal as a data is also called hidden, intermediate layer. In this research, we have implemented multi-layer feed forward neural network.[15,41] We have used FFNN for analysis.

FFNN consists of one and more hidden neural layer. In feed-forward learning algorithm, we have used 10 sigmoid algorithms for training process as shown in Figure 2. The number of hidden layers and their respective number of neurons depends upon the nature and complexity of the problem being mapped by neural network. The amount of output signal will always be précised with number of neurons from their respective layers.[15,45] We have also used LM Neural Network for data analysis. The LM algorithm is an approximation to the Newton method used for training ANNs.

6.2 | Fuzzy rule-based systems

A Knowledge Base (KB) and Inference Engine (IE) are two main components of FRBS. There are various ways to represent knowledge. Perhaps the most common way to represent human knowledge is to form it into natural language expression.[46] KB generally represents the knowledge about the problem being solved in the form of fuzzy linguistic IF-THEN rules, and the Inference Engineering (IE), which puts into effect the fuzzy inference process, is needed to obtain an output from the FRBS, when an input is specified. This form in expression is commonly referred to as the IF-THEN rule-based form like IF premise (antecedent), THEN conclusion (consequent) parameters.[47] The schematic view of an FRBS is shown in Figure 4.

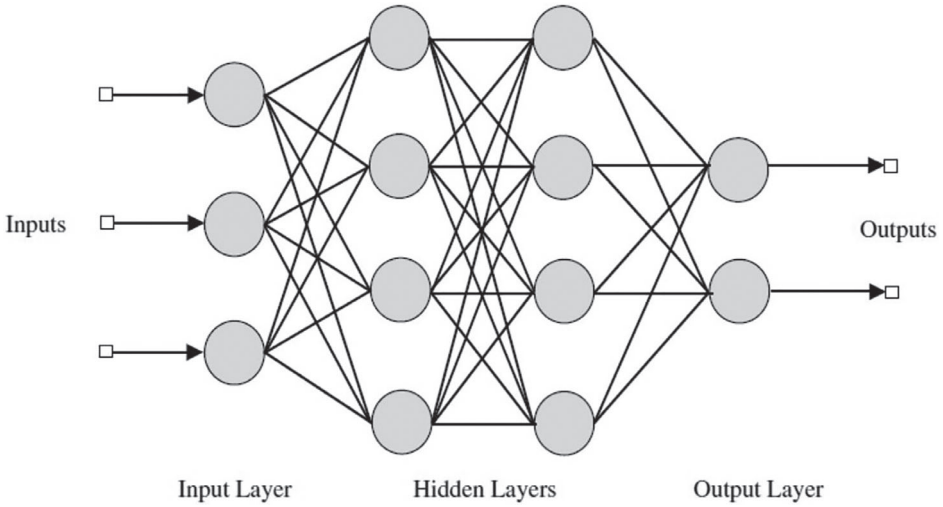

FIGURE 2 25 × 2 input output neural network architecture

An FRBS consists of three modules, namely fuzzification, inference, and defuzzification. Fuzzification is the process, in which the input parameters are converted into appropriate fuzzy sets to express measurement uncertainty. The fuzzified measurements are then used by inference engine to evaluate the control rules stored in the fuzzy rule base and a fuzzified output is determined. The fuzzified output is then converted into a single crisp value. This conversion is called de-fuzzification.[48]

6.3 | Fuzzy linguistic variable and membership functions

Fuzzy linguistic approach provides a systematic way to represent linguistic variables in a natural evaluation procedure.[49] A fuzzy linguistic label can be represented by a fuzzy number, which is represented by a fuzzy set. Fuzzy sets capture the ability to handle uncertainty by approximation methods. A fuzzy set α is represented by a pair of two things—the first one is the element x and the second one is its membership value $\mu\alpha\,(x)$ (varying in the range of [0, 1]), as given below:

$$\alpha = \{(x, \mu_\alpha(x)) : x \in X\}.$$

For the inputs and output, triangular membership functions were used in order to keep the design of the FLCs simple. A degree of overlapping of two was used, as shown in Figure 4. Furthermore, a universe of discourse normalized to the range of [0.0, 1.0] was utilized. This value, called membership value or degree of membership (as given below), quantifies the grade of membership of the element in X to the fuzzy set A.

$$\mu_A(x) = \begin{cases} 0 & x \le a \\ \frac{x-a}{m-a} & a < x \le m \\ \frac{b-x}{b-m} & m < x < b \\ 0 & x \ge b \end{cases} \tag{1}$$

Here, a, b, m are real numbers. In this formula, b and a are the upper and lower values of the support of A, respectively, and m is the median value of A.[50]

6.4 | Working principle of traditional FLC (Mamdani approach)

An FLC consists of a set of rules presented in the form of IF (a set of conditions are satisfied) THEN (a set of consequences can be prepared). Here, antecedent is a condition in its application domain and the consequent is a control action for the system under control. Both the antecedents and consequents of the IF-THEN rules are represented using some linguistic

TABLE 5 Comparison between feed-forward backpropagation neural network (FFNN) and Levenberg-Marquardt (LM) neural network

Different NN architecture	Process	Sample size	RMSE	R^2
Feed-forward backpropagation	Training set	1000	0.28	.92
	Testing sets (10 set each size 100)	1000	0.42	.82
	10-fold cross validation	100	0.24	.94
Levenberg-Marquardt neural network	Training set	1000	0.30	.91
	Testing sets (10 set each size 100)	1000	0.55	.69
	10-fold cross validation	100	0.46	.78

terms.[51] The inputs of FRBSs should be given by fuzzy sets, and therefore, we have to fuzzify the crisp inputs. Moreover, the output of an FLC is always a fuzzy set, and therefore, to get the corresponding crisp value, a method of defuzzification is to be used. The fuzzification of input variables involves the following steps:

1. Measure all the input variables.
2. Perform a scale mapping that transfers the range of values of inputs variables into corresponding universes of discourse.
3. Perform the function of fuzzification that converts input data to suitable linguistic values, which may be viewed as label of fuzzy sets.

The rule base comprises of knowledge of the application domain by using the information of data base. Thus, the data base provides necessary data to design the control rules involving linguistic terms. The rule base characterizes the control goals and policy of the domain experts by means of a set of linguistic control rules.[52] The Inference Engine of an FLC has the capability of simulating human decision-making based on fuzzy concepts and of inferring fuzzy control actions by employing fuzzy implication and the rules. A method of defuzzification is used to obtain the crisp value corresponding to the fuzzified output. In this study, Center of Sums (COS) method of defuzzification was utilized, which is given below:

$$U'_{f'} = \frac{\sum_{j=1}^{P} A(\alpha_j) \times f_j}{\sum_{j=1}^{P} A(\alpha_j)} \tag{2}$$

Where $U'_{f'}$ is the output of the controller, $A(\alpha_j)$ represents the firing area of j-th rule, p is the total number of fired rules and f_j represents the center of the area. Like fuzzy logic control based on Mamdani approach. We have also applied other method called Fuzzy Takagi-Sugeno Inference Engine.[50,53] In this approach, the outcomes of the variables depend upon a function of several input variables. A function may be linear or non-linear depend upon problem specification. We assumed all the features of URLs are dependent each other which is a nature of complex task (nonlinear) for getting output for function.[54] During experiment it is observed that the Mamdani FIS results were quite appropriate than Fuzzy Takagi-Sugeno Inference Engine.

7 | IMPLEMENTATION OF PROPOSED APPROACH PHASE I

The APMF test the collected data of the 2000 phishing URLs and legitimate as input and thereafter, employed to machine learning for evaluation of the performance of APMF. The ANN methods, FFNN and LM Neural Network is used. In both ANN methods, same data set is segregated in the form of training, testing 50%, 50%, respectively. The neural network toolbox of MATLAB version R2016a is used for ANN applications and validation using statistical analysis is done. The result of this approach has been depicted in the Table 5 and in Figures 5 and 6.

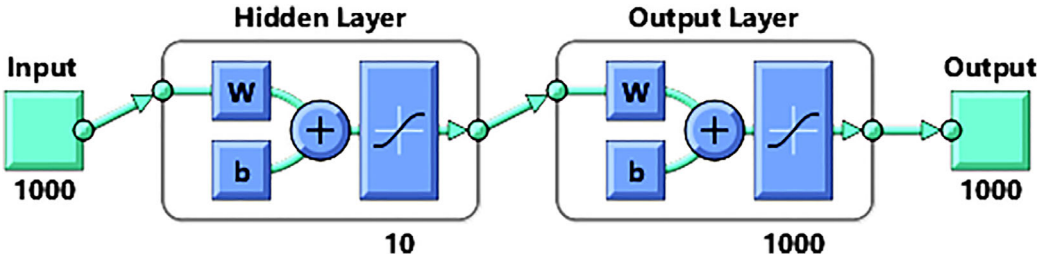

FIGURE 3 Artificial neural network

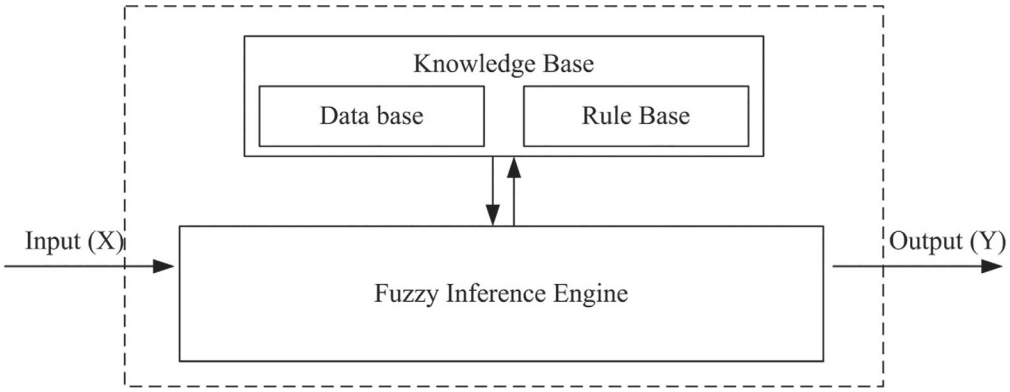

FIGURE 4 A schematic view of an Fuzzy rule-based system (FRBS)

7.1 | Data set

The collected data set is online data of the 2000 phishing URLs and legitimate. Specifically, the distribution ratio of phishing and legitimate data is in 60:40 ratio, respectively. Phishing URLs data source is Phishing tank and legitimate URLs data source is DMOZ and Alexa.[55,56] In both ANN methods, same data set is segregated in the form of training, testing 50%, 50%, respectively. The result of this approach has been depicted in the Table 5 and Figures 5 and 6.

7.2 | Performance evaluation

In order to demonstrate the overall performance of the study experiments performed on two aspects: The performance of both the methods where measured using root mean square error (RMSE) and R^2 value. The result of both the methods are shown in Table 5. For getting the accuracy of classifier with small data set, k-fold Cross-Validation is adapted. k-fold cross-validation is used for validation of proposed phishing detection techniques. The total 2000 data set divided into 10 smaller data sets with equal size. This data set is used for training, testing, validation. 10-fold cross-validation is applied in both FFNN and LM Neural Network.

7.3 | Result and discussion of phase I

In both the approaches we have considered 50% of input data as a training set and 50% as a testing set. The method FFNN result reveals that the RMSE is 0.28 in case of training with R2 Value 0.92, whereas the testing error was less than 20% with R^2 value .82. 10-fold cross-validation method used to validate the model. Similarly, the result of LM Neural Network RMSE having 0.3% with R^2 value .91. In comparison of both the methods FFNN yield quiet precise result are shown in Table 5. This optimization technique is more powerful than standard Backpropagation Neural Network (BPNN). LM algorithm is very efficient and fast, having also a quite good global convergence property. For these reasons, LM algorithm is used in this research as shown in Figure 3.[45,46]

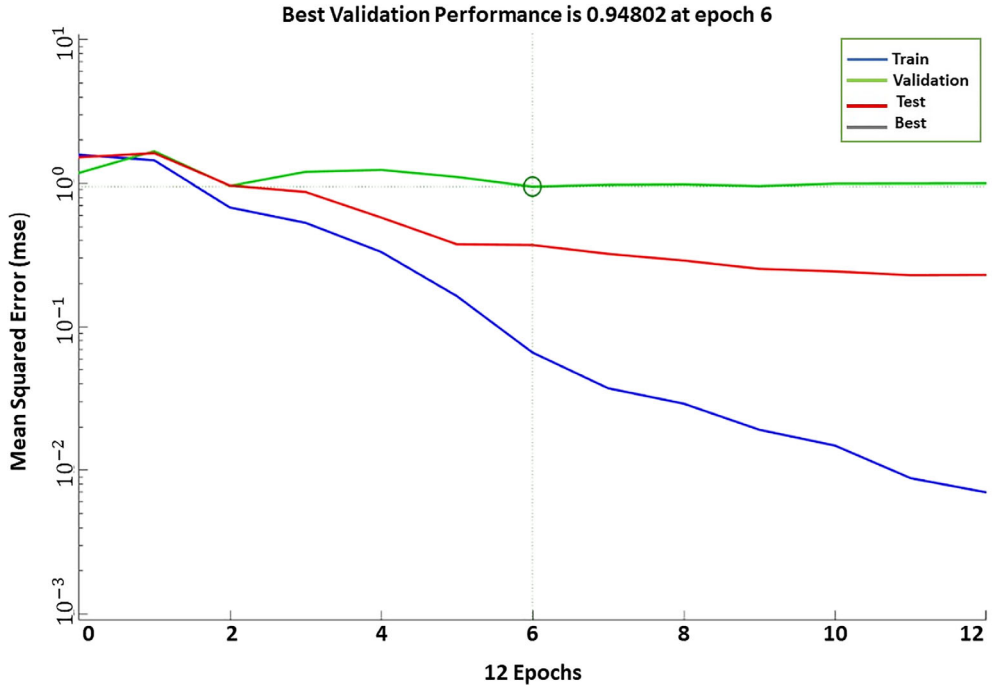

FIGURE 5 Performance of feed-forward backpropagation neural network

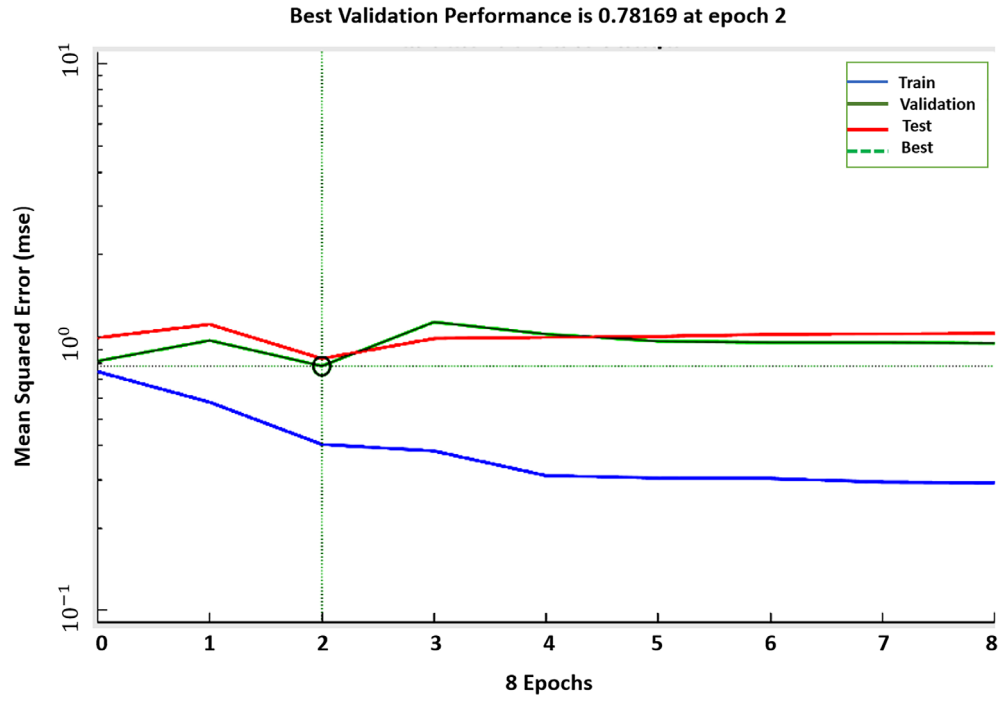

FIGURE 6 Performance of Levenberg-Marquardt neural network

8 | IMPLEMENTATION OF THE PROPOSED APPROACH PHASE II

As we already executed the phase I of proposed approach and achieved 94% performance in terms of accuracy in phishing detection. In this phase II, the known and unknown phishing are determined. Therefore, same approach is applied in real world data of and an enterprise which has combined data of email and social media contacts. The neural network toolbox of MATLAB version R2016a is used for ANN applications and validation by statistical analysis [109]. In this study, Mamdani FIS method is used with four linguist variables such low, medium, high, and very high each having input variable, that is, X_1, X_2, X_3, and X_4 (Section 5).

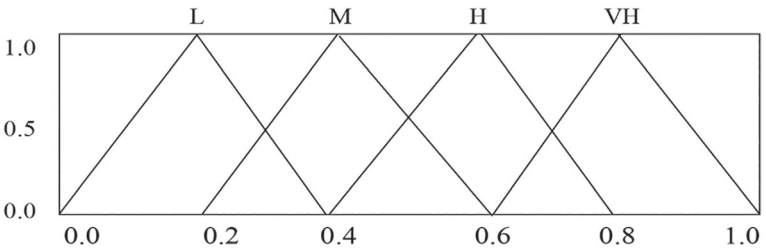

FIGURE 7 Membership function distributions for the variables

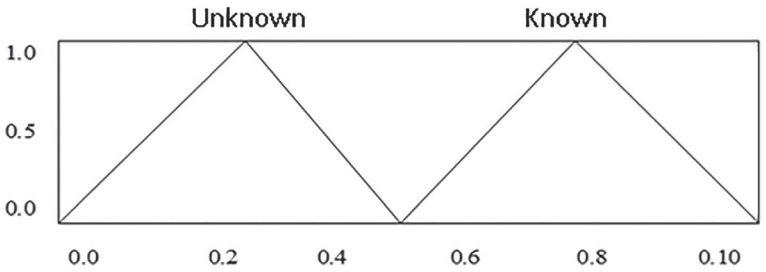

FIGURE 8 Membership function distributions for output fuzzy variable

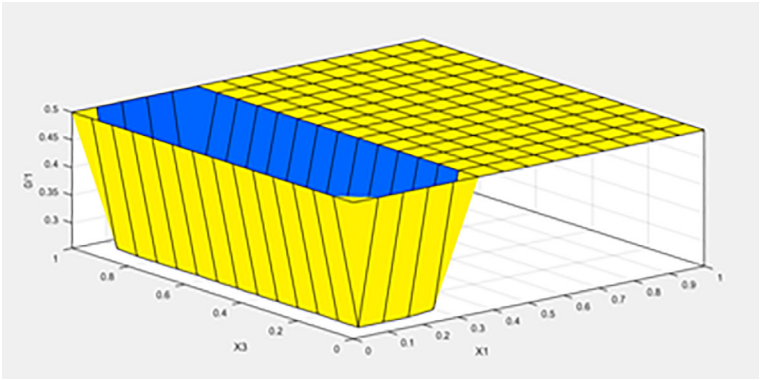

FIGURE 9 Social media contacts (X_1) vs social media common contacts (X_2)

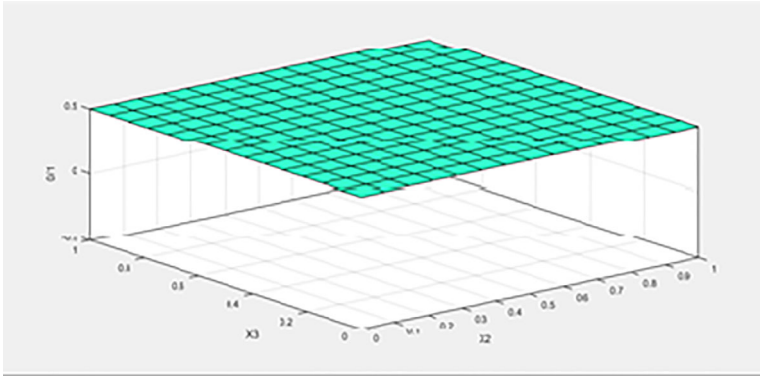

FIGURE 10 Social media common contacts (X_2) vs common activity in social media (X_3)

8.1 | Data set

Data set has been collected from real world data to check whether the sender is the known and unknown for known and unknown phishing attacks. Implementation is done on total 2000 emails with corresponding 2000 social media contacts of an enterprise. The source of all the data are originated from a real enterprise of Software Development and Training, Private Limited.[57]

TABLE 6 Linguistic term and their range

Linguistic terms	Membership function	Range of parameter
Low (L)	Trimf	[0.0, 0.4]
Medium (M)	Trimf	[0.2, 0.6]
High (H)	Trimf	[0.4, 0.8]
Very High (VH)	Trimf	[0.6, 1.0]

TABLE 7 Description of fuzzy linguistic term

Abbreviation	Expression	Index representation
L	Low	0.25
M	Medium	0.35
H	High	0.55
VH	Very High	0.85

8.2 | Description of fuzzy input and output variables

Description of fuzzy input variables: The input fuzzy variables are $X_1 = \{\text{Social Media Contacts}\}$, $X_2 = \{\text{Social Media Common Contacts}\}$, $X_3 = \{\text{Common Activity in Social Media}\}$, $X_4 = \{\text{Times of Email Communication}\}$ and each of them was represented using four linguistic term low (L), medium (M), high (H), and very high (VH). The linguistic term and their ranges are shown in the Figure 7.

Linguistic term and their range for the variables are $X_1 = \{\text{Social Media Contacts}\}$, $X_2 = \{\text{Social Media Common Contacts}\}$, $X_3 = \{\text{Common Activity in Social Media}\}$, $X_4 = \{\text{Times of Email Communication}\}$ mentioned in Table 6.

Description Fuzzy output variables: Membership function distributions for output fuzzy variable are $X_5 = \{\text{Known Phishing (1)/Unknown phishing (0)}\}$ which is crisp in nature as shown in Figure 8.

Determining fuzzy rule base from input and output variables: Rules are the core of the FRBS which represent the relationship between inputs and output. In the present problems, four input variable were considered and each of them was represent using four linguistic terms. Thus, there could be maximum of rules in the FRBS. In this study, 256 fuzzy rules ($4 \times 4 \times 4 \times 4 = 256$) are generated. For instance, the first and last rule as follows.

R_1 : If X_1 is L AND X_2 is L AND X_3 is L AND X_4 is L THEN output is *Known Phishing*
Similarly,
$\vdots$
R_{256} : If X_1 is VH AND X_2 is VH AND X_3 is VH AND X_4 is VH THEN output is *Unknown Phishing*.

Fuzzy rules and coding: Four input variables are in this section each have four linguistic terms which constitute 64 rules. Linguistic terms are denoted with their index value as listed in the Table 7.

8.3 | Result and discussion of phase II

The traditional fuzzy reasoning tools was developed using four inputs namely Social Media Contacts, Social Media Common Contacts, Common Activity in Social Media, Times of Email Communication and each having four different responses (ie, Low, Medium, High, Very High) a set of 256 rules designed manually for analysis of the result. The result of this approach suggested that Social Media Contacts (X_1) and Social Media Common Contacts (X_2) are more influenced the output variable known and unknown person (S_id & R_id) refer Figure. 9 whereas other input variables are Common Activity in Social Media (X_3), and Social Media Common Contacts (X_2) are that much more influenced output variables as shown in Figure 10. The outcome variables depend detection of phishing URL and Enterprise Environ. This shows that the Social media common contact and social medial common activity are most used Social facets used to launch phishing attack.

9 | CONCLUSION

Phishing is a catastrophic enterprise risk which relies on decentralized decision making of enterprise's employees. For example, enterprise environ security risk depends on quite an extent over the response and reversion to phishing attacks laid. The most alluring target for the phishers here is the enterprise employees or personnel. Employees Behavioral towards internet usage shows lay decision making, that is the reason, victims typically deviate from systematic measure of rationality and get into trap of phishers. As the phishers plot successful deceptions over employee peripheral route permission and shun direction logical argumentation. Further, manipulating splanchnic emotions, that is, fear, lust, greed, pity, anxiety urgency and acquainted contextual cues play a major role in persuasion or undermining the employee's confidence as well as trust to proceed towards the snares laid by the hoodwinkers. In this research, a novel anti-phish model is proposed and implementation of the proposed model is done in two phases, in first phase, performance of the model is measured using two different methods of ANN, that is, FBNN and LM neural network by training and testing the data set. The results show the advantages of FBNN over LM neural network in terms of RMSE and R^2 value. feed-forward back-propagation approach was able to yield better results as compared to other one. It might happen to the reason of each processing element of neural network properly trained with optimized weight. In the second phase, adoption of Mamdani FIS with four social features (Social Media Contacts, Social Media Common Contacts, Common Activity in Social Media, Frequency of email communication) are used for detection of known and unknown e-mail sender in enterprise environ. Finally, in both the output of two phase, combined used as input to method to determine unknown or known phishing e-mail sender. The result of this approach suggested that Social Media Contacts (X_1) and Social Media Common Contacts (X_2) are more influenced the output variable known phishing attack whereas other input variables are Common Activity in Social Media (X_3), and Social Media Common Contacts (X_2) are that much more influenced output variables. The outcome variables depend detection of phishing URL and Enterprise Environ. This shows that the Social media common contact and social medial common activity are most used Social facets (features) used to launch email phishing.

ORCID

Shweta Sankhwar https://orcid.org/0000-0003-0743-6854
Raees Ahmad Khan https://orcid.org/0000-0002-9454-1312
Sachi Nandan Mohanty https://orcid.org/0000-0002-4939-0797

REFERENCES

1. Shankhwar S, Pandey D, Khan RA. Phishing prevention guidelines. *Big Data Analytics and Computing for Digital Forensic Investigations*. Boca Raton, FL: CRC Press; 2020:171-181.
2. Krombholz K, Hobel H, Huber M, Weippl E. Advanced social engineering attacks. *J Inform Secur Appl*. 2015;22:113-122. https://doi.org/10.1016/j.jisa.2014.09.005.
3. Stolfo S, Hu C-W, Li W-J, Hershkop S, Wang K, Nimeskern O. Combining behavior models to secure email systems. 2003. doi:https://doi.org/10.7916/D8F47VVN
4. Sankhwar S, Pandey D. Defending against phishing: case studies. *Int J Adv Res Comput Sci*. 2017;8(5):2605-2607.
5. McGrath DK, Gupta M. Behind phishing: an examination of phisher Modi operandi. *LEET*. 2008;8:4.
6. Cialdini RB. The science of persuasion. *Sci Am*. 2001;284(2):76-81.
7. Sankhwar S, Pandey D, Khan R. Email phishing: an Enhanced classification model to detect malicious URLs. *EAI Endorsed Trans Scalable Inform Syst*. 2019;6(21):e5.
8. Medvet E, Kirda E, Kruegel C. Visual-similarity-based phishing detection. Paper presented at: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks-SecureComm '08. ACM Press; 2008: doi:https://doi.org/10.1145/1460877.1460905
9. Wang M-F, Tsai M-F, Jheng S-L, Tang C-H. Social feature-based enterprise email classification without examining email contents. *J Netw Comput Appl*. 2012;35(2):770-777.
10. Keshtkar F, Inkpen D. Using sentiment orientation features for mood classification in blogs. Paper presented at: 2009 International Conference on Natural Language Processing and Knowledge Engineering; 2009;1-6.
11. Kim Y, Hsu S-H, de Zúñiga HG. Influence of social media use on discussion network heterogeneity and civic engagement: the moderating role of personality traits. *J Commun*. 2013;63(3):498-516.
12. Wakker PP. *Prospect theory: for risk and ambiguity*. Cambridge: Cambridge University Press; 2010.
13. Almomani A, Gupta B, Atawneh S, Meulenberg A, Almomani E. A survey of phishing email filtering techniques. *IEEE Commun Surv Tutor*. 2013;15(4):2070-2090.
14. Chandrasekaran M, Narayanan K, Upadhyaya S. Phishing email detection based on structural properties. Paper presented at: NYS Cyber Security Conference. Vol 3. Albany, New York; 2006.

15. Kotsiantis SB, Zaharakis I, Pintelas P. Supervised machine learning: a review of classification techniques. *Emerg Artif Intell Appl Comput Eng*. 2007;160:3-24.
16. Fette I, Sadeh N, Tomasic A. Learning to detect phishing emails. Paper presented at: Proceedings of the 16th International Conference on World Wide Web; 2007, pp. 649–656.
17. Shah R, Trevathan J, Read W, Ghodosi H. A proactive approach to preventing phishing attacks using Pshark. Paper presented at: 2009 Sixth International Conference on Information Technology: New Generations. 2009, pp. 915–921.
18. Xiang G, Hong J, Rose CP, Cranor L. CANTINA+: a feature-rich machine learning Framework for detecting phishing web sites. *ACM Trans Inf Syst Secur*. 2011;14(2):1-28. https://doi.org/10.1145/2019599.2019606.
19. Zhang J, Porras PA, Ullrich J. Highly predictive blacklisting. Paper presented at: USENIX Security Symposium; 2008, pp. 107–122.
20. G Aaron, R Rasmussen. Anti-Phishing Working Group. Global Phishing Survey, Trends and Domain Name Use in 2H2011. https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf
21. Center RA-FC. RSA monthly online fraud report, May 2012.
22. Sankhwar S, Pandey DA. Comparative analysis of anti-phishing mechanisms: email phishing. *Int J Adv Res Comput Sci*. 2017;8(3):567-574.
23. Yearwood J, Mammadov M, Webb D. Profiling phishing activity based on hyperlinks extracted from phishing emails. *Soc Netw Anal Min*. 2012;2(1):5-16.
24. Suriya R, Saravanan K, Thangavelu A. An integrated approach to detect phishing mail attacks: a case study. Paper presented at: Proceedings of the 2nd International Conference on Security of Information and Networks; 2009, pp. 193–199.
25. Netcraft Anti-Phishing Toolbar. Netcraft. 2004. https://news.netcraft.com/archives/2004/12/28/netcraft_antiphishing_toolbar_available_for_download.html.
26. Gansterer WN, Pölz D. E-mail classification for phishing defense. Paper presented at: European Conference on Information Retrieval, Springer; 2009, pp. 449–460.
27. Firake SM, Soni P, Meshram B. Tool for prevention and detection of phishing E-mail attacks. Paper presented at: *International Conference on Network Security and Applications*, Springer; 2011, pp. 78–88.
28. Al-Momani A, Wan T-C, Al-Saedi K, et al. An online model on evolving phishing e-mail detection and classification method. *J Appl Sci*. 2011;11(18):3301-3307.
29. Almomani A, Wan T-C, Altaher A, et al. Evolving fuzzy neural network for phishing emails detection. *J Comput Sci*. 2012;8(7):1099.
30. Malaysia U. An enhanced online phishing E-mail detection framework based on evolving connectionist system.
31. Nguyen LAT, To BL, Nguyen HK, Nguyen MH. A novel approach for phishing detection using URL-based heuristic. Paper presented at: 2014 International Conference on Computing, Management and Telecommunications (ComManTel); 2014, pp. 298–303.
32. Smadi S, Aslam N, Zhang L, Alasem R, Hossain M. Detection of phishing emails using data mining algorithms. Paper presented at: 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA); 2015, pp. 1–8.
33. Gupta BB, Tewari A, Jain AK, Agrawal DP. Fighting against phishing attacks: state of the art and future challenges. *Neural Comput Applic*. 2017;28(12):3629-3654.
34. Jayakanthan N, Ramani A, Ravichandran M. Two phase classification model to detect malicious URLs. *Int J Appl Eng Res*. 2017;12(9):1893-1898.
35. Chandrasekaran M, Chinchani R, Upadhyaya S. PHONEY: Mimicking user response to detect phishing attacks. Paper presented at: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06). 2006, pp. 668–672. doi:https://doi.org/10.1109/WOWMOM.2006.87
36. Herzberg A. DNS-based email sender authentication mechanisms: a critical review. *Comput. Secur.* 2009;28(8):731-742.
37. Bedingfield Sr JC, Gehl JM. Substitute Uniform Resource Locator (URL) Generation. Google Patents; 2012.
38. Berners-Lee T, Masinter L, McCahill M, et al. Uniform resource locators (URL). 1994.
39. Page L, Brin S, Motwani R, Winograd T. *The Pagerank Citation Ranking: Bringing Order to the Web*. Stanford, CA: Stanford InfoLab; 1999.
40. Baeza-Yates R, Davis E. Web page ranking using link attributes. Paper presented at: Proceedings of the 13th International World Wide Web Conference on Alternate Track Papers & Posters. 2004, pp. 328–329.
41. Mohammad R, McCluskey T, Thabtah FA. Predicting phishing websites using neural network trained with back-propagation. Paper presented at: World Congress in Computer Science, Computer Engineering, and Applied Computing; 2013.
42. Damerau FJ. A technique for computer detection and correction of spelling errors. *Commun ACM*. 1964;7(3):171-176.
43. Phelps TA, Wilensky R. Robust hyperlinks and locations. *D-Lib Mag*. 2000;6(7/8):1082-9873.
44. Levenshtein VI. Binary codes capable of correcting deletions, insertions, and reversals. *Soviet Phys Doklady*. 1966;10:707-710.
45. Mitchell R, Michalski J, Carbonell T. *An Artificial Intelligence Approach*. New York: Springer; 2013.
46. Jang J-SR, Sun C-T, Mizutani E. Neuro-fuzzy and soft computing-a computational approach to learning and machine intelligence [book review]. *IEEE Transactions on Automatic Control*. 1997;42(10):1482-1484.
47. Yazdanbakhsh O, Dick S. A systematic review of complex fuzzy sets and logic. *Fuzzy Set Syst*. 2018;338:1-22.
48. Nauck D, Kruse R. Neuro-fuzzy systems research and applications outside of Japan. In: Guyon I, Nikravesh M, Gunn S, Zadeh LA, eds. *Feature Extraction. Studies in Fuzziness and Soft Computing*. Vol 207. Berlin, Heidelberg: Springer; 1996:108-134.
49. Buckley JJ, Hayashi Y. Fuzzy neural networks: a survey. *Fuzzy Set. Syst.* 1994;66(1):1-13.
50. Negnevitsky M. *A guide to intelligent systems. Artificial Intelligence*. 2nd ed. London: Pearson Education; 2005.
51. Alali M, Almogren A, Hassan MM, Rassan IA, Bhuiyan MZA. Improving risk assessment model of cyber security using fuzzy logic inference system. *Comput Secur*. 2018;74:323-339.

52. Srivastava PK, Bisht DC. Recent trends and applications of fuzzy logic. *Advanced Fuzzy Logic Approaches in Engineering Science*. Hershey, PA: IGI Global; 2019:327-340.
53. Back S, LaPrade J. The future of cybercrime prevention strategies: human factors and a holistic approach to cyber Intelligence. *Int J Cybersecur Intell Cybercrime*. 2019;2(2):1-4.
54. Sahingoz OK, Buber E, Demir O, Diri B. Machine learning based phishing detection from URLs. *Expert Syst Appl*. 2019;117:345-357.
55. Phishing Tank. https://www.phishingtank.com
56. Alexa Topsites datasource. https://www.alexa.com/topsites.
57. Askysoftware Development Pvt. https://www.askysofware.com.

How to cite this article: Sankhwar S, Pandey D, Khan RA, Mohanty SN. An anti-phishing enterprise environ model using feed-forward backpropagation and Levenberg-Marquardt method. *Security and Privacy*. 2020;e132. https://doi.org/10.1002/spy2.132