ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

Intelligent Detection for Cyber Phishing Attacks using Fuzzy Rule-Based Systems

Phoebe Barraclough and Gerhard Fehringer

Computer Science and Information Sciences, Northumbria University, Newcastle Upon Tyne, NE1 8ST, United Kingdom

ABSTRACT: Cyber phishing attacks are increasing rapidly, causing the world economy monetary losses. Although various phishing detections have been proposed to prevent phishing, there is still a lack of accuracy such as false positives and false negatives causing inadequacy in online transactions. This study constructs a fuzzy rule model utilizing combined features based on a fuzzy inference system to tackle the foreseen inaccuracy in online transactions. The importance of the intelligent detection of cyber phishing is to discriminate emerging phishing websites with a higher accuracy. The experimental results achieved an excellent accuracy compared to the reported results in the field, which demonstrates the effectiveness of the fuzzy rule model and the feature-set. The findings indicate that the new approach can be used to discriminate between phishing and legitimate websites. This paper contributes by constructing a fuzzy rule model using a combined effective feature-set that has shown an excellent performance. Phishing deceptions evolve rapidly and should therefore be updated regularly to keep ahead with the changes.

KEYWORDS: Phishing detection; Cyber phishing attack; Fuzzy rule-base; Phishing websites; Intelligent detection

I. INTRODUCTION

At present, users interact with the Internet more often, making transactions on web technology instead of interacting with financial service institute employees. Most recently, cyber phishing attacks have become more frequent, further reaching and more sophisticated, putting the existing phishing detections under pressure [1]. In general, main types of phishing detections include phishing emails detection [2], phishing websites detection [3] and phishing toolbars detection systems [4]. Phishing emails detection analyzes text in e-mails and identify phishing attacks to protect users. Phishing websites detection compares current website's characteristics with specific blacklist features stored in a program to distinguish website status. Although the phishing researchers have a common goal to prevent users from phishing threats, the proposed study focuses on phishing websites detection systems and on rule-based approaches. Despite various counter measures existing to fight against phishing attacks, there are still inaccurate solutions [5], [6], [7], [8], [9]. As such, this study is concentrating to address this problem by constructing a fuzzy rule model using clean combined features to address the erroneousness.

The main contribution in this paper is the construction of a fuzzy rule model using combined features in [17] and in [20] for the first time based on fuzzy inference systems. Especially, this study responds to the question, how can phishing detection systems be enhanced to reduce inaccuracy and prevent cyber phishing attacks?

More specifically, this research has five main objectives: i) To investigate rule-based systems using existing literature ii) To explore phishing maintained websites to identify new phishing deception iii) To construct fuzzy-rules to distinguish between levels of websites iv) To train and test the models v) Compare results with the best results in the field.

The proposed intelligent detection for cyber phishing (IDCP) is based upon fuzzy inference systems, the most popularly utilized zero-order Sugeno that applies fuzzy rules generated from features also known as input data. A generalized bell membership function is specified by three parameters for smooth classification of fuzzy set characteristics. The IDCP is not only able to generate fuzzy models, but also to classify between phishing, suspicious and legitimate characters accurately.

The remainder of the paper is structured as follows: Section II discussed related works on phishing emails, phishing websites, feature-based and rule-based approaches together with machine learning techniques. Section III described the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

methodology including feature selection and feature size. Also, experimental procedure was discussed in sections III including training, testing, fuzzy models, fuzzy rule-base and fuzzy inference systems. Experimental Results is presented in section IV. Discussions and Comparisons including limitation are provided in section V. Conclusion and future work are presented in section VI.

II. RELATED WORK

Phishing attacks are various, but the main types are phishing email and phishing websites. In the attempt to explore email-based phishing attacks, a study was conducted by Sunil and Terrek [10] focused on classification algorithms, utilizing integration of Bayesian Classifier, Decision Tree and C4.5 applying phishing URLs. The approach achieved 95.54% true positives, which out-performed an approach applying Bayesian classifier that achieved 94.86% accuracy. To reduce false positives, Sunil and Tareek [11] proposed a model that utilises 23 hybrid features of email headers and bodies extracted from approximately 1000 emails. These were divided equally between 500 genuine and 500 unsolicited emails. They applied the J48 classification algorithm to classify phishing and genuine emails. The approach obtained 98.1% true positives with 1.9% false positives. In the attempt to improve the feature-based approach, a study by [12] applied Support Vector Machine classifier to classify emails using a set of 9 structure-based and behaviour-based features. The model achieved 97.25% accuracy rates, however it has a relatively small training dataset.

A. *Rule-based applying machine learning techniques:*

Rule-based approaches also exist. The works by [13] concentrated on a feature-based approach to explore how rule-based classification data-mining techniques are applied in phishing site detection. They employed 450 legitimate and phishing websites for features extraction. By using JavaScript feature extractor, they extracted features related to the address bar. Rule-based classification algorithms employed C4.5, RIPPER, PRISM and Classification using Associate algorithm and 17 features to identify phishing attacks. On their experiment, C4.5 attained 5.76% error-rates, RIPPER obtained 5.94% errors and PRISM achieved 21.24% error rates. After reducing the feature size to 9, classification based on association (CBA) achieved 4.75% error rates which was lower compared to other classifiers they used. However, the features are not wide-ranging enough to cover phishing characteristics that users can experience in their daily browsing. Additional features could improve the system.

A rule-based study proposed by Shukla and Rai [1] was an organization open source Intrusion Detection System known as Snort, a solution for filters. The method uses rules and features to filter phishing mails to reduce false positives and negatives. The author concluded that the approach is promising. However, validation results should be provided.

Equally, rule-based approach proposed by Ead, Abdelwahed and abdul-Kader [14] is Classification-rule discovery algorithm that integrate artificial immune system and fuzzy systems. The method considered the fitness of a fuzzy rule based on training set. A 5-fold cross validation using a test set achieved 94.66% accuracy, while a simplicity evaluation of a discovered rule set using the C4.5 data mining classification algorithm achieved 87.32%. This can be improved significantly by using an effective data set to generate effective fuzzy rules.

In addition, Moghimi and Varjani [15] proposed a rule-based for web identity. Their method used 4 features to evaluate the page resources identify and 4 features to identify protocol of page resource elements and approximate string matching algorithms based on SVM model to determine the relationship between the content and the URL webpage. Their method achieved 99.14% true positives and suffered 0.84% false negatives.

A feature-based approach using data-mining was conducted [16]. They utilised Associate Classification algorithms such as Multi-class Associative Classification (MCAC), classification based on association (CBA), missing completely at random MCAR, Multi-attribute co-cluster (MMAC), rule induction and decision trees algorithms including C4.5, PART, RIPPER with 16 features to distinguish between phishing and legitimate sites. The results attained are the following: the MCAC algorithm was misclassified by 0.8% error rates, C4.5 1.24% error rates, RIPPER 1.86% errors and PART misclassified 4.46% error rates. Although MCAC achieved a high accuracy, their features have been

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

extracted from only one source without considering all other different possible sources. In this case, more sources could improve features to detect emerging phishing attacks.

A feature-based approach was explored by Barraclough [17], applying a Neuro-fuzzy using features extracted from five different sources also known as inputs to detect phishing websites accurately. Their approach achieved 98.5% accuracy, but suffered 1.5% error rates. This work could be improved by adding more features.

In the attempt to improve the phishing detection scheme, Barraclough [18] proposed a parameter tuning framework, a novel method to distinguish phishing websites with low false positives. The approach was based on fuzzy systems, using six sources with 352 features to detect phishing websites, which offered 98.7% accurate results.

As it can be seen in this section, various studies have employed feature-based approaches applying machine learning techniques and different classification algorithms such as PART, RIPPER, Random Forest and Partial, NaiveBayes, SVM, C4.5 to create the rule-base. However, the existing approaches have not used cleaned features based on adaptive fuzzy inference to construct fuzzy rules and fuzzy models.

III. PROPOSED METHODOLOGY

The intelligent detection cyber phishing (IDCP) method is proposed to reduce the inherent inaccuracy in phishing detection systems. The IDCP consists of four main components, which include a feature base, feature sources, current websites and Inference engine. This can be seen in Fig. 1.

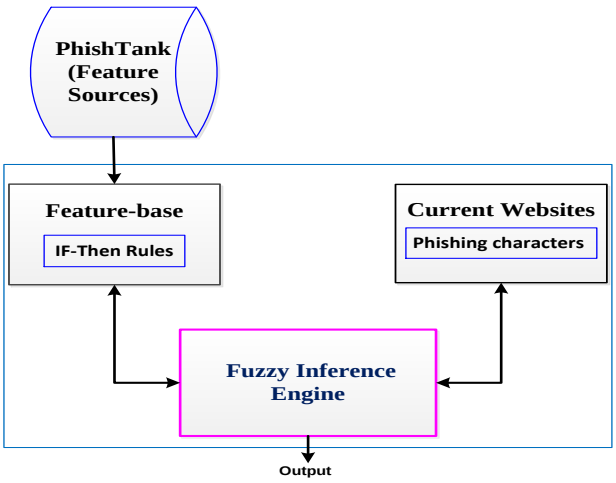

Fig. 1. The intelligent detection for cyber phishing process

The Feature-base contains phishing features also known as identifiers. Features are phishing deceptions expressed in the form of text. While identifiers are matched against the IF condition of the rules, deceptions are used to convince users to give up their sensitive information.

The If-Then rule is a structure which has 'IF' and THEN components. It is based on the idea that online phishing attack techniques evolve, phishers convince users to give up their sensitive information by applying deceptions on emails and websites. An example of a web deception can be seen in Fig. 2. The features are important because they are used as phishing identifiers in the phishing website detection system. As well as this, they are used to generate fuzzy rules and to classify between phishing, suspicious and legitimate websites.

Current website may carry three possible characteristics: phishing, suspicious and legitimate characteristics.

The feature sources are phishing websites from PhishTank archive where phishing websites are maintained for public access [21].

Fuzzy Inference Engine is a Sugeno systematic approach that carries out the reasoning in which the detection system searches for a solution. In general, the inference engine compares the antecedent part of the rule with the features

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

provided in the feature base. If such a rule is found and its antecedent matches the characteristics in the feature base, the rule is executed and an output is achieved [19].

A. *Feature Selections*

The intelligent detection cyber phishing is based on a fuzzy inference system (FIS) and incorporates six layers with numbers of neurons in the hidden layer. Features for cyber phishing detection are extracted from different sources. While phishing features can be of different characteristics, features for IDCP are textual as the tools used can handle textual data. In this case, well extracted features are utilized from the study by [17] and from a E-web-form model by [20]. Samples of six features are shown in Fig. 2 by red arrows and are described and summarised on Table 1. The remaining fifty features can be seen in the study "Intelligent security for phishing online using adaptive neuro-fuzzy systems" [20]. Fig. 2 is a phishing website which is an exact imitation of Barclays bank website and features are shown by red arrows.

Fig. 2. Feature sources for cyber phishing rule-based detection system

Table 1: The intelligent detection for cyber phishing

Features	Description
First Name	The feature "First Name" has a low risk
Last Name	The feature "Last Name" has a low risk
Date of birth	The risk of "Date of birth" is medium
Five-digit-passcode	"Five-digit-passcode" has a high risk
Your sort code	The feature "sort code" has a high risk
Account number	"Account number" has a high risk

B. *Feature Size*

The size of features used in this paper are 56 in total. Specifically, thirty-four features are taken from a previous study [20]. Twenty-two significant novel features were added from E-web-forms. With the existing issues associated with false positives and false negatives in mind (a lack of effective features), sources and features are reduced in size by identifying the most effective ones. For training and testing sets, a careful selection and further cleaning are conducted to decrease redundancy records. This process is essential to construct state-of-the-art IDCP fuzzy rules which can decrease the inherent problem of false positives to keep up to date with emerging phishing attacks.

C. *Training and Testing*

In training and testing the models, two-fold cross-validation method is employed to measure the system merit. To accomplish this, features are split randomly into 28 training set and 28 testing set. First, training is carried out on the training-set only once and testing is carried out on the test-set only once. Then the roles of training and testing are reversed. Training is performed on the testing-set and testing is done on the training-set. The results are assembled to obtain an average error. These features can be generalized to be used in toolbars phishing detection applications.

D. *Fuzzy Set*

A fuzzy set means a set with fuzzy boundaries. It can be of various shapes, but trapezoidal is used for this problem because not only can it offer sufficient presentation of cyber phishing detection, but it can also reduce the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

computational process. The intelligent detection cyber phishing has membership values from [0,1] as shown in Fig. 3, which consist of legitimate (low risks), suspicious (medium risk) and phishing (high risk). These are defined as:

$\overline{A}_1$ = 'Last_Name is Legitimate' …, Legitimate ε [0, 30]

$\overline{A}_2$ = 'Bank_Name is Suspicious' …, Suspicious ε [12, 76]

$\overline{A}_3$ = 'User_code is Phishing' …, Phishing ε [60, 90]

Therefore, the membership functions for legitimate, suspicious and phishing are represented in the form of:

Legitimate: $\mu \overline{A}_1 (10)$ = 0.1.

Suspicious: $\mu \overline{A}_2 (10)$ = 0.5.

Phishing: $\mu \overline{A}_3 (10)$= 0.9.

Features with low risk have a membership value range between 0% - 0.1. At the same time, it overlaps and becomes a member of the suspicious set with a degree of 30%. Features with medium risk have a degree of membership of 12%. At the same time, it is also a member of the phishing set with a degree of 76%. Features with high risk have a degree of membership of 90%. When it overlaps, it become a member of the suspicious set with a degree of 60%.

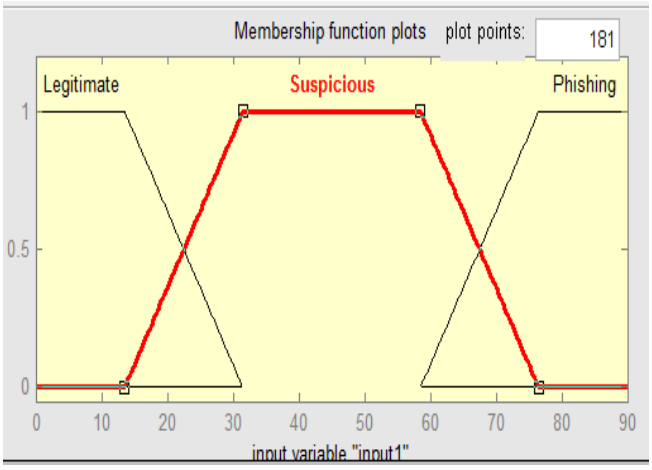

Fig. 3. Membership function and fuzzy sets

E. *Fuzzy rule model*

The cyber phishing detection system utilizes 56 features as stated in section B to generate fuzzy rule model, to learn and to test the model. To accomplish the goal, fuzzy rules are obtained by describing how the problem can be solved utilizing fuzzy linguistic values defined in section D. In each rule a clause that identifies the status of a website is included. A fuzzy rule can be expressed as a conditional statement in the form:

R_1:

IF X is $K3$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

THEN Y is $L1\{0.1\}$

R_2:
IF X is $K2$
THEN Y is $L2\{0.5\}$

R_3:
IF X is $K1$
THEN Y is $L3\{0.9\}$

Wherever X and Y (Last-Name, Bank_Name, User_code) are linguistic variables, K1, K2 and K3 (low, medium and high) are linguistic values decided by fuzzy sets on universe of discourse X. L1, L2 and L3 (legitimate, suspicious and phishing) are linguistic values decided by fuzzy sets on universe of discourse Y (risk). Cyber phishing detection fuzzy rule model can be seen in Fig. 4 in a fuzzy form:

Rule: 1

IF Feature is Last_name
THEN website is legitimate
...

IF Feature is Email
THEN website is legitimate

Rule 2:

IF Feature is Bank_Name
THEN website is suspicious
...

IF Feature is Date_of_birth
THEN website is suspicious

Rule 3:

IF Feature is User-code
THEN the website is phishing
...

IF Feature is Memorable_word
THEN website is phishing

Fig. 4. Fuzzy rule model

F. *Fuzzy inference systems*

A fuzzy inference system corresponds to a set of fuzzy IF-THEN rules that have learning ability to estimate nonlinear functions. For instance, inferring membership functions for input and output variables of the Cyber phishing detection system. The IDCP in Fig. 5 is functionally equivalent to zero-order Sugeno fuzzy inference. The structure generated utilizing grid partition is similar with a multi-layer neural network that has six layers including hidden ones, which are input, input- membership function (MF), rules, output- membership function, output and a summation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

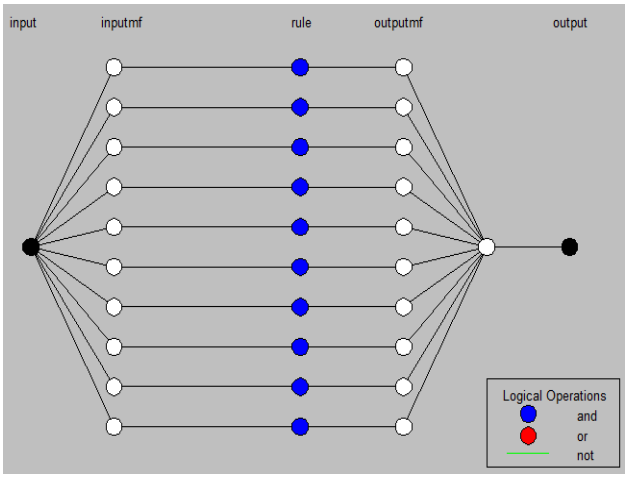

Fig. 5. Fuzzy Structure

Every layer in the fuzzy inference system (FIS) is correlated with specific steps in the process of fuzzy inference.

The first Layer:
Is input. Inputs in this layer are transmitted directly to the second layer by each neuron. This is presented as:

$$y_i^{(1)} = x_i^{(1)} \quad \text{eq. (1)}$$

In layer 1, $y_i^{(1)}$ is the output and $x_i^{(1)}$ is the input.

The second Layer:
Is an input membership. A fuzzification neuron receives input and decides the degree to which this specific input belongs to the fuzzy set. The activation of membership functions is set to the function that specifies the neuron's fuzzy set. The MF presented in Fig. 3 in section 3 D is set to the trapezoidal membership function.

The third layer is the fuzzy rule:
In this layer, every neuron replies to a single fuzzy rule. A fuzzy rule gets inputs from layer 2 that represent fuzzy sets in the antecedents of the rule. Therefore, the output of I in layer 3 is achieved as:

$$y_i^{(3)} = x_{1i}^{(3)} \text{ X } x_{2i}^{(3)} \text{ X} \ldots \text{X } x_{ki}^{(3)} \quad \text{eq. (2)}$$

The inputs are $x_{1i}^{(3)}, x_{2i}^{(3)}, \ldots, x_{ki}^{(3)}$ and $y_i^{(3)}$ the output of fuzzy rules in the third layer.

Normalized degree of Confidence:
A fuzzy rule implies that different rules represented in the fuzzy inference system can relate to different degrees of confidence. Intelligent detection cyber phishing features expert may attach the degree of confidence to each feature, which forms each fuzzy IF-THEN rule by setting corresponding weights within the range of [0,1]. During training time, weights can change. To keep them within the specific range, the weights are normalized.

The fifth Layer:
Is an output membership. In this layer, neurons represent fuzzy sets utilized in the rule consequent. Output membership gets inputs from the corresponding fuzzy rule and mixes them by utilizing union operation. This is presented as:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

$$y_i^{(4)} = x_{1i}^{(4)} \oplus x_{2i}^{(4)} \oplus \ldots \oplus x_{li}^{(4)} \quad \text{eq. (3)}$$

$x_{1i}^{(4)}, x_{2i}^{(4)}, \ldots, x_{li}^{(4)}$ are inputs and $y_i^{(4)}$ is the output of membership in fourth layer.

Sixth Layer (defuzzification):
In this layer, neuron represents one output. It receives the output fuzzy sets. The output of fuzzy inference system is a crisp, therefore the aggregated output fuzzy set must be defuzzified. The sum is calculated as a weighted average of the centroid of the whole MF output. This is represented as:

$$Y = \frac{\mu C1 XaC1 XbC1 + \mu C2 XaC2 XbC2}{\mu C1 XbC1 + \mu C2 XbC2} \quad \text{eq. (4)}$$

Whenever aC1 and aC2 are centroid, and bC1 and bC2 are the widths of fuzzy sets C1 and C2.

IV. EXPEERIMENTAL RESULTS

Firstly, training is performed on a training set using 28 features and 12 numbers of epochs. The estimation output achieved is 0.00087668 representing the training feature error as presented in the graph in Fig. 6. The second training requires the roles to be reversed and training is performed on the testing set. The output produced 0.00087668 errors, which is equal to the preliminary training. When the training result is converted to a percentage, the overall training accuracy is 100% with 0% error. After the training is completed, testing is performed on testing set and the estimation for testing achieved is 0.0008759 average testing errors. This is presented in the graph in Fig. 7. The roles are reversed and testing is performed on training set. The output errors produced is 0.0008759 which is equal to the previous results.

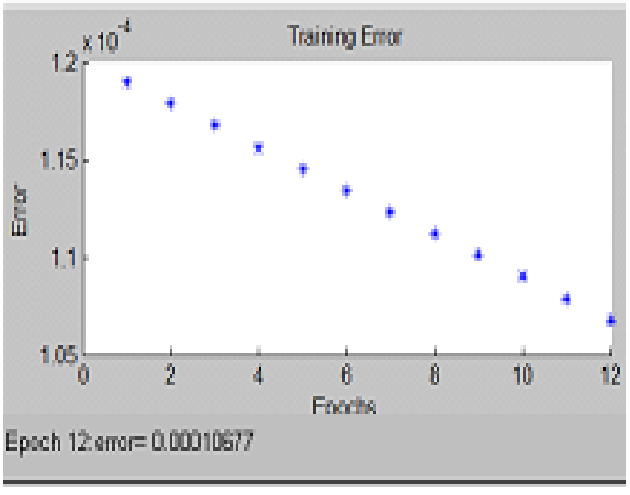

Fig. 6. Training result

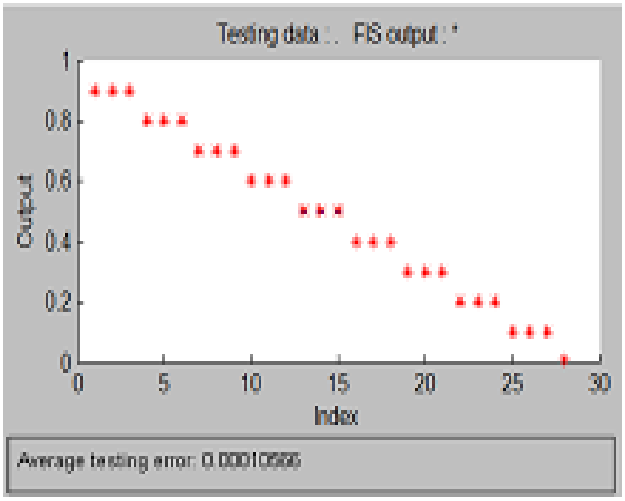

Fig. 7. Test result

The results are summarized as presented in Table 2. Column 6 shows the average training error results, while column 7 shows the average testing error results. All executions are summed-up and divided by two to obtain an average. When converted into percentage and in two decimal point, the overall average error rates attained for both training and testing is 0%. An overall average testing result is 100% accurate. The results demonstrate a higher performance compared to the best results in the field.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

Table 2: Summary of the results

Experiment	Input MFs	Output MFs	Training size	Testing size	Training Error	Test Error	Average Accuracy results
Train1, Test1	Trapmf	Linear	28	28	0.00010677	0.00010566	100%
Train2, Test2	Trapmf	Linear	28	28	0.00010677	0.00010566	100%

V. DISCUSSION

This study aims to create a fuzzy rule model based on a Fuzzy Inference System utilizing combined features to tackle the inaccuracy in online transactions. The contribution is a novel fuzzy rule model using combined features to reduce erroneousness in phishing detection systems. The results reveal that after two-fold cross validation, the proposed method obtained 100% accuracy. This clearly indicate that a novel fuzzy rule model using combined features can detect phishing websites with a higher accuracy compared to the existing ones.

As seen in Table 3, the comparison is focused on the most closely related methods based on the literature reviewed in section II. The similarities between existing work and the IDCP is that they all use feature-sets and machine learning techniques. The difference is in the use of algorithms. For instance, the study by [12] and [15] applied SVM, [14] and [16] used C4.5. Also [16] used MCAC, PART, RIPPER, MCAR, MMAC, DT and CBA compared to Adaptive Neuro-Fuzzy Inference Systems used by the IDCP. However, the study by [17], [18] and [20] used the same Sugeno model and feature-sets. The existing approaches achieved between the range of 94.66% - 99.2% accuracy. If compared, the IDCP accurateness is 100% which is an excellent result. The IDCP method shows that combined features are important for detecting phishing websites.

Table 3: Comparative summary of best results in the field with proposed study results

Authors	Methods	Algorithms	Results
[12]	feature-based using 9 features	SVM	97.25%
[14]	Rule-based using features	Fuzzy system, C4.5	94.66%, 87.32%
[15]	Rule-base using 4 features	SVM	99.14%
[16]	Feature-based using 16 features	MCAC, C4.5, RIPPER, PART, MCAR, MMAC, DT, CBA	99.2%, 98.76%, 98.14%, 95.54%
[17], [18], [20]	Feature-based, 288, 300, 56 features	A Neuro-fuzzy Systems ANFIS	98.5% 98.4% 98.4%
The IDCP	Rule-base using 56 features	ANFIS	100%

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering
(An ISO 3297: 2007 Certified Organization)
Website: www.ijircce.com
Vol. 5, Issue 6, June 2017

A. *Limitations*

Even though the intelligent detection cyber phishing has proved to be successful, phishing characteristics evolve rapidly, while the features are updated manually. An investigation to make updates automated should be considered along with intelligent search strategy to allow more rules to be used effectively in real-time.

VI. CONCLUSION AND FUTURE WORK

This paper introduces a rule-based future-driven cyber phishing detection system based on ANFIS. The fuzzy rule of the proposed system is constructed by utilizing a clean feature set from the work of [20]. The training and testing results using the given features demonstrate that the IDCP is not only capable of increasing systems performance, but is also capable of reducing the inherent inaccuracy in the phishing detection systems. As well as this, the IDCP can generalize to the new phishing.

The IDCP is based on the Sugeno model, but there are challenges in Mamdani method. Therefore, this study will explore Mamdani methods and rules for further work.

REFERENCES

1. V. Shukla and M. K. Rai, "A rule based approach for detecting phishing attacks" International Journal for research in applied science and Engineering technology (IJRASET), vol. 2 (1X), ISSN: 2321 – 9653, 2014.
2. A. Almomani, B. B. Gupta, T. Wan, A. Altaher and S. Manickam "phishing dynamic evolving neural fuzzy framework for online Detection Zero-Day Phishing Email" Indian Journal of Science and Technology Vol. 6 ISSN: 0974-6846, 2013.
3. R. Priya, "An Ideal Approach for Detection of Phishing Attacks using Naïve Bayes Classifier", International Journal of Computer Trends and Technology (IJCTT) Vol. 40, 2, ISSN: 2231-2803, 2016.
4. P. A. Barraclough, G. Sexton and N. Aslam, "Online phishing detection toolbar for transactions" Science and Information conference (SAI), IEEE XPlore, pp. 1321 – 1328, 2015.
5. L. Fang, W. Bailing, H. Junheng, S. Yushan and W. Yuliang, "A Proactive Discovery and Filtering Solution on Phishing Websites", IEEE International Conference on Big Data (Big Data), 2015.
6. B. Kumar, P. Kumar, A. Mundra and S. Kabra, "DC Scanner: Detecting Phishing Attack", IEEE Third International Conference on Image Information Processing, 2015.
7. S. Smadi, N. Aslam, L. Zhang, R. Alasem and M. A. Hossain, "Detection of Phishing Emails using Data Mining Algorithms", 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2015.
8. Z. Dong, A. Kapadia, J. Blythe and L. J. Camp, "Beyond the Lock Icon: Real-time Detection of Phishing Websites Using Public Key Certificates", APWG Symposium on Electronic Crime Research (eCrime), 2015.
9. M. Aburrous, and A. Khelifi, "Phishing Detection Plug-In Toolbar Using Intelligent Fuzzy-Classification Mining Techniques", Vol. 3. International Journal of Soft Computing and Software Engineering [JSCSE], pp.54-61, 2013.
10. B. R. Sunil and M. P. Tareek, "Content based spam detection in email using bayesian classifier", IEEE International Conference on Communications and Signal Processing (ICCSP), 1257 – 1261, 2015.
11. B. R. Sunil and M. P. Tareek, "A Comparative Performance Evaluation of Content Based Spam and Malicious URL Detection in E-mail", IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS), 2015.
12. L. M. Form, K. L. Chiew, S. N. Szeand and W. K. Tiong, "Phishing Email Detection Technique by using Hybrid Features", IT in Asia (CITA), 9th International Conference, 2015.
13. R. Mohammad, T. L. McCluskey and F. A. Thabtah, 'Intelligent Rule based Phishing Websites Classification'. IET Information Security, 8 (3). pp. 153-160. ISSN 1751-8709, 2014
14. W. Ead, W. Abdelwahed and H. Abdul-Kaderm "Adaptive fuzzy classification-ryke algorithm in detection malicious web sites from suspicious URLs", International Arab Journal of e-Technology Vol. 3 (1), 2013.
15. M. Moghimi, A. Y. Varjani, "New rule-based phishing detection method", Expert Systems with Applications, Vol. 53 pp. 231-242, 2016.
16. N. Abdelhamid, A. Ayash and F. Tabatah, "Phishing Detection Based Associative Classification Data Mining", Expert System with Application, Vol. 41, pp. 5948-5959, 2014.
17. P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton and N. Aslam, "Intelligent phishing detection and protection scheme for online transactions" Expert Systems with Applications, Vol. 40, (11) pp. 4697-4706, 2013.
18. P. A. Barraclough, M. A. Hossain, M. A. Tahir, G. Sexton and N. Aslam, "Intelligent phishing detection parameter framework for e-banking transactions based on neuro-fuzzy", Science and Information Conference (SAI), pp. 545 – 555, 2014.
19. W. Suparta, and K. M Alhasa, "Modeling of Tropospheric delays using ANFIS" Spring international Publishing, 1st ed., 2016.
20. G. Fehringer and P. A. Barraclough, "Intelligent security for phishing online using adaptive neuro-fuzzy systems", International Journal of Advanced Computer Science and Applications, Vol. 8 (4), 2017.
21. PhishTank, Statistics about phishing activity and phishTank usage. Online available <http://www.phishtank.com/stats.php. 2.2.4, 3.1, 4.4.2> Accessed, April 2017.