Northumbria
University
NEWCASTLE

Parameter optimization for intelligent phishing detection using Adaptive Neuro-Fuzzy

P. A. Barraclough
Computer Science and Digital Technology
Univeristy of Northumbria
Newcastle Upon Tyne, NE 18ST, United Kingdom

G. Sexton
Computer Science and Digital Technology
Univeristy of Northumbria
Newcastle Upon Tyne, NE 18ST, United Kingdom

M.A. Hossain
Computer Science and Digital Tecnology
University of Northumbria
Newcastle Upon Tyne, NE1 8ST, United Kingdom

N. Aslam
Computer Science and Digital Tecnology
University of Northumbria
Newcastle Upon Tyne, NE1 8ST, United Kingdom

***Abstract*— Phishing attacks has been growing rapidly in the past few years. As a result, a number of approaches have been proposed to address the problem. Despite various approaches proposed such as feature-based and blacklist-based via machine learning techniques, there is still a lack of accuracy and real-time solution. Most approaches applying machine learning techniques requires that parameters are tuned to solve a problem, but parameters are difficult to tune to a desirable output. This study presents a parameter tuning framework, using adaptive Neuron-fuzzy inference system with comprehensive data to maximize systems performance. Extensive experiment was conducted. During ten-fold cross-validation, the data is split into training and testing pairs and parameters are set according to desirable output and have achieved 98.74% accuracy. Our results demonstrated higher performance compared to other results in the field. This paper contributes new comprehensive data, novel parameter tuning method and applied a new algorithm in a new field. The implication is that adaptive neuron-fuzzy system with effective data and proper parameter tuning can enhance system performance. The outcome will provide a new knowledge in the field.**

Keywords—FIS; Intelligent phishing detection; fuzzy inference system; neuro-fuzzy

I. INTRODUCTION

Phishing is a technique utilized by attackers to obtain user's sensitive information and financial account credential for financial benefit. Phishing attacks have become a major concerned in online transactions causing monitory losses annually. According to the Press Association report, an increase in phishing attacks in online transaction caused losses of £21.6 million between January and June 2012, which was a growth of 28% from June 2011[1]. Due to this problem, various anti-phishing approaches have been proposed to solve the problem.

These approaches include feature-based techniques [2], [3], blacklist-based [4], [5], [6], [7], and content-based approaches applying machine learning algorithms have attempted to solve the problem [8], [2]. However, there is still high false positive causing inaccuracy in online transaction. The machine learning techniques also require parameter settings to solve a problem. However parameters are difficult to set to a desirable output, and parameter tuning framework are non-existent particularly for phishing website detections [9].

The main phishing website detection approaches are either utilizing: (1) Feature-based including content based approaches applying machine learning algorithms to discriminate between legitimate sites and illegitimate sites or *(*2) URL blacklist-based approach that uses a list of URL of known illegitimate websites.

This paper has made the following contributions: (1.) identified user's credential profiles as one of core component of input data that has not been utilized in the field, (2.) introduced novel data based on user's credential profile, introduced novel parameter tuning framework based on ANFIS algorithm using comprehensive feature, (3.) applied ANFIS for the first time in (phishing detection website) a new field. This is a novel work that has not been considered in literature in a unified platform.

This study focused in answering the question: how can parameter tuning method be used to maximize phishing detection accuracy using ANFIS with six sets of inputs? The aim is to design a parameter tuning method based on an adaptive neuro-fuzzy inference system, using comprehensive data from six inputs that can be used by researchers in the field. The specific objectives are: (1) to identify samples and gather comprehensive data to be used as input data, (2) to develop fuzzy models based on ANFIS comprehensive dataset, (3) to train and check/test the models using cross-validation methods, and (4) to conduct a comparative study to prove the capability and merit of the parameter tuning framework.

The outcome generated from this study should help researchers in the field with a great knowledge and understanding about the capability of fuzzy systems and six inputs.

The proposed approach applies adaptive neuro-fuzzy inference system, using six inputs including: legitimate site rules, user-behaviour profile, phishTank, user-specific sites, pop-up windows and user's credential profile. 352 data are gathered based on these six inputs. 300 data are used as input data in to the inference engine to generate fuzzy models and fuzzy rules. During 2-fold cross-validation data are split into 150 training set and 150 testing set. Trained on 150 data-set and validated on the remaining 150 set. This was repeated four-times so that data set is used only ones. This multiple experiment achieved 98.8% accuracy in real time.

Generally, phishing detections are divided into two main categories: Phishing emails and phishing websites. This study focuses on feature-based in phishing website detection, using adaptive neuro-fuzzy inference system. There are also other common machine learning algorithms that could be used including logistic regression, fuzzy logic, neural network, perceptron and many more.

The remaining sections are as follows: Section II covers literature review. Section III describes methodology including feature gathering and Analysis. Section IV covers experimental set up. Section V covers experimental set up including, training and testing. Section VI presents results and discussions and analysis. Section VII concludes the paper and provides future work.

II. RELATED WORK

Phishing attacks have increased and are becoming sophisticated, which have led to $15 billion losses in the global economy in 2012 [1]. This has caused a number of phishing solutions to be developed to tackle the problem. Anti-phishing detection solutions mainly utilize two approaches: feature-base approaches that utilize Uniform Resource Locator (URL), blacklist-based and approaches that utilize data-based including content, using machine learning techniques.

A. Content-based through Machine Learning techniques

Major researches have considered content-based approaches based on machine learning techniques to detect phishing websites [2], [10], [11], [12], [13 [14], [15]. Aburrous proposed a model to identify electronic banking sites [2]. The method utilized a combined fuzzy logic and data mining algorithms, using twenty seven characters and factors that identify phishing websites. Their approach achieved 84.4%, but suffered 15.6% error rates, which is a high risk for online users.

In an attempt to improve the detection approaches, Suriya proposed fuzzy logic, using factors and a case study to assess whether phishing attack was taking place or not [10]. Their method employed three layered checker in web pages to check for tricks of attackers, using JavaScript to hide data from users. The result revealed that their approach can detect phishing 96% correctly. However using only 3 layer method to detect phishing is limited since phishing techniques are varied.

Similarly, Wenyin considered a method based on reasoning of Semantic Link Network, using 1000 illegitimate web pages and 1000 legitimate web pages to directly discover the target name if it is a phishing website or a legitimate website [11]. Their approach had ability to identify phishing sites using inferring rules. Wenyin, however, acknowledged that the model suffered 16.6% false negative and 13.8% false positive, which are high level of error rates.

Equally, Xiang explored content-based probabilistic method that incorporates URL blacklists with shingling algorithms utilized by search engine and information retrieval technologies (IRT) to identify phishing websites [12]. Their approach had advantage of using TF-IDF and a scoring function in the search engine, when they match queries to pages that produces a probabilistic framework for detecting phishing sites. The experimental result was 67.74% and 73.53% accuracy with 0.03% error rates. Although this method has low false positives, its accuracy can make user vulnerable to phishing attacks.

Moreover, Dong focused on defending the weakest link in phishing websites detection, by analyzing online user behaviours based on visited websites and the data a user submitted to those websites [13]. Taking user's behavior into consideration is important in addressing phishing attack, but only dealing with the data users submitted to detect phishing sites is a major limitation in handling a well designed phishing websites.

Likewise, Wardman came along with a new method using file matching algorithms, hashing function index MD5 hash value and Deep MD5 Matching, to decide if a file can be utilized to classify a new file in the same group of phishing web pages [14]. Their method was tested to identify the system performance. The results demonstrated that their technique could achieve more than 90% in performance. However, the approach suffered high level of false positive rates (10%).

In the attempt to improve phishing detection scheme, Barraclough proposed a novel method to detect phishing website [15]. The approach was based on machine Neuro-fuzzy, using five sets of inputs with 288 features, which offered accuracy results of 98.4%. This result demonstrated high accuracy, but suffered 1.6% error rates. Their finding was that a hybrid neuro-fuzzy with 5 input feature-sets can detect phishing websites with high accuracy in real-time.

B. URL Blacklis-based Approaches

Another study explored blacklist-based that uses a list of URL of known illegitimate websites [4], [5], [7], [16], [17], [18], [19], [20]. For instance, Xiang proposed blacklist and content-based model to strengthen human-verified blacklist by using probabilistic techniques to obtain higher accuracy [4]. Their experiment obtained 87.42% true positive, but suffered 4.34% false positives, which is a high error rates.

Similarly, Ma conducted a study and explored phishing website detection [5]. Their approach was based on machine learning algorithms consisting of Support Vector Machine (SVM), Logistic Regression (LR) and Naïve Bayes (NB), using 10,000 host-based features from WHOIS queries with Lexical features to classify website reputation on the relationship between the lexical and host-based features. Their approach yielded 95% and 99% accuracy, and error rates range of 0.9% and 3.5%. However, Ma acknowledged that their method could not handle large evolving phishing websites that are created regularly [5].

Equally, Whittaker designed Google's phishing classifier to automate the maintenance of Google's blacklist [7]. Their method was based on logistic regression classifier, using URL-based lexical features, web page content and Hypertext Markup Language (HTML) to automatically classify phishing web pages. Their experimental results achieved 90% accuracy in real-time with 10% error rates. However, Whittaker recognized that their blacklist keeps behind with update and can only identify phishing site after it has been published and appeared on the Internet [7].

Similarly, PhishDef was developed by Le [16]. Their method was based on URLs lexical features, using algorithms to compare phishing websites. Their features were evaluated utilizing online learning algorithms including batch-based Support Vector Machine (SVM), Online Perceptron (OP), Confidence Weighted (CW) and Adaptive Regularization of Weights (AROW) that overcomes noisy data when detecting phishing websites. For each URL inputs, the classifier makes a decision whether a website is suspicious or not. Their approach achieved an average of 97% accuracy using offline algorithms and 90% using online algorithms. However, Le's research suffered features inadequacy, which is a similar problem to the study of Xiang [4]. Le's study is related to the study of Ma in their methodology. Both methods used URL feature-based [16], [5].

In addition, Huh and Kim applied search engines to measure URL which identified phishing websites and ranked them below 10, while legitimate sites were ranked top [17]. For evaluation performance, Google, Bing and Yahoo were used. As well as this, 100 legitimate websites and 100 illegitimate websites were employed, applying classification algorithms to measure website reputation including linear discrimination analysis, Naïve Bayesian, K-Nearest Neighbour and Support Vector Machine. Using K-Nearest Neighbour achieved accuracy of 95% and 6.2% error rates. Although K-Nearest Neighbour performed better in comparison with the best classifiers, URL features alone is very limited to detect phishing websites, while legitimate websites can be compromised easily by attackers and spoil their validity. Canali proposed Prophiler, a lightweight malware static filter, using HTML, JavaScript and URL with features through a classifier that identifies non-malicious pages to assess more malicious pages to a great extent [18]. While Prophiler was intended to be a fast filter, it allows higher false positive rates in order to reduce false negative rate. In addition, CANTINA+ was proposed by Xiang [19]. The approach was based on machine learning techniques, using URL, Search Engines, the HTML Document Object Model (DOM) and PhishTank with fifteen features. Although the results revealed 92% accuracy, it suffered 8% error rates. Furthermore, Ead proposed a combination of artificial immune systems and Fuzzy systems with both lexical and host-based URL features [20]. The advantage of this approach is that it classifies URLs automatically as phishing or legitimate sites.

Although the above mentioned approaches are effective to some degree of accuracy, there are still high false positive rates due to a lack of adequate data and parameter tuning methods are non-existent [9], [21]. Thus, this study address the problem: introduce a novel comprehensive data, a new parameter tuning framework and apply neuro-fuzzy system in a new field to maximize phishing detection system performance. Fig. 7 is the conceptual design of our work that illustrates the overall flow.

III. METHODOLOGY

The proposed approach consists of machine learning techniques, adaptive neuro-fuzzy and six inputs. Adaptive neuro-fuzzy is a combination of fuzzy logic and neural network. The choice of Neuro-fuzzy is that it has the advantage of both neural network which is capable of learning new data and fuzzy logic which deals with linguistic values as well as making decisions using fuzzy [If-Then] rules [9]. Six inputs include legitimate sites rules, user-behaviour profile, phishing sites, online banking sites, pop-up windows, user's credential profile. From these six sets of inputs, data are extracted that help detect phishing websites. Our phishing detection architecture with possible overall flow is presented in Fig. 1. The six inputs in part A are explained next before moving on to the fuzzy inference systems in part B.

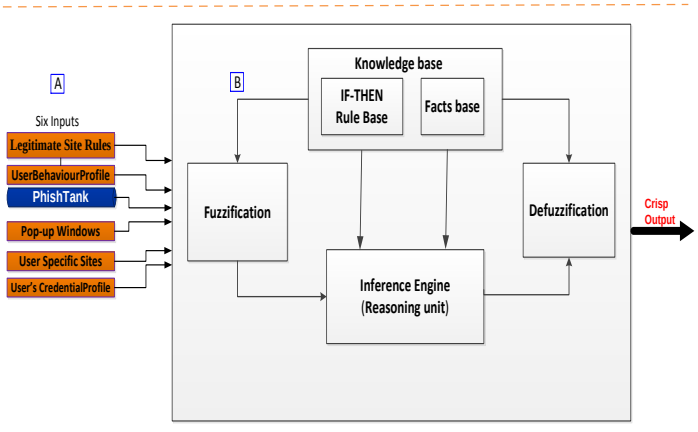

Fig.1. Fuzzy inference system for phishing website detection

A. six inputs

In part A, six inputs are diverse samples in which data are extracted, which include: Legitimate site rules, user-behaviour profile, phishTank, user-specific site, pop-up windows and

user's credential profile. From these 300 data that characterize phishing techniques are gathered and are used as input data in the system to generate fuzzy models, IF-Then rules and to distinguish between phishing, suspicious and legitimates sites accurately and in real-time. The six inputs are selected carefully because they are a whole representative of phishing tactics and strategies

B. Fuzzy inference system

Part B consist of Fuzzy inference system (FIS) also called fuzzy models. Mainly, FIS for phishing detection similar to Sugeno type consist of 5 functional components: Fuzzification interface converts crisp inputs into a degree that go with linguistic value, knowledge-base is made up of rule-base that contains a number of fuzzy [IF-THEN] rules and fact-base classifies the MFs of the fuzzy sets, inference-engine performs reasoning in the decision making unit and defuzzification interface converts the fuzzy results of the inference into a crisp output.

C. Data collection and Analysis

Based on six inputs, data are randomly and carefully extracted utilizing qualitative and quantitative research method that produces numerical results. Specifically, 66 data are extracted from legitimate Site rules in the period of 23 November 2011 to 5 December 2011. A freely accessible Pinsent Manson Law Experts was consulted to identify legislations covering phishing crime and their order of importance [22]. As well as this, the European Commission documentation was explored [30]. Based on User-Behaviour profile, 60 data are extracted that cover user's information when interacting with illegitimate site (Dong et al., 2008). These data are extracted using the knowledge provided in recent journals and conference papers during the period of 8 December 2012 and 11 February 2013. Moreover, PhishTank websites provide 72 data that are extracted by exploring journal papers and 200 phishing websites from PhishTank archive [31]. Having considered that phishing techniques evolve with time, an automated wizard is utilized to extract website URLs and store in Excel Worksheets. The automated wizard also allows updates every 10 minutes when new phishing website is added into the PhishTank archive [23]. PhishTank consist of 1,038,011 verified phishing websites submitted within 3 years from 1st January 2010 to 30th December 2013. 48 data are extracted based on User-specific sites. A consultation with bank experts was done which highlighted important information and 200 legitimate bank websites were explored and compared information with phishing ones [24], [25] in the period from 8th December 2012 and 2nd February 2013. Equally, Pop-up windows consist of 42 features which are gathered by observing pop-ups that appears on websites. This was an on-going process between 28 November 2011 and 6th April 2012. 64 data are extracted from user's credential profile during the period of 8th January 2012. That makes the overall total of 352 data, also known as features in phishing terms. Data are organized in to 6 sets. In particular, set1 up to set5 which are legitimate site rules, user-behaviour, phishTank, user-specific sites and pop-up windows have been taken from our previous paper [15]. Specifically, Fig. 1 present 64 data extracted from User's credential profile that are novel and are our major contribution in this paper.

a) Data Normalization: Most frequent terms was performed across data using the 'find' function to identify data. The data is prepared using normalization method by assigning weight to each data using a value range between [0 and 1]. While 0 (zero) indicates low, 1 (one) is high and there are in between values such as 0.3. This normalization is done in order to remove deffects that occurs in data to make sure that the impact of technical bias are reduced in the results. Table I shows that data is is assigned a weight of 0.6 which indicates that the data has high importance in combating phishing, while the data weighted 0.3 is moderate, 0.1 indicates low risk.

b) Feature size: Our choice of 300 data size is adequate to produce a desirable output for our model. The size of data used for modelling could be any number because the number is within the recommended range to obtain a stable cross-validation split [26]. Kohavi [27] conducted Cross-Validation experiments for accurate estimation and model selection, and found that a given number of data sets that can be partitioned into 10-fold cross-validation is good enough.

c) Methodology limitations: one of the challenge in phishing is that phishing websites are taken down within 48 hours of launching which make it hard to find them while a life. The way to solve this is to use the phishing websites published by the community service after the phishing websites have been in circulation.

IV. Experimental Set-Up

The aim of this paper is to design parameter tuning framework for phishing detection utilizing adaptive neuro-fuzzy inference system. Practically, rules are determined by expert in expert systems. In supervised learning, algorithms are trained on inputs. Thus, all input and output membership function parameters assigned are selected empirically by determining the desired input. Since there is no easy way to decide the smallest number of the hidden nodes essential to obtain a preferred level of performance, adjustments are done after evaluation if the results are not satisfying. For our experiment MATLAB fuzzy logic tool box was used because it has a FIS editor and other four integrated editors which are useful for training and testing process. Cross validation methods are used to validate the model and various Cross-validation methods exist, such as 20-Fold, 10-Fold, 5-Fold, 2-Fold and LOOCV, but 2-Fold CV is used in this paper because it can handle the conventional data well [29]. During cross-validation, 300 data is split into 150 training pair and 150 testing pair. The training pair is used to train the model, while testing pair is used for testing the model's capability. Checking, also handles the model overfitting during the training process [29].

TABLE.I. DATA EXTRACTED FROM USER'S CREDENTIAL PROFILE

No.	User Credential PhishRegister	Layer 3
1	UpdatePersonal Details	Weight 0.6
2	Passcode	
3	PIN	
4	Last 4 digits number	
5	Mother Maiden Name	
6	UserName	
7	Password	
8	Security code	
9	YourUserCode	
10	SecurityNumber	
12	PINsentry Number	
13	Secret Data Items	
14	Confidential Data	
15	Security Question	
16	Debit Card Number	
17	Credit Card Number	
18	Sort Code	
19	Card type	
20	Cardholder name	
21	Your Passport Number	
22	Account Number	
23	Account Username	
24	Issue number	
25	Start Date	
26	Expiry Date	
27	Three digit Security Number	
28	Secure Number	
29	Membership Number	
30	Online Account	
31	Memorable Word	
32	Bank name	
33	Last date of Banking	
34	Online customer	
35	Customer Number	
36	Savings AccountNumber	
37	Current AccountNumber	
38	NI Number	
39	SirName	
40	First Name	
41	Social Security	
42	Date of Birth	
43	ContactInformation	
44	Telephone Number	
45	PhoneNumber	
46	EmergencyPhoneNumber	
47	CellphoneNumbe	
48	Email	
49	Fax Number	
50	Address 1	
51	Address 2	
52	Town	
53	City	
54	Post Code	
55	State	
56	Zip code	
57	Five-DigitTelephoneBankingNumber	
58	due date	
59	Bill to	
60	Recipt date	
62	Copy of your passport	
63	Sex	
64	Merital Status	
	TOTAL WEIGHT	0.6

A. Parameter Framework Descriptions

Parameter tuning framework for intelligent phishing detection is presented in Table II. It shows parameter optimal specification that has impact in fuzzy system performances. The parameters are assigned as follows: Membership Function is assigned 4 values in column 2. Input membership function (MF) is assigned Gbell shape in column 3. Column 4 demonstrates that output membership functions are linear. 16 epochs are assigned as shown in column 5 which presents the number of iterations. The number of tolerance is assigned to 0.01 in column 6. 150 training set are assigned in column 8, while 150 validation sets are assigned as shown in column 9. The experiment is run multi-times using two-fold cross-validation method as illustrated in column 10. This process is summarized in the next section. The results and analysis of this experiment are presented in section 5 and 6 and the best performance is also highlighted.

B. Parameter Framework Summaries

- Step 1: A total of 300 data are utilized in Framework, which are split into 150 training set and 150 test set. The training set is utilized to generate a model and to train the fuzzy model while the remaining 150 set is utilized for testing the model.
- Step 2: 4 membership functions values are assigned for the input.
- Step 3: Linear is set for the output membership functions.
- Step 4: Parameter optimization methods are assigned to hybrid, back-propagation and least square
- Step 5:16 epochs are assigned so that after 0.01 iterations, the process stops at the minimal error tolerance which is assigned to zero tolerance.

C. Training

To perform training and testing for the parameter tuning framework, Cross validation (CV) methods as mentioned above is applied to train and test the parameter tuning framework models. Using 2-Fold CV, data is randomly split into training and testing sets. 2-Fold cross-validation method is used since it can handle conventional data well given the 300 data-set [29]. While training set is used to train the model. Testing set is used to check the generalization and capability of the fuzzy models and to handle over-fitting that occur during training process.

D. Adaptive neuro-fuzzy Inference Architecture for Phishing Detection

A model similar to Sugeno type is generated and presented in Fig. 2. The structure consists of five functional components: Input Layer, Fuzzification, Rule base, Normalisation, and defuzzification [9]. ANFIS is a multilayer neural network and applies conventional learning algorithms including back-propagation when training set is present. The processes of learning and fuzzy reasoning performed by ANFIS based on rules include:

a) Layer 1: This is the input layer. Neuron in this step simply transmits crisp straight to the next layer.

b) Layer 2: is fuzzification. In this layer, inputs are taken and classified into a degree of membership functions in which they belong as fuzzy sets. This is shown in Fig. 3.

c) Layer 3: is a Rule base where all the rules are assigned weight between [0 and 1]. For every rule, implication is implemented that generates qualified consequent as a fuzzy set of each rule depending on the firing strength. A rules-base sample containing 5 fuzzy IF-THEN rules generated through experiments is presented in Fig. 4.

d) Layer 4: is Aggregation. In this layer, each rule is combined to make a decision. The output of the aggregation process is a fuzzy set whose membership function assigns a weighting for each output value.

e) Layer 5: is defuzzification. In this layer, the input for the defuzzification process is acombined output fuzzy set and the output is a single number. The most common defuzzify method is the centroid calculation [9].

Fig. 2, a fuzzy model shows that given the values of premise parameters, the overall output is expressed as *linear* combining consequent parameters. Hybrid learning algorithm is used as parameter optimization method to enhance performance. In the forward pass for that particular algorithm, functional signals move forward until layer 4. Then consequent parameters are classified by the least square estimate (LSE). The error rates in the backward pass get propagated backward, while the premise parameters get updated using the gradient descent [9].

TABLE.II. PARAMETERS FRAMEWORK ASSIGNED

							300 Data Set		**Cross-Validation**
Parameters & Dataset	**MFs value**	**Input MFs**	**Output MFs**	**Para. Optimization**	**No. of Epoch**	**No. of Tolerance**	**Training set**	**validation set**	2-Fold
Assigned Value	4	Gbell	Linear	Hybride	16	0.01	150	150	

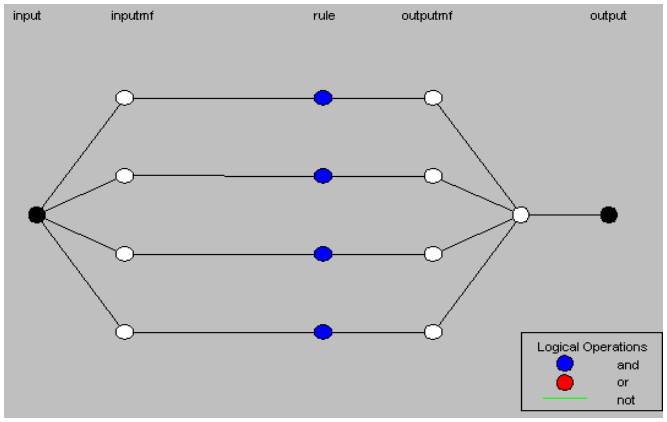

Fig.2. Fuzzy inference model for detecting phishing

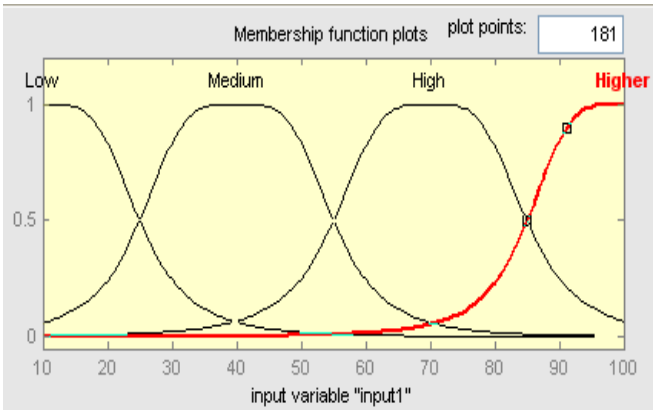

Fig.3. Fuzzy sets values with 4 membership functions after training.

If input1 is Legitimate then output is out1mf1 = 1
If input1 is Suspicious then output is out1 mf2 =1
If input1 is Phishing then output is out1 mf3 =1
If input1 is Legitimate then output is out1 mf4 =1
If input1 is Suspicious then output is out1 mf5 = 1

Fig.4. Rule base containing 5 fuzzy IF-THEN rules

E. Testing Framework

After the training was completed, the checking set was used to check and to test the model. The training process is repeated twice and the testing process is also repeated two-times utilizing training and validation sets only once.

The results are observed. Training outputs are presented in Fig. 3 which is input membership function, type generalized bell shape (Gbell) membership function with the value range of [0, 1] in Y-axis and a value range between [10, 100] on the X-axis. It is defined by linguistic terms including: low indicating legitimate, medium as presents suspicious, while high indicates phishing.

F. Basic Rules

Fuzzy IF-THEN rules are expressed in the form:

If A Then B, where A and B are labels of fuzzy sets [29] characterized by appropriate membership functions. Regarding their concise form, fuzzy if-then rules are usually utilized to obtain the imprecise modes of reasoning that does an important role in the human ability to decide in an environment of uncertainty and imprecision. A description of a simple fact in phishing detection is: If the risk is high or 100% risk, then it is a phishing. If the risk is 0% risk then it is a legitimate. Any number of risks between 0% to 100 is suspicious. An example of rules is shown in Fig. 4. During training, the learning algorithms learn data and use it to create rules. If-Then rules are used because fuzzy rules have been widely utilized successfully in controls and modeling [15].

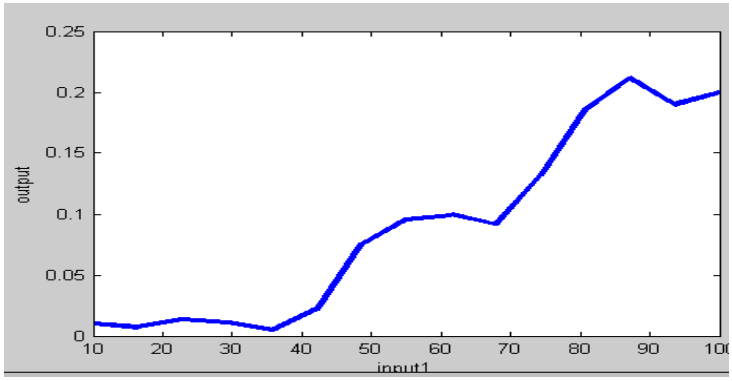

Fig.5. Performance evaluation graph for phishing website detection

TABLE.III. TRAINING AND TESTING RESULTS

Training set	validation set	Training Average error %	Testing Average error %	Testing Error Result %	Average Accuracy Results
150	150	0.012643	0.0126431	1.3%	98.74%

V. TESTING RESULTS AND DISCUSSIONS

After conducting extensive experiments, testing results are obtained in average error rates, which is a measure of the model accuracy performance in real time. The exact measurement is the overall output in which the model is compared. Fig. 6 presents the results as follows: Blue crosses on graphs indicate training results, while red stars indicate test results. An average test error rate obtaining is 0.012631 as shows in fig. 6. Fig. 4 also presents the system performance The training and testing errors are converted in to percentages and presented in Table III. Average testing errors in column 4 are rounded to 2 decimal places and converted in to percentage average error rates which is 1.3% as shown in column 5 and error rates into accuracy percentage in which is 98.74% overall achievement.

VI. ANALYSIS

The parameter tuning framework was evaluated using 2-fold cross-validation methods to measure the capability of the model. Parameters were assigned 4 membership functions values, and set to linear the output membership functions, hybrid was assigned as parameter optimization methods. 16 epochs are assigned so that the process stops at 0.01the minimal error tolerance. 0.012631 average errors was obtained, which demonstrated best results compared to other previous works. Our model suffered a modest error rate of 1.6%, which can be explained that the 4 membership function value was not the least visible by the given data. Thus is greater than the given variable example. Otherwise, the lower the average error rates, the better the results. The highest result achieved is nearer to the expected results, given the target performance to be closer to 100% accurate if not 100% accurate. In which case, 98.74% accuracy is nearer enough.

A. Comparisions

The techniques and the previous results are compared to determine the best results. The proposed approach utilized 300 data set randomly split in 150 training pair and testing on the remaining set which demonstrated an improvement of 0.34% higher compared to our previous work. Our previous work that is being improved which is Framework 3 and Framework 4 that used 228 and 342 features, assigned values of 15 parameters. 3 and 4 MFs were specified and assigned 12 and 10 Epochs. This experiment achieved 98.4%. Therefore the new approached have significant improvement.

To compare our results with other existing results in the field, our results are not directly comparable with the previous results for the following reasons: Firstly, our work has considered all possible components which are used as inputs in which features are extracted, which include legitimate site rules, user-behaviour profile, PhishTank, user-specific site, pop-up windows and user's credential. Secondly, from those inputs, 342 comprehensive data are gathered that were used for modeling.

Thirdly, adaptive neuro-fuzzy algorithm has been our proposed work which has not been considered in phishing detection field by other studies in this field. The previous work for example: Aburrous's studies applied fuzzy logic and datamining techniques with 27 features to detect phishing websites and achieved 83% and 84.4% accuracy [2], [32]. Aburrous's studies suffered high false positives. They only considered phishTank as their source for 27 features which are a small size. Ma also used a similar approach to Aburrou, but with large lexical features extracted from URL only [5], [28]. They achieved 95-99% accuracy.

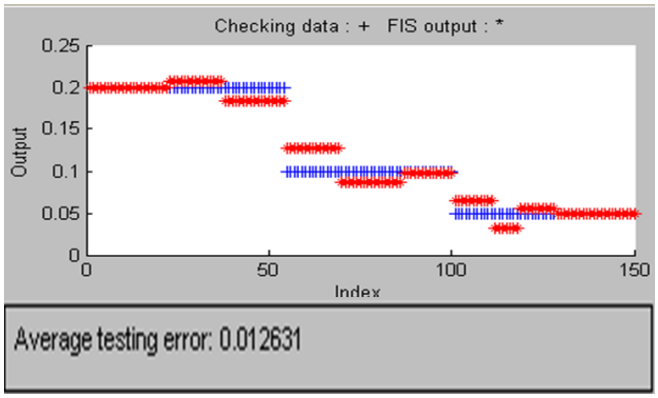

Fig.6. Result for framework

These previous studies have not actually used all the possible data in terms of size and diversity, therefore our 98.74% accuracy is much stronger than the existing results. Moreover parameter tuning framework has not been considered in literature in this field [9].

B. Findings

Based on the results of our experiment, we found that applying adaptive neuro-fuzzy algorithm with comprehensive data and proper parameter tuning can detect phishing website with high accuracy. We also found that while data and parameters can have influence on model performance, parameters have direct effect.

C. Limitations

In light of our results from extensive experiment, our results suffered an average errors rate of 1.3%. This can be explained that there was some defective data that caused overfitting and or unrefined parameter tuning also confused parameter that caused the model performance to suffer. The challenge in using ANFIS is that input membership function parameter is limited to either constant of linear.

VII. Conclusions and Future Work

Data has been extracted. Extensive experiments have been conducted. During 10-fold cross-validation data has been randomly split into train and to validate sets. We found that using comprehensive data through ANFIS with proper parameter tuning can detect phishing websites with high accuracy.

A. Contributions

The main contributions made in this paper includes: (1.) identified user's credential profiles as one of core component of input data that has not been utilized in the field. (2.) introduced novel data based on user's credential profile, introduced novel parameter tuning framework based on ANFIS algorithm using comprehensive feature, (3.) applied ANFIS for the first time in (phishing detection website) a new field.

The information about parameter tuning can provide a novel knowledge to researchers about the capabilities of applying ANFIS with comprehensive data and proper parameter settings.

The advantage is that the outcome from this study should provide a great knowledge and understanding to researchers in the field. The method can also be used across other fields in solving similar problems.

B. Feature work

The work do be done next is to extract large data from a wide range of samples and use different cross-validation with large data-sets.

References

[1] Financial Fraud Action UK, Cheque & Credit clearing Company, UKCARDS Association. Deception crimes drive small increase in card fraud and online banking fraud losses. Press Release, pp. 2, 2012 [online] www.financialfraudaction.org.uk. Accessed 24.7.2013.

[2] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Modelling Intelligent Phishing Detection System for e-Banking using Fuzzy data Mining," International, 2009.

[3] N. Sanglerdsinlapachai, and A. Rungsawang, "Using Domain Top-page Similarity Feature in machine learning-based Web Phishing Detection," In Procedings of IEEE 3rd International Conference on knowledge Discovery and Data Mining, pp. 187-190, 2010.

[4] G. Xiang, B. A. Pendleton, J. Hong, "Modelling content from human-verified blacklist for accurate zero-hour phish detection," probabilistic approach for zero hour phish detection, In Proceedings of the 15th European, 2009.

[5] J. Ma, L. Saul, S. Savag, G. Voelker, "Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs," Proc. of the 15th International Conference on Knowledge Discovery and Data Mining, Paris, France, pp. 1245-1254, 2009..

[6] PhishTank Site Checker (2013), GS! Networks, [online] < https://addons.mozilla.org/en-US/firefox/addon/phishtank-sitechecker/reviews/> Accessed 22.2.2014.

[7] C. Whittaker, B. Ryner, M. Nazif, "Large-Scale Automatic Classification of Phishing Pages," In the 17th Annual Network and Distributed System Security {NDSS'10} Symposium, 2010.

[8] S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, C. Zhang, "An empirical analysis of phishing blacklists" in Proceedings of the 6thConference on Email and Anti-Spam, 2009.

[9] J. S. R. Jang, "ANFIS: adaptive-network-based fuzzy inference system. IEEE,". Transactions on systems, MAN, and Cybernetics, Vol. 23, No. 3, 1993.

[10] R. Suriya, K. Saravanan, A. Thangavelu, "An integrated approach to detect phishing mail attacks a case study," SIN Proceedings of the 2nd international conference on Security of information and networks, north Cyprus, Turkey, October 2009, 6-10, pp. 193-199, vol. 3 ACM New York.

[11] L. Wenyin, N. Fang, X. Quan, B. Qiu, G. Liu, "Discovering Phishing Target based on Semantic Link Network," *Future Generation Computer Systems*, Elsevier, Volume 26, Issue 3, March 2010, pp. 381-388.

[12] G. Xiang, B. A. Pendleton, J. I. Hong, C. P. Rose, "A hierarchical adaptive," Symposium on Research in Computer Security (ESORICS'10). 268–285, 2010.

[13] X. Dong, J. A. Clerk, J .L. Jacob, "Defending the weakest link: Phishing Website Detection by analysing User Behaviours," IEEE Telecommun System, 45: pp. 215 – 226, 2010.

[14] B. Wardman, T. Stallings, G. Warner, A. Skjellum, "High-Performance Content-Based Phishing Attack Detection," eCrime Researchers Summit (eCrime), pp. 1-9, Conference: 7-9 Nov. 201 1, San Diego, CA.

[15] A. P. Barraclough, M. A. Hossain, M.A. Tahir, G. Sexton, N. Aslam "Intelligent phishing detection and protection scheme for online transactions," Expert Systems with Application 40, pp. 4697-4706, 2013.

[16] A. Le, A. Markopoulou, M. Faloutsos, "Phishdef: Url names say it all," INFOCOM, Proceedings IEEE, pp. 191-195, 2010.

[17] H. Huh, H. Kim, "Phishing Detection with popular search engine: Simple and effective", In Proceeding FPS'11 Proceedings of the 4th Canada-France MITACS conference on Foundations and Practice of Security, pp 194-207, 2012.

[18] D. Canali, M, Cova, G. Vigna, C. Krugel "Prophiler: A fast filter for the large-scale detection of malicious web pages," In Proceedings of the International World Wide Web Conference,. 2011.

[19] G. Xiang, J. Hong, C. P. Rose, L. Cranor," Cantina+: A feature-rich machine learning framework for detecting phishing web sites," ACM Transactions on Information and System Security (TISSEC), 14(2), pp. 2- 21, 2011.

[20] W. Ead, W. Abdelwahed, H. Abdul-Kader, "Adaptive Fuzzy Classification- Rule Algorithm in Detection Malicious Web Sites from Suspicious URLS," International Arab Journal of e-Technology 3 (1), pp. 1-9, 2013.

[21] G. Xiang , "Toward a phish free world: A feature-type-aware cascaded learning framework for phish detection", Thesis, Language technologies institute, School of computer science., 2013.

[22] Pinsent manson law expert, (2011). [online] http://www.pinsentmasons.com/en/expertise/sectors/core-industries--markets/universitiesandhighereducation/ Accessed 28.12.11.

[23] PhishTank, "Join the fight against phishing," 2011. [online] < http://www.phishtank.com/ > Accessed 5.6.2012 and 10.7.2013.

[24] Barclays Bank "online banking," 2012. [online] < http://www.barclays.co.uk/ > Accessed 8.12.2012.

[25] Financial Service Authority (FSA), (2013), UK [online] http://hb.betterregulation.com/external/List%20of%20banks%20-%2028%20February%202013.pdf and <www.fsa.gov.uk> Accessed 8.12.2012.

[26] G. B., Huange, Q. Y., Zhu, K. Z., Mao, C. K., Siew, P. Saratchandran, & N.Sundararajan, , (2006). Can threshold networks be trained directly? *IEEE Trans. Circuits syst. II*, vol. 53, no 3, 187-191.

[27] R. Kohavi, (1995). A study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection. *The International Joint Conference on Artificial Intelligence*, Computer Science Department Stanford University (IJCAI).

[28] J. T. Ma, "Learning to detect malicious URLs," Thesis, University of California, 2010.

[29] P. B. Sivarao, N.S.M. El-Tayeb, "A New Approach of Adaptive Network-Based Fuzzy Inference System Modelling in Laser Processing-A Graphical User Interface (GUI) Based," Journal of Computer Science. 5 (10), pp. 704-710, 2009.

[30] Complying with anti-phishing regulation (2012) http://help.wildapricot.com/display/DOC/Complying+with+anti-spam+regulations

[31] PhishTank, "Join the fight against phishing," 2012. [online] < http://www.phishtank.com/ > Accessed 5.7.2013 and 10.7.2013.

[32] M. Aburrous, M. A. Hossain, K. Dahal and F. Thabtah "Intelligent phishing detection system for e-banking using fuzzy data mining,"Expert Systems with Applications 37, pp. 7913-7921, 2010.

APPENDIX

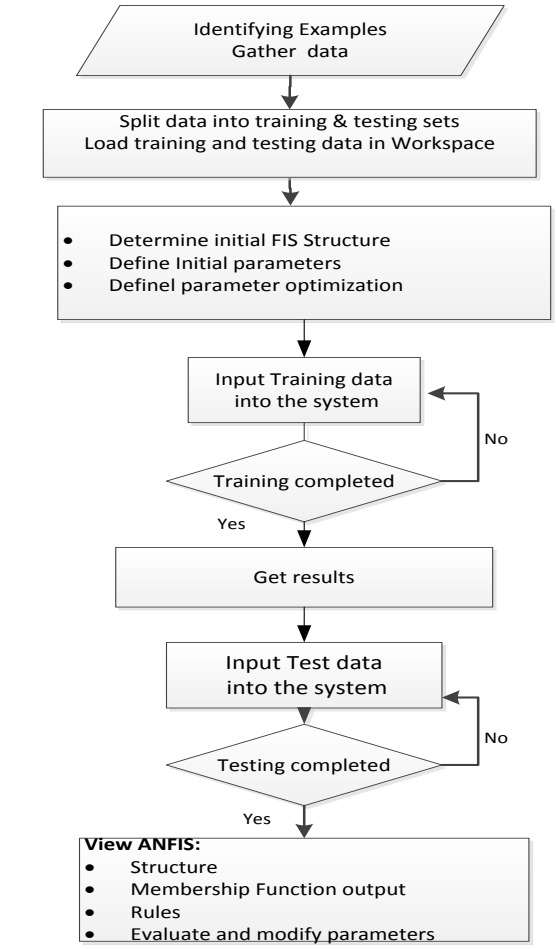

Fig.7. Conceptual method