Phishing Website Detection Fuzzy System Modelling

Phoebe Barraclough
Computer Science and Digital Technologies
Northumbria University
Newcastle Upon Tyne, NE1 8ST, United Kingdom
Phoebe.barraclough@northumbria.ac.uk

Graham Sexton
Computer Science and Digital Technologies
Northumbria University
Newcastle Upon Tyne, NE1 8ST, United Kingdom
Graham.sexton@northumbria.ac.uk

***Abstract*—This study investigates and identifies parameters in a single platform based on fuzzy system and neural network for phishing websites detection. The new approach utilizes Fuzzy systems, neural network with a set of parameters and a data set to detect phishing sites with high accuracy in real-time. A total of 300 data from six sources were used as training and testing sets using 2-fold cross-validation to train and validate the model, which has achieved the best performance (99.6%) compared to other results in the field.**

Keywords—phishing detection; fuzzy system; parameters

I. INTRODUCTION

Phishing attacks are almost doubled. The estimated cost is $1.5 billion in 2012 alone [1]. Despite various approaches developed to detect phishing attacks, these approaches still suffer high false positives, a lack of accuracy and real-time solutions, causing inadequacy in online transactions due to a lack of effective fuzzy rules, a lack of proper parameter tuning to facilitate a desirable output [2], [3], [4].

This study is focused on combating phishing attacks robustly by building a state-of-the-art fuzzy models, fuzzy rules, using parameter tuning base on Fuzzy System and neural network with six data sources to detect phishing websites accurately for online transaction users. As a result of this research, the main contributions are:

1) Introduced novel fuzzy rules for inference in order to classify between phishing, suspicious and legitimate websites

2) Iidentified new number of parameters based on Fuzzy system for phishing detection for the first time in the field which has offered the best performance compared to other studies in anti-phishing field.

A. Aim

The aim is to review and refine parameters based on fuzzy system using optimization techniques such as hybrid learning method.

B. The objectives are:

- To identify a wide-ranging data based on a diverse data sources.
- To identify appropriate set of parameters so that algorithm can solve a given problem.
- To generate Fuzzy models based on fuzzy logic and neural network algorithms.
- Train and validate the Fuzzy models in real-time environment.
- Provide a comparative study to demonstrate the effectiveness and capabilities of the system.

This study would add new knowledge in the field about fuzzy systems and motivate future development.

II. REVIEW OF LITERATURE

Anti-phishing methods widely utilize either URL blacklist or features based on machine learning techniques to detect phishing websites. The first is more intuitive requiring comparing URLs with blacklist, whereas the latter is complex. Features have been proposed in anti-phishing field to generate fuzzy rules and to detect phishing attacks, but some of these features are not discriminative enough. For example, Afroz and Greenstadt presented PhishZoo to identify phishing attacks [5]. Their method utilized website contents including images and HTML elements and applied Scaling Invariant Feature Transformed (SIFT) algorithm with fuzzy hashing to identify phishing websites. While fuzzy hashing method can identify a new phishing website, this approach can easily be broken through by restructuring HTML elements with no alteration of appearance to the websites.

In the attempt to improve the approaches, Aburrous applied Fuzzy-Data mining that include: JRip, RIPPER, PART, PRISM, C4.5, Classification Based-Association (CBA) and priori algorithms (except MCAR) with 27 features and a case study [6]. This approach obtained 83.7% accuracy, but suffered 16.3% error rates which are either caused by less features or poor parameter tuning. Additional features and proper parameter tuning could alleviate the problem.

Suriya considered quantifying and qualifying all phishing website characteristics [7]. Their method was based on fuzzy logic, using Link Guard and 3 layers. The main criteria include ‘code script checker’ that looks for tricks of attackers using JavaScript to hide data from users, a‘page content checker’ that checks for phishing sites based on its sub-criteria and a ‘domain name checker’ in web pages to assess whether phishing activity was taking place or not. Their approach accurately obtained 96%. However, this approach is limited because of using only 3 specific parts of a website, considering that phishing techniques are varied and evolve regularly. This can be overcome by extracting features from a wide spectrum of sources to cover techniques used by phishers enticing victims into giving up their credentials.

III. METHODOLOGIES

The new approach utilizes six data sources based on fuzzy systems and neural network in order to address the problem robustly. The six data sources: Legitimate site rule, User-behaviour profile, PhishTank, User-specific-site, Pop-up windows and User-credential profile are the core of our combined framework from which 300 features are extracted as shown in Fig. 1. The concept of feature-based approach is to find effective features that can be used through machine learning algorithms to generate fuzzy models, fuzzy rules and to classify between phishing, suspicious and legitimate websites. These are extended sources from our previous work that described feature extraction in detail [8].

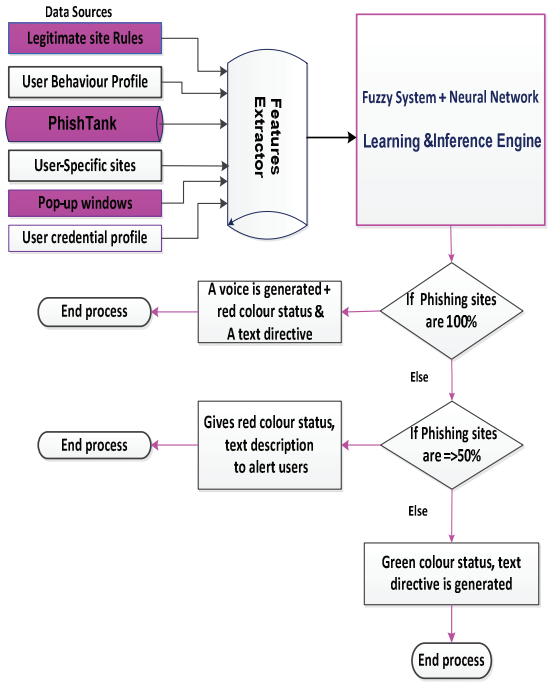

Fig. 1. Flow diagram for Phishing Detection

A. *Fuzzy [IF-THEN] Rules*

Our proposed Fuzzy If-Then rules similar to Sugeno-type [9] are expressed as:

Rule 1: If (legitimate_site_Rules features are Low) then (website is Legitimate) (0.3)

Rule 2: If (user_Behaviour_Profile features are Low) then (website is Legitimate) (0.3)

Rule 3: If (PhishTank features are Low) then (website is Legitimate) (0.3)

Rule 4: If (user_Specific_Site features are Low) then (website is Legitimate) (0.3)

Rule 5: If (Pop_Ups_Windows features are Low) then (website is Legitimate) (0.3)

Rule 6: If (user_credential_profile features are Low) then (website is Legitimate) (0.3)

Rule 7: If (legitimate_siteRules features are Medium) then (website is Suspicious) (0.6)

Rule 8: If (user_Behaviour_Profile features are Medium) then (website is Suspicious (0.6)

Rule 9: If (PhishTank features are Medium) then (website is Suspicious) (0.6)

Rule 10: If (user_Specific_Site features are Medium) then (website is Suspicious) (0.6)

Rule 11: If (Pop_Ups_Windows features are Medium) then (website is Suspicious) (0.6)

Rule 12: If (user_credential_profile features are Medium) then (website is Suspicious) (0.6)

Rule 13: If (legitimate_site_Rules features are High) then (website is Phishing) (1)

Rule 14: If (user_Behaviour_Profile features are High) then (website Phishing) (1)

Rule 15: If (PhishTank features are High) then (website is Phishing) (1)

Rule 16: If (user_Specific_Site features are High) then (website is Phishing) (1)

Rule 17: If (Pop_Ups_Windows features are High) then (website is Phishing) (1)

Rule 18: If(user_credential_profile features are High) then (website is Phishing) (1)

Where legitimates-site-rules, User-behaviour-profile, PhishTank, User-specific-sites, Pop-up-windows and User-credential profile are labels of fuzzy sets

Fuzzy IF-Then rules have been utilized successfully in fields such as controls and modelling.

IV. EXPERIMENTAL SETTINGS

Our Fuzzy Inference model is similar to sugeno-type. It has 5 functional components that enable the model to learn and reason. These include input layer, fuzzification, rule-base, normalization and defuzzification. These are illustrated in Fig. 2. The model is measured for its accuracy using 2-fold cross-validation. 300 features are randomly split into training and testing sets. Train on training-set and test on testing set.

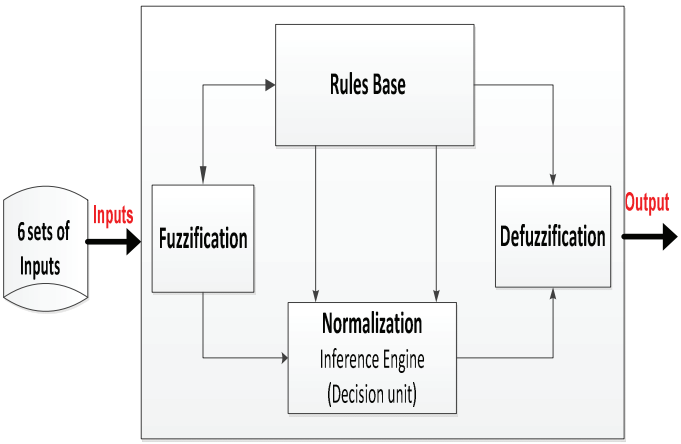

Fig. 2. Fuzzy inference systems functions

A. Training and Testing Results

For training and validating, first, parameters were tuned. The best result achieved from all 6 units tested is 99.6% accuracy. The parameter setting framework for the best results is given as follows:

- 6 number of membership functions are assigned to each input variable.
- The output type membership function is set to linear.
- Parameter optimization method for learning are assigned to hybrid, a mixed back-propagation and least square and error tolerance set to 0.
- 24 epochs of training are assigned so that the training performs 24 iterations.
- The process stops at zero as an error minimal tolerance.

B. Discussions

TABLE I. summarizes the average training and testing accuracy for six data sources (units) tested. The overall average test accuracy results achieved is 98.7%. The best achievement compared to the rest of the units tested is 99.6%.

The new approach based on Fuzzy system with six inputs has out-performed the previous results in the field. This result suggests that fuzzy systems and proper parameter tuning together with wide-ranging effective data can detect phishing websites with a higher accuracy.

TABLE I. SUMMARY RESULTS

	Six Data Sources Results					
	LSR%	***UBP%***	***PT%***	***USS%***	***PPW%***	***UCP%***
Training accuracy Results	97.95	98.82	98.07	98.73	98.00	98.9
Testing accuracy Results	97.95	98.80	98.06	98.74	97.99	99.6

V. CONCLUSIONS AND FUTURE WORK

This topic was chosen in order to investigate and extend the existing approaches. We have described the phishing detection process and the core of the framework, the fuzzy If-then rules for reasoning and identified the Fuzzy inference system functions. The results have shown that fuzzy systems using six data source and proper parameter settings can detect phishing sites with a higher accuracy. As a result of this research, two contributions are made as follows: Firstly, we introduced novel fuzzy rules for inference in order to classify between phishing, suspicious and legitimate websites. Secondly, we identified new numbers of parameters based on fuzzy systems for phishing detection which has offered the best results compared to other results in anti-phishing field.

Future work will be to extract a large data and utilize 20-fold cross validation to measure the models accuracy.

REFERENCES

[1] RSA Anti-Fraud Command Center. Available at: www.rsa.com (Accessed: 20 September 2013).

[2] H. Hamdan, "An Exploration of the Adaptive Neuro-Fuzzy Inference System (ANFIS) in Modelling Survival". PhD Thesis, 2013.

[3] J. S. R. Jang "ANFIS: Adaptive-Network-Based Fuzzy Inference System". *IEEE Transactions on systems, MAN, and Cybernetics*, (23) 3. 1993.

[4] J. Ma, "Parameter Tuning Using Gaussain Processes", Doctoral dissertation, University of Waikato, 2012.

[5] A. Afroz & R. Greenstadt, PhishZoo: "Detecting Phishing Websites by looking at them". In Proceedings of the IEEE Fifth International Conference on Semantic Computing (ICS '11), 2011.

[6] 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.

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

[8] P. A. Barraclough, A. M. Hossain, A.M., Tahir, G. Sexton & N. Aslam "Intelligent phishing detection and protection scheme for online transactions", *International Journal of Expert Systems with Applications* (ESWA) (40) 4697-4706, 2013.

[9] L.A. Zadeh, Fuzzy sets. "Information and Control", 8:338-353, 1965.