Journal of Multimedia Information System VOL. 5, NO. 2, June 2018 (pp. 99-104): ISSN 2383-7632(Online)
http://dx.doi.org/10.9717/JMIS.2018.5.2.99

A Comparative Study of Phishing Websites Classification Based on Classifier Ensembles

Bayu Adhi Tama[1] and Kyung-Hyune Rhee[1*]

Abstract

Phishing website has become a crucial concern in cyber security applications. It is performed by fraudulently deceiving users with the aim of obtaining their sensitive information such as bank account information, credit card, username, and password. The threat has led to huge losses to online retailers, e-business platform, financial institutions, and to name but a few. One way to build anti-phishing detection mechanism is to construct classification algorithm based on machine learning techniques. The objective of this paper is to compare different classifier ensemble approaches, i.e. random forest, rotation forest, gradient boosted machine, and extreme gradient boosting against single classifiers, i.e. decision tree, classification and regression tree, and credal decision tree in the case of website phishing. Area under ROC curve (AUC) is employed as a performance metric, whilst statistical tests are used as baseline indicator of significance evaluation among classifiers. The paper contributes the existing literature on making a benchmark of classifier ensembles for web phishing detection.

Keyword: Phishing website, classifier ensembles, performance comparison, significance test

I. INTRODUCTION

Hitherto, phishing has gained a lot of attention from cyber security researchers and practitioners due to its widespread escalation. Phishing deals with the trial to acquire personal information such as usernames, passwords, and credit card details, apparently for malevolent intention, by camouflaging as a trusted users over the Internet. Users can be targeted either through email scam, websites, or short message service. Using such a fake company branding, for instance, a well-known company with large customer base is a priceless target for brand-jacking; an attempt to abuse the trademarks of a company to fool targets. According to the report, nearly 90% of users have faced a security incident originating with a deceptive email, making an increase of phishing attacks at 65% in 2017 in comparison with the previous year [1].

Web phishing detection using machine learning techniques have been proposed in order to establish a deterrent action taken to countermeasure threat [2]. It detects threat intelligently using pre-defined model which is built by classification algorithm. The task of constructing classification model could be considered as binary classification problem which the classifier is trained to classify web phishing data set either as normal or malicious. Solving binary classification problem is non-trivial process as it oftentimes suffers high false positive rate (FPR). Most prior works have been focused on single classifier which might not appropriate to enhance detection accuracy and to reduce FPR at once [3].

Classifier ensembles train multiple learners to predict the final output. They aggregate several weak classifiers whose individual class prediction are incorporated in some techniques, i.e. voting, averaging, and so forth to establish final class prediction. Instinctively, classifier ensembles solve different problems that might be difficult to be tackled by only a single classifier [4]. Because of this benefit, classifier ensembles have been adopted in many real-world applications. Furthermore, 'no free lunch' theorem shows that there is no single classifier which is applicable for any problems [5]. Thus, in practical point of view, it is not straightforward to seek a good single classifier.

This paper investigates the performance of classifier ensembles for automatic web phishing detection. Several ensemble learning approaches are included in the study such as random forest (RF) [6], rotation forest (RotFor) [7], gradient boosted machine (GBM) [8], and extreme gradient boosting (XGBoost) [9]. Since these ensembles are constructed using a number of weak classification

Manuscript received January 31, 2018 ; Revised May 11, 2018 ; Accepted May 14, 2018. (ID No. JMIS-2018-0004)

Corresponding Author (*): Kyung-Hyune Rhee, Dept. of IT Convergence and Application Engineering, Pukyong National University (48513) , +82-51-629-6247, khrhee@pknu.ac.kr

[1]Dept. of IT Convergence and Application Engineering, Pukyong National University, Korea, bayuat@pukyong.ac.kr

models, several tree-based classifiers, i.e. decision tree (DT) [10], classification and regression tree (CART) [11], and credal decision tree (CDT) [12] are also incorporated in our experiment.

The rest of the paper is structured as follows. Section 2 presents state-of-the-art review of phishing web detection found in the literature, while Section 3 describes overview of classification algorithms used in this study. The data set, validation technique, and significance test based on statistics are provided in Section 4. Next, Section 5 further discusses the experimental result, and finally the paper is concluded in Section 6.

II. PHISHING WEB DETECTION: A REVIEW

Prior researches have considered various machine learning algorithms for phishing web detection. However, most related works have been focused on a single classifier. Even though there exist a plethora of detection methods have been previously proposed such as LibSVM [13], fuzzy classifier [14], and to name a few, we restrict only several researches which data set in [15] is used for the experimentation. Phishing web detection using self-structuring neural network is proposed by [16] [17]. The proposed algorithm show competitive results in terms of various evaluation metrics. A study in [18] suggests hybrid approach for identifying phishing websites. The proposed approach eliminates unused features from previous works.

Rule based phishing detection is proposed by [19]. The experiment reveals that the error-rate has decreased for all the algorithms, CBA classifier algorithm has the lowest error-rate with 4.75%. A performance comparison of machine learning algorithms for web phishing detection has been conducted by [20]. Several classifiers have been included in the study, i.e. RF, DT, REP Tree, decision stump, and so forth. The authors claimed that RF with REP Tree is the best performer. The combination of computational based feature selection and a number of classification algorithms, i.e. RIPPER, PART, and C4.5 have been suggested to improve the performance of web phishing detection [21]. According to the their experiment, there are slightly performance drop when comparing full feature set against reduced set for RIPPER classifier. However, for PART and C4.5 show undeviating performance.

A novel web phishing website based on probabilistic neural network (PNN) has been presented in [22]. A k-medoids clustering approach is also incorporated in order to evaluate the complexity of the proposed method. Based on their experiment, an effective detection model with a reduced complexity can be built without sacrificing detection accuracy. Finally, a hybrid feature selection technique by combining scores from two effective feature selection methods, i.e. information gain and chi-square is described in [23]. The results obtained from applying the proposed method against full feature set, it has been revealed that the proposed method is able to pick relevant features that impact on the phishing detection rate.

III. CLASSIFICATION ALGORITHMS

3.1 Single Classifier

In this section, different single classification algorithms used in our study are briefly illustrated as followings.

- Decision Tree (DT)

Tree are produced in a top-down approach from root to nodes. The selection of the feature for a node is based on the impurity of the distribution of the class label. The impurity might be quantified in different way, e.g. entropy-based and Gini index. In order to avoid over-fitting in the training set, it is recommended to apply pruning strategy in order to generalize the tree generated by generating sub tree during the growing stage. The two main alternatives for constructing trees are the ID3 algorithm and the C4.5 algorithm, however, in this experiment, we use C50 algorithm which is the most renowned tree-based implementation [24]. There are several parameter in C50, i.e. confident factor (CF), sampling factor that specifies the random proportion of the data should be used to train the model, and global pruning step to simplify the tree.

Classification and Regression Tree (CART)

The classifier is a tree-constructing technique which identifies splitting variables based on an exhaustive search. It has a number of advantages over other classification methods i.e. it can handle numerical data that are highly skewed and it has sophisticated method for dealing with missing variables. For CART, there are two parameters, i.e. the number of folds in the internal cross-validation (f) and the minimal number of observations at the terminal nodes (t). We considered f and t are 5 and 2, respectively. Furthermore, heuristic process for binary split of nominal attributes and the pruning strategy are used. We used CART which space parameter of tree is optimized by evolutionary algorithm.

- Credal Decision Tree (C-DT)

Unlike DT which uses imprecise information gain ratio as split criterion to select the split attribute at each branching node, C-DT comes with an imprecise probabilities and the application of uncertainty measures for the original split criterion [25]. It uses reduced-error pruning (with back-fitting) and sorted values for numeric attributes. Missing values and numeric attributes are treated like C4.5. Learning parameter setting of C-DT includes fold numbers which specifies the amount of data used for pruning, root attribute which is used to fix the root node of the tree, and S value which is a parameter in the Imprecise Dirichlet Model to obtain imprecise probabilities as intervals.

3.2 Classifier Ensembles

Now, we discuss about different orchestration techniques to combine single classifier as follows.

Random Forest

This generates a number of trees. Random trees are grown without pre- or post-pruning, which contributes to their diversity. At each node, the feature to split upon is chosen from a randomized split of the original feature. Classification accuracy is gained some increase since the diversity of the trees. There are only two parameters in RF, i.e. number of trees and the number of variables to try at each split. Because selecting large number of trees leads to reduce the performance of ensemble, we consider the number of trees is 500 and set the number of variables to the square root of the total number of predictors.

Rotation Forest

Rotation forest depends upon unstable classifiers, i.e. decision tree regarding rotation of the space. It emphasize on the idea that diversity can be implemented without jeopardizing either data objects or features. The potential accuracy loss of the base classifiers is counterbalanced by increasing diversity. The feature set F is randomly partitioned into L subsets, PCA is run separately on each subset, and a new set of the extracted attributes is constructed by pooling all principal components. Then the data are transformed into the new feature space. An iteration number is one parameter which represents the number of iterations to be performed. Besides, base classifier and projection technique can also be specified.

Gradient Boosted Machine

Gradient boosted machine is constructed to improve the performance of CART. Final class prediction is made through the same type of base classifiers forming the ensemble. One of the main problem in the tree learning is to find the best split. To solve this issue, exact greedy algorithm is commonly used. We use original GBM algorithm found in [8] and a fast implementation of GBM, so called XGBoost [9]. Like RF, different parameters can be assigned such as num_trees is 500, nrounds = 10, α, λ, and max_depth.

IV. EXPERIMENT CONFIGURATION

4.1 Data set

We employed publicly available data set which is specifically for web phishing detection [15]. Even though there exist plethora of researches about detecting phishing website have been done, no dependable training data set has been proposed for evaluating machine learning algorithms. The data set is made up of 30 input features with 1 class label feature. The number of samples is 11,055 instances with the proportion of samples belonging to negative (-1) and positive (+1) class is 44.31% and 55.69%, respectively. The data set has been pre-processed by the authors of [19] [17] into a unified format and no missing values are found. In the data set, some new features are introduced and only the important features that have been proved to make an effective phishing website detection are included.

4.2 Resampling Approaches

Performance evaluation of a machine learning algorithm relies on the model selection procedures. Resampling procedures offer a performance approximation in terms of repeatedly dividing data set D to form a training set and a test set. Suppose Tr_i depicts the training set and Te_i is the test set, in the i-th iteration of the resampling procedure, such that:

$$Tr_i \cap Te_i = \emptyset \text{ and } Tr_i \cup Te_i = D. \tag{1}$$

In this experiment, different resampling procedures are used such as k-fold cross validation, subsampling, and bootstrap. In the k-cross validation, make k disjoint partitions of approximately equal size. Each k iteration, a different partition is used for testing and the others for training. Subsampling is a hold-out with repetition, where only a subset of the data set is used in each iteration. Furthermore, bootstrap obtain Tr_i by sampling n items with replacement from D and $Te_i = D \,/\, Tr_i$.

In order to acquire the same element at each resampling procedure, we are interested to investigate the following methods: 2 times repeated 10-fold (2x10f), 4 times repeated 5-fold (4x5f), 20 times repeated 2/3 hold-out (20xho), and 20 times repeated boostrap (20xboot). Area under ROC curve (AUC) is used as a performance metric and Demsar procedure [26] is followed to determine whether a statistically significance exist in the performance of multiple classifiers. Demsar proposes Friedman test as a wide-ranging nonparametric paired test. The test calculates the p-value based on the null hypothesis that all classifiers have performed 'equivalent' with respect to their rankings. If the Friedman test indicates 'significant', a post-hoc test using Nemenyi is recommended.

V. RESULT AND DISCUSSION

In this section, the results of our experiment are discussed. Fig.1 depicts the mean average of classifier's performance with respect to AUC value. Random forest (RF) has shown the best performance, followed by extreme gradient boosted machine (xgboost), and C50. Surprisingly, the worst algorithm goes to gradient boosted machine (GBM). Among single classifiers, C50 denotes the most effective algorithms for web phishing detection, followed by credal decision tree (C-DT) and CART. In addition, the results indicate that in the group of ensemble learners, RF outperforms xgboost and there is a notable performance gap between xgboost and GBM as well.

Some classifiers have no performance differences regardless of resampling strategies used, i.e.xgboost, GBM, and RF, whilst other classifiers, i.e. rotation forest (RoF) and C-DT show their performance variability with reference to resampling approaches. In addition, performance result of each classifier ensemble with respect to standard cross-validation technique, i.e. 10fold cross-validation (10f) is presented in Fig.2.

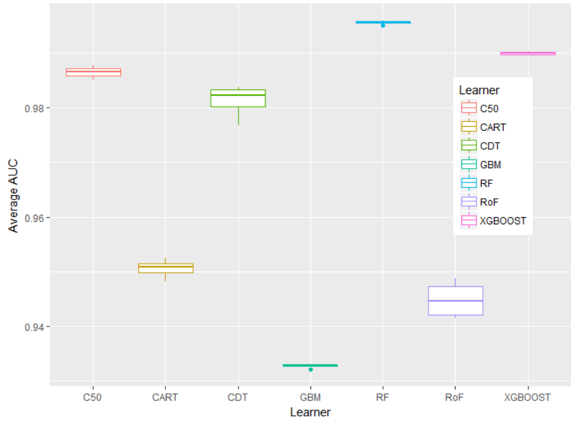

Fig. 1. Performance average in terms of AUC value over different resampling strategies.

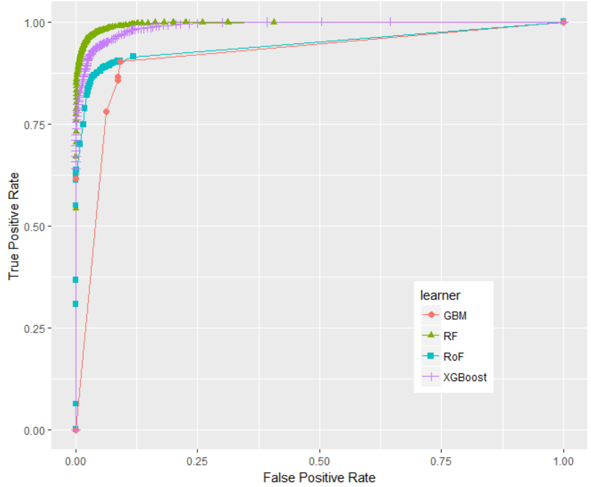

Fig. 2. Performance average of classifier ensembles for 10f

It is obvious that the top performer among ensemble algorithms is RF, whilst GBM have performed worse in phishing web detection. In order to provide an ample comparative study, the performance differences of all classifiers are subsequently benchmarked using statistical test. First of all, the result of Friedman test is shown in Table 1. The Friedman test indicates that there exist a highly significant (p < 2.2E-16) difference among classifiers regardless of resampling approaches used. Since Friedman test points out the significance of these results, it is worthwhile to conduct Nemenyi post-hoc test. The results of the post-hoc test at each resampling approach are visually represented with critical difference (CD) diagram as shown in Figure 3-6. We are interested to use significant level α=0.01.

Table 1. The result of significant test using Friedman test.

Resampling approaches	Chi-squared	*p*-value
2x10f	111.73	< 2.2E-16
4x5f	112.74	< 2.2E-16
20xho	116.96	< 2.2E-16
20xboot	117.43	< 2.2E-16

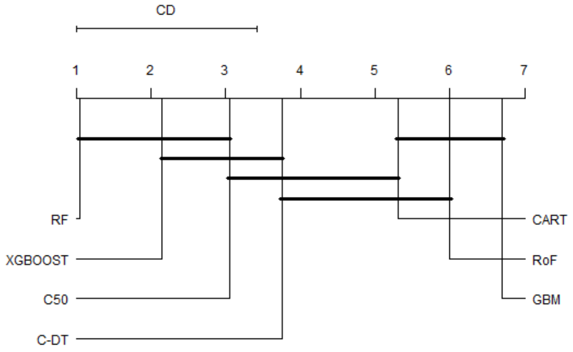

Fig. 3. Critical difference diagram of 2x10f

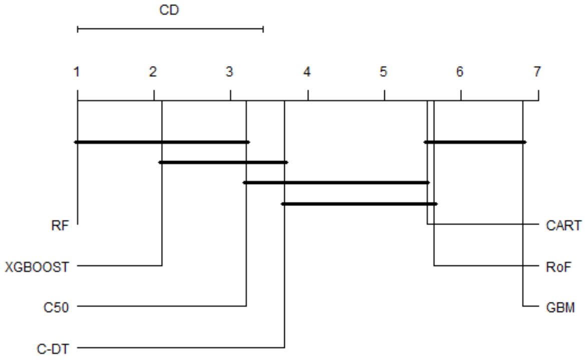

Fig. 4. Critical difference diagram of 4x5f

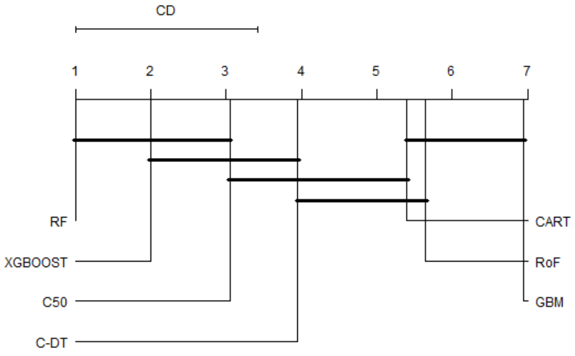

Fig. 5. Critical difference diagram of 20xho

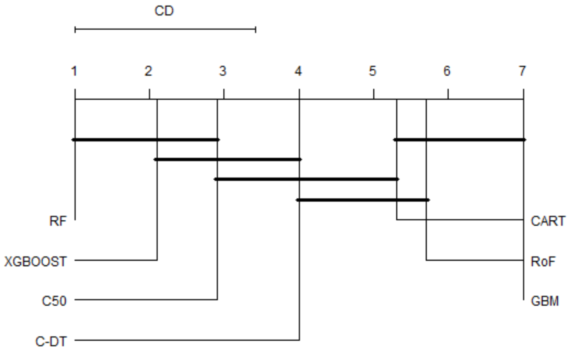

Fig. 6. Critical difference diagram of 2x10f

The comparison of the groups of classifiers against each other are described in Fig.3-6. The groups of classifiers that are not significantly different with other groups are connected with the straight line, whilst the top line indicates the interval of the Friedman CD's value. The graphs indicate that the performance of RF, xgboost, and C50 are not significantly different regardless the validation methods used. In addition, the Friedman test reveals that GBM performs significantly worse than RF and xgboost, which seems to possess equivalent AUC value in all resampling approaches. Furthermore, CART and RoF share equivalent performance in terms of 4x5f and 20xho approaches.

VI. CONCLUSION

This paper provided a comparative study of classifier ensembles for phishing web detection. A number of ensembles algorithms and single classification algorithms were included in the experiment. Their detection performance were evaluated using AUC value with respect to different resampling approaches. The experimental results revealed that random forest was superior to other ensembles, i.e. xgboost, rotation forest and GBM and to single classifiers, i.e. C50, C-DT, and CART. Further study should include other web phishing data set in order to provide a more comprehensive benchmark.

Acknowledgement

This work was supported by a Research Grant of Pukyong National University (2017).

REFERENCES

[1] A.-P. W. Group, "White paper: Phishing response trends," tech. rep., 2017.

[2] S. C. Jeeva and E. B. Rajsingh, "Intelligent phishing URL detection using association rule mining," Human-centric Computing and Information Sciences, vol. 6, no. 1, pp. 1-19, 2016.

[3] B. A. Tama and K. H. Rhee, "Performance analysis of multiple classifier system in DoS attack detection," in International Workshop on Information Security Applications, pp. 339-347, Springer, 2015.

[4] N. C. Oza and K. Tumer, "Classier ensembles: Select real-world applications," Information Fusion, vol. 9, no. 1, pp. 4-20, 2008.

[5] D. H. Wolpert, "The lack of a priori distinctions between learning algorithms," Neural computation, vol. 8, no. 7, pp. 1341-1390, 1996.

[6] L. Breiman, "Random forests," Machine learning, vol. 45, no. 1, pp. 5-32, 2001.

[7] J. J. Rodriguez, L. I. Kuncheva, and C. J. Alonso, “Rotation forest: A new classifier ensemble method," IEEE transactions on pattern analysis and machine intelligence, vol. 28, no. 10, pp. 1619-1630, 2006.

[8] J. H. Friedman, “Greedy function approximation: a gradient boosting machine," Annals of statistics, pp. 1189-1232, 2001.

[9] T. Chen and C. Guestrin, “Xgboost: A scalable tree boosting system," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 785-794, ACM, 2016.

[10] J. R. Quinlan, C4.5: programs for machine learning. Elsevier, 2014.

[11] W.-Y. Loh, “Classification and regression trees," Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, vol. 1, no. 1, pp. 14-23, 2011.

[12] C. J. Mantas and J. Abellan, “Credal-C4.5: Decision tree based on imprecise probabilities to classify noisy data," Expert Systems with Applications, vol. 41, no. 10, pp. 4625-4637, 2014.

[13] R. B. Basnet, S. Mukkamala, and A. H. Sung, “Detection of phishing attacks: A machine learning approach," Soft Computing Applications in Industry, vol. 226, pp. 373-383, 2008.

[14] 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, vol. 37, no. 12, pp. 7913-7921, 2010.

[15] M. Lichman, “UCI machine learning repository," 2013.

[16] F. Thabtah, R. M. Mohammad, and L. McCluskey, “A dynamic self-structuring neural network model to combat phishing," in Neural Networks (IJCNN), 2016 International Joint Conference on, pp. 4221-4226, EEE, 2016.

[17] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, no. 2, pp. 443-458, 2014.

[18] M. Dadkhah, M. Dadkhah, S. Shamshirband, S. Shamshirband, A. W. Abdul Wahab, and A. W. Abdul Wahab, “A hybrid approach for phishing web site detection," The Electronic Library, vol. 34, no. 6, pp. 927-944, 2016.

[19] R. M. Mohammad, F. Thabtah, and L. McCluskey, ”Intelligent rule-based phishing websites classification," IET Information Security, vol. 8, no. 3, pp. 153-160, 2014.

[20] A. Hodzic, J. Kevric, and A. Karadag, “Comparison of machine learning techniques in phishing website classification," 2016.

[21] F. Thabtah and N. Abdelhamid, “Deriving correlated sets of website features for phishing detection: A computational intelligence approach," Journal of Information & Knowledge Management, vol. 15, no. 04, p. 1650042, 2016.

[22] E.-S. M. El-Alfy, “Detection of phishing websites based on probabilistic neural networks and k-medoids clustering," The Computer Journal, pp. 1-5, 2017.

[23] K. D. Rajab, “New hybrid features selection method: A case study on websites phishing," Security and Communication Networks, vol. 2017, 2017.

[24] R. Quinlan, “Data mining tools See5 and C5.0," 2004.

[25] J. Abellan and S. Moral, “Building classification trees using the total uncertainty criterion," International Journal of Intelligent Systems, vol. 18, no. 12, pp. 1215-1225, 2003.

[26] J. Demsar, “Statistical comparisons of classifiers over multiple data sets," Journal of Machine learning research, vol. 7, no. Jan, pp. 1-30, 2006.

Authors

Bayu Adhi Tama received his PhD degree from Pukyong National University, Rep. of Korea in 2018. He is currently a postdoctoral research fellow at the School of Management Engineering, Ulsan National Institute of Science and Technology, Rep. of Korea. His current research interests include data analytics for business process management, information security, and healthcare informatics.

Kyung-Hyune Rhee received his MS and PhD degrees from Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea in 1985 and 1992, respectively He is currently a Professor in the Department of IT Convergence and Application Engineering at Pukyong National University, Republic of Korea. His research interests are data mining and its applications, multimedia engineering, and information security.