Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 3, March 2018, pg.68 – 72

Deep Auto-Encoder Neural Network for Phishing Website Classification

Sefer Kurnaz[1], Wisam Gwad[2]

[1,2]Computer Engineering & Altınbaş University, Turkey

[1] sefer.kurnaz@altinbas.edu.tr; [2] wisam.gwad@ogr.altinbas.edu.tr

Abstract— In this paper, deep auto-encoder technique proposed for website phishing classification problem. The dataset obtained from UCI which contain most common machine learning datasets. The obtained dataset consists from 30 attributes and the 31th attribute represented (target) there is phishing or not). The first auto-encoder extracted sensitive features and reduce the dimension of features. The second auto-encoder also extracted features from output of first auto-encoder and reduce the dimension of features too. The extracted features classified by using SoftMax classifier. All these parts stacked and trained in supervised learning. The experimental results show that proposed method presented best results than previous works.

Keywords— Phishing website, Deep Auto-encoder, SoftMax.

I. Introduction

As people progressively trust on the Internet and online applications for business, personal backing and asset, Internet deception becomes a better and greater risk. Internet scam takings several methods, from affected objects offered for sale on eBay, to insulting reports that manipulate supplies prices, to fraud that capacity great riches if the prey will aid a foreign monetary deal through his own bank account.

Recently, phishing is understood as an inspiring risk increasing speedily every day. It is measured as an illegal action that assimilates social-engineering and technical approaches to steal confidential data of consumers such as usernames and passwords (Manning & Aaron ,2015). In that sense, Lungu and Tabusca argues that the current economic crisis is a reflection of the increasing attacks and violations of internet users' data (Lungu & Tabusca, 2010). Phishing techniques are classified into several types according to the applied channel of proliferation, these include malware, phishing emails, and bogus websites (Jain & Richariya, 2011).

United states business losses tens of million dollars, if not billions, every year produced by phishing attacks (T. Kitten, 2015). Anti-Phishing Working Group (APWG) informed 123,972 unique phishing attacks worldwide over millions of fake websites on the second half of the year 2014.

Phishing has been growing really fast, in the past two years, the number of unique reported phishing attacks per month has increased more than 160 times and the number of unique reported phishing sites per month has increased about 16 times. In June 2006, 130 legitimate brands have been attacked (Anti-Phishing Working Group, 2006). Financial services were the most targeted industry sector. Depend on their information, the average uptime of a phishing website is 10 hours and 6 minutes while the normal is three times inferior. The best ten target firms have been always attacked even more than a thousand times each month (Aaron & Rasmussen, 2014). The Phish Tank's case information presents more than a half a million effective phishing website for the year 2015 (Phishtank, 2016). Furthermore, in February 2016 the Scam Watch displays almost $180,000 money loss in less than 1800 reports while only %1.4 of them are reports with financial loss (Scamwatch, 2016). These alerts demonstrate that cyber criminals are doing their job excellently, and now it is our turn to make some countermeasures in order to mitigate this huge amount of loss.

II. LITERATURE SURVEY

The phishing classification solutions are usually separated into two main classes: human-based methods and machine-based methods.

Altaher et al. relied on Adoptive Developing Fuzzy Neural Network (EFuNN) to generate Phishing Evolving Neural Fuzzy Framework (PENFF) to distinguish of unidentified "zero-day" phishing emails by treatment all related feature vectors to found rules for guess. Thus, PENFF method trusts on the resemblance of features involved in the email's body and URL. (Altaher & Al-Momani & Wang, 2012).

Jameel and George presented a feedforward neural network to classify the phishing email by mining features from the email's slogan and HTML organization. Their proposed algorithm was verified on 18 features using 5 hidden neurons. For this algorithm, a training is requisite before applying it which takes 173.55 msec. The time for testing a single email is 0.00069 msec. The spent time will growth with the growth in the neurons number while it is still measured low. With respect to the results, the algorithm demonstrated high precision of 98.72%, and a learning rate of 0.01. (Jameel & Loay and George 2013)

Zhang et al. intended at approximating the precision of the cross validation method in distinguishing phishing emails. The author used multilayer feedforward neural networks (NN) model with various numbers of hidden units and activation functions to verify that NNs can offer fairly precise and effective results with a predictable number of hidden elements. It is cost declaring that he showed these results even with little training while choosing the features set will attain improved results (Zhang & Yuan, 2013)

Al Momani et al. presented a new idea that showed exceptional results in terms of true positive, true negative, sensitivity, accuracy, F-measure and general correctness compared with other methods. Additionally, the method presented competence in guessing the values of these emails in online manner, and long-life employed with footmark overwhelming memory. The model Al Momani industrialized is named Phishing Dynamic Developing Neural Fuzzy method (PDENF) for guessing unidentified phishing emails and distinguishing them in zero day (Almomani & Gupta &Wan, 2013).

Rathi et al. intended at comparing the performance between method with a feature selection and method without a feature selection. Firstly, the appraised data was observed without any filters or features selection, then the classifiers were verified every at time start with the best-first feature selection to be talented to designate the most useful features and then relate different classifiers for classification. The Random Tree classifier showed a 99.72% correctness which means it works greatest to distinguish spam emails. (Rathi & Pareek, 2013)

Additional method was industrialized later in 2014 by Akinyelu to improved categorize phishing emails using forest machine learning method. This method was verified on data comprising about 2000 phishing emails with innovative features, and it was able to classify phishing emails with high efficacy (99.7%) with low false negative (FN) and false positive (FP) rates. Hence, Akinyelu's method is more effective in terms that it needs less features to classify phishing and supply additional precise results. (Akinyelu & Adewumi, 2014)

Nizamani et al. Proposed a new classification model by using an innovative selection of features where the various categories were compared in terms of the fraudulent email classification rate. The research was showed applying different classification methods and algorithms, such as J48, SVM, NB, and CCM, furthermore, to various features sets. A correctness ratio of 96% was implemented and the results showed that the level of correctness was pretentious by the kind of determined features rather than the classifiers' type (Nizamani & Memon & Glasdam, 2014)

The listed researchers are most famous researches in this field. The proposed method different from all these techniques which used deep auto-encoders also presented more satisfactory results when compared with previous works.

III. PROPOSED METHOD

In this paper, deep auto-encoder proposed for phishing website classification. The features of phishing website become input to the first auto-encoder which extracted high level features and reduced dimension of features from 30 to 28. The output of first auto-encoder become input to the second auto-encoder which reduce the dimension of extracted features from first auto-encoder to the 27.

The purpose from two auto-encoder is to reduce the feature dimension gradually and learn most important and sensitive features. The output of the last auto-encoder become input to the SoftMax that classify the features in to two labels there is phishing or not.

In the last stage, the two auto-encoders and SoftMax are stacked and trained by using supervised learning. Then, the system tested by using another data to check the performance of the proposed method. The accuracy is calculated after the testing is complete see Fig. 1.

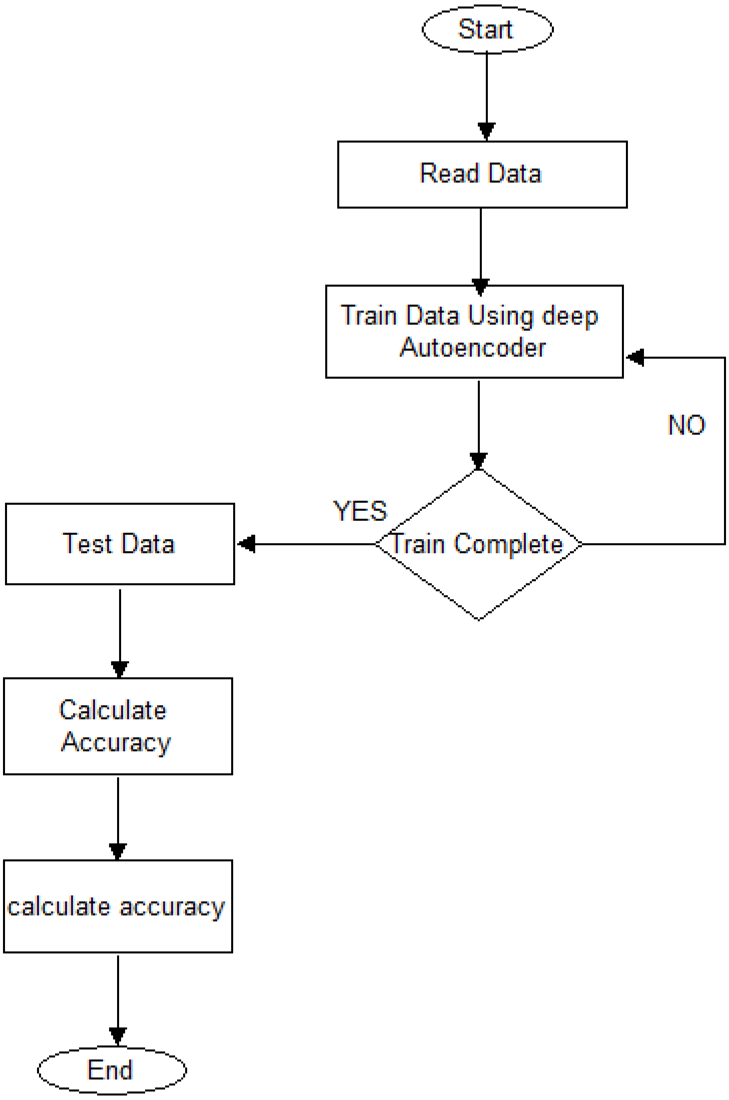
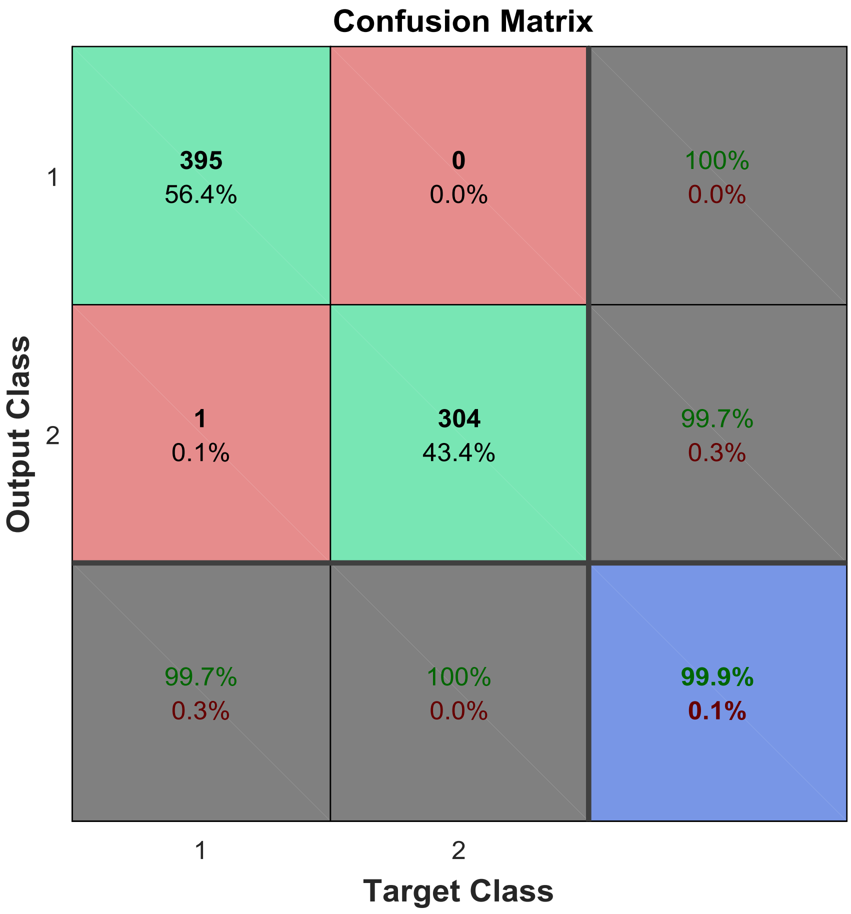


Fig. 1 Proposed Method Flowchart

IV. EXPERIMENTAL RESULTS

The proposed method tested by using data published in UCI repository which more famous machine learning datasets published on it. The experimental done by using intel core-i7 machine with 8GB Ram. The experimental results show 99.9% accuracy which is satisfactory result when compared which previous research's.

The results presented in confusion matrix see Fig.2. for presenting the performance the system in details in phishing and not phishing cases.



The proposed results compared with famous and newest research in this field, the proposed method compared with 10 techniques proposed for phishing website classification.

The best performance in previous researches is 97.75 which our proposed method best than this technique nearly 2.20%.

The comparison is presented in the TABLE I, furthermore the table proposed the techniques and the obtained results compared with our proposed method.

TABLE II
COMPARISON OF RESULTS

NO	Performance Comparisons		
	Reference	Methods	Accuracy
1	([Tahir et al, 2016)	J48 + RF	97.4491%
2	([Tahir et al, 2016)	J48+IBk	97.75%
3	([Tahir et al, 2016)	RF+IBK	97.3134%
4	([Tahir et al, 2016)	NB+RF	97.422%
5	([Tahir et al, 2016)	NB+IBK	97.5305%
6	([Tahir et al, 2016)	BN+IBK	97.75%
7	([Tahir et al, 2016)	BN+RF	97.4491%
8	([Tahir et al, 2016)	SMO+RF	97.53%

9	([Tahir et al, 2016)	FURIA+IBk	97.53%
10	([Tahir et al, 2016)	FURIA+RF	97.37%
11	**Proposed Method**	**Deep auto-encoder+SoftMax**	**99.9 %**

V. CONCLUSIONS

Phishing website problem increased in the recent years because of increasing in the internet application such as online shopping, banking and registrations. In this paper, a new method was proposed for classifying the phishing website by using deep auto-encoder neural network. The proposed method is first time used to classify phishing problem. The new method proposed satisfactory results when compared with previous researches.

As future work the phishing websites can by classified by using another deep learning technique such as LSTM, Deep belief neural network and recurrent neural network.

REFERENCES

[1] Manning, R., & Aaron, G. (2015). Phishing Activity Trends Report. Anti-Phishing Work Group, Tech. Rep. 1st -3rd Quarter.

[2] Lungu, I., & Tabusca, A. (2010). Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions. Informatica Economica, 14(2), 27.

[3] Jain, A., & Richariya, V. (2011). Implementing a web browser with phishing detection techniques. arXiv preprint arXiv:1110.0360.

[4] T. Kitten, \FBI Alert: Business Email Scam Losses Exceed $1.2 Billion," http://www.bankinfosecurity.com/fbi-a-8506/op-1, 2015.

[5] Anti-Phishing Working Group. Phishing activity trends report, June 2006. http://antiphishing.org/reports/apwg report june 2006.pdf, June 2006.

[6] M G. Aaron and R. Rasmussen, \Global Phishing Survey: Trends and Domain Name Use in 2H2014," APWG, no. May, pp. 1{38, 2014. [Online]. Available: http://docs.apwg.org/reports/APWG Global Phishing Report 2H 2014.pdf

[7] *Phishtank status, " http://www.phishtank.com/stats.php, accessed: 2016-03-12.*

[8] Scamwatch status," http://scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing, accessed: 2016-03-12.

[9] Altaher, A , Al-Momani, A., Wan, T. C, Manasrah, A., Al -Momani, E., Anbar, M., ... & Ramadass, S. (2012). Evolving fuzzy neural network for phishing emails detection. Journal of Computer Science, (7), 1099.

[10] Jameel, Noor Ghazi M., and Loay E. George. Detection of phishing emails using feed forward neural network. International Journal of Computer Applications 77 2013.

[11] Zhang, N., & Yuan, Y. (2013). Phishing detection using neural network. Department of Computer Science, Department of Statistics, Stanford University. Web, 29.

[12] Al-Momani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Al-Momani, E. (2013). A survey of phishing email filtering techniques. Communications Surveys & Tutorials, IEEE, 15 (4), 2070-2090.

[13] Rathi, M., & Pareek, V. (2013). Spam Mail Detection through Data Mining-A Comparative Performance Analysis. International Journal of Modern Education and Computer Science, (12), 31.

[14] Akinyelu, A. A., & Adewumi, A. O. (2014). Classification of phishing email using random forest machine learning technique. Journal of Applied Mathematics.

[15] Nizamani, S., Memon, N., Glasdam, M., & Nguyen, D. D. (2014). Detection of fraudulent emails by employing advanced feature abundance. Egyptian Informatics Journal, 15(3), 169-174.

[16] Dua, D. and Karra Taniskidou, E. (2016). UCI Machine Learning Repository [http://archive.ics.uci.edu/ml]. Irvine, CA: University of California, School of Information and Computer Science.

[17] M. Amaad Ul Haq Tahir, Sohail Asghar, Ayesha Zafar and Saira Gillani (2016). A Hybrid Model to Detect Phishing-Sites using Supervised Learning Algorithms. 2016 International Conference on Computational Science and Computational Intelligence. DOI 10.1109/CSCI.2016.213.