Journal of Theoretical and Applied Information Technology
31st August 2020. Vol.98. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EFFICIENT PREDICTION OF PHISHING WEBSITES USING MULTILAYER PERCEPTRON (MLP)

AMMAR ODEH [1], ABDALRAOUF ALARBI [2], ISMAIL KESHTA [3], EMAN ABDELFATTAH [4]

[1] Princess Sumaya University for Technology P.O.Box 1438 Al-Jubaiha - Amman, 11941 Jordan

[2]Department of Computer Engineering, Karabuk University,78050, Karabuk, Turkey.

[3]College of Applied Sciences, AlMaarefa University Riyadh, Kingdom of Saudi Arabia

[4]School of Theoretical & Applied Science, Ramapo College of New Jersey, NJ , USA

[1]a.odeh@psut.edu.jo, [2] abdalraoufa.m.alarbi@ogrenci.karabuk.edu.tr, [3]imohamed@mcst.edu.sa, [4]eabdelfa@ramapo.edu

ABSTRACT

Maximizing user protection from Phishing website is a primary objective in the design of these networks. Intelligent phishing detection management models can assist designers to achieve this objective. Our proposed model aims to reduce the computational time and increase the security against the phishing websites by applying the intelligent detection model. In this paper, we employed Multilayer Perceptron (MLP) to achieve the highest accuracy and optimal training ratio to maximize internet security. The simulation results show the selection of the most significant features minimize the computational time. The optimal training percentage is 70% as it minimizes the time complexity and it increases the model accuracy.

Keywords: *MLP, Activation function, semantic attack, Phishing*

1. INTRODUCTION

Cyber-Attacks are classified into two classes: Syntactic attacks and Semantic attacks. Syntactic attacks which are considered as malicious programs that harm computer networks or computer software by attacking through worms, viruses, spyware or adware [1]. In Semantic attacks, the attackers use a computer system to fool the victim users, the semantic attacks pretend to do something but they are doing something else, yet the computing system works exactly as it is intended [2, 3].

The semantic attacks circumvent technological protections by deliberately exploiting system attributes, such as system or machine applications, to trick the victim instead of targeting him/her directly [4]. Table 1 shows families of different semantic attacks such as Phishing, File Masquerading, Application Masquerading, Web Pop-Up, Advertisement, Social Networking, Removable Media, and Wireless [5].

Phishing is a kind of intrusion that acquires sensitive users' information such as usernames, passwords, and other confidential information. Phishers use a variety of forms to fool users in different ways, for example, email, fake link, or phone call [6].

Phishing is an attack by an individual or a group that uses social engineering strategies to solicit personally identifiable information from unsuspecting customers. Phishing emails are built to look as if they were sent from a lawful institution or a familiar person. Often these emails try to attract subscribers to click a link which will take the customer to a fraudulent site that seems credible [7].

PhishLabs report identified phishing sites in 2019 which target 1,263 different brands belonging to 773 parent organizations. The top five targeted industries (Figure 1) comprised 83.9 percent of the total amount of phishing. United States organizations remained the most popular target for phishing scams in 2019, ranking for 84 percent of the total malware amount [8, 9].

Contemporary browsers like Firefox typically use black-list lists, i.e., a comprehensive list of fake URLs to counter phishing attacks [10, 11]. Therefore, when a Link is submitted via the browser, the system scans the list for the URL and blocks the website if the entry exists. These approaches could be ineffective solutions, as the phishers may use false addresses to pass by through some filters. Studies show steady growth in both phishing activities and the associated costs [12, 13].

Cyber-attacks cost companies more than $5 million between 2013 to 2017 [14].

Phishing attacks are classified into four main categories as shown in Figure 2. Credential harvesting where the attacker sends a trusted link to spoofed login pages. In extortion, the attacker asks victims for money exchange as a donation. Malware is a kind of hidden downloadable file as soon as the victim press in link. Spear-phishing where attacker targets high-level employees to enforce them to fill some tasks manually [15, 16].

2. LITERATURE REVIEW

Different researchers have conducted a lot of work in website security, some of them manipulated the routing security [17, 18], and other researchers work with intrusion detection, intrusion prevention, and smart grids security [19].

Pawan Parakash proposed two methods to identify phishing website. The first proposed method introduced the five heuristics to enumerate the combination if they are known phishing websites to find out the new phishing websites. The second method used the matching algorithms to find out the new phishing websites [20].

Samuel Marchal analyzed the URL of the websites and extracted the features of the URL. Based on the several queries through Google and Yahoo search engines, the authors determined the keywords for each website. Then, the keywords with extracted features used in machine learning classification algorithm to find out the phishing websites from the real dataset [21]. In [22], authors introduced models using machine learning and data mining algorithms to detect websites' phishing.

The authors in [23] used the artificial neural network to spot phishing websites. The proposed work used 17 neurons as input that match 17 characteristics in the dataset and one hidden layer level and two neurons as output to decide whether or not the website is phishing. The dataset was divided as 80 percent for training set and 20 percent for testing set. The model achieved 92.48 percent accuracy.

Authors in [24] introduced a model relying on machine learning techniques called PLIFER. This model requires an age of the URL domain (?). In addition, ten features are extracted and a Random Forests (RFs) model is used to identify the phishing website. 96% of phishing emails were correctly identified by this model. Classification models are also used to identify phishing utilizing labeled datasets. Different classification methods use features, like URL-based and text-based applications.

Proposed software collection model hybrid set of features (HEFS) to identify phishing websites relying on machine learning algorithms. A cumulative distribution gradient technique is used to extract the primary feature set. Then, the second set of features is extracted using a method called data perturbation ensemble. A Random Forests (RFs) model, an ensemble learner, is subsequently implemented to identify phishing websites. The results indicate that HEFS identified phishing features with a precision of up to 94.6 percent [25].

2.1 Preliminaries

This section provides a brief description of the phishing dataset for the experimental comparison, as well as background about the search algorithm, heat map, and a multilayer perceptron (MLP) algorithm used in this study.

2.2 Dataset

The dataset used are collected from PhishTank archive [26], MillerSmiles archive [27] and Google searching operators. The website phishing dataset consists of 30 features. These features were classified into four categories: Address Bar features, abnormal features, HTML and JavaScript features, and Domain features.

2.3 Search algorithm (CfsSubsetEval)

Correlation-based Feature Subset Selection for machine learning evaluates the importance of a subset of attributes by calculating the individual predictive capabilities of each function along with the degree of consistency among them. The heat map is a Visual presentation of values where the features found in the graph are described as colors [28].

2.4 A Multilayer Perceptron (MLP)

A MLP is a feeding forward artificial neural network (ANN). A MLP consists of a large number of extremely connected neurons running concurrently to achieve certain tasks. Mainly a MLP contains input and output layers, and some hidden (intermediate) layer(s). Each node contains an activation function (sigmoid, RBF). The core mechanism of the MLP network consists of signals flowing chronologically through multiple layers from the input to the output layer [29].

The training phase at MLP consists of three steps, the first step is input pattern X of the dataset then the output is generated and compared with the desired output. The second step is back propagated

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

based on the error signal between the network's output and the desired output. The last step is synaptic weights. This process is repeated for the next input vector until all instances in the training set are processed [30].

3. THE PROPOSED SYSTEM

In this work, an intelligent neural network model for efficient phishing website detection on the Internet is presented with the use of the classification algorithm. In this study, a web phishing dataset is used to evaluate the performance of the intelligent algorithm in terms of classification accuracy.

Figure 3 shows the block diagram of the proposed system. In the first step, the data are read and the needed features and their categories are recognized. Then, the dataset is cleaned and prepared in the proper format to read the file in MATLAB and Python.

The second step is processing which consists of three functions to be performed on the Phishing website dataset. The first function is Rank () to sort the feature from the most significant to the least significant according to their correlation to the class attribute. Based on the ranking function, the significance of each feature is calculated. Then, these features are sorted in descending order. For the ranking purpose, the MATLAB built-in procedure called independent significance features test (IndFeat()) is used [31, 32]. Then, the attribute evaluator Correlation-based Feature Selection (CfsSubsetEval()) [33] based on specific searching method is applied. Then, the intersection is performed between the output features from IndFeat() and CfsSubsetEval() to utilize the best features to determine if the URL is phishing or not.

In step 4, a MLP classifier is applied on the selected N features, based on the training dataset the machine learning model builds the optimal knowledge base. The intelligent model learns the correlation between the N features and the expected output. After that, the testing dataset will pass through the intelligent system. Then, the intelligent model is evaluated by measuring different performance metrics such as classification accuracy and computational speed.

4. EXPERIMENTAL WORK

The proposed model is set up based on the following experimental parameters as shown in Table 2.

Table 2 lists the values of the important parameters such as learning rate, number of epochs (number of passes through all instances in the dataset), and number of hidden layers, Batch size, and momentum.

This experiment was conducted on the Phishing Websites dataset; the dataset contains 30 attributes (one of them is a label). MATLAB is used to apply ranking for features from the most significant to least significant, and Python is used to draw the heat map as shown in Figure 4. Also, WEKA simulator v3.6 is used in the MLP classification process.

5. DISCUSSION OF RESULTS

To evaluate the performance of the intelligent classification algorithm MLP, the confusion matrix is used [34, 35]. The confusion matrix gives a visualization of how the classifier has performed on the input dataset. Different performance metrics, such as recall, precision, accuracy, and F-measure, can be derived from this matrix. The confusion matrix consists of four possible outcomes as shown in Table 3, which are false positive (FP), true positive (TP), false negative (FN), and true negative (TN) [36].

False Positives (FP) occur when the actual class of the test sample is negative and is wrongly marked as positive. True Negatives (TN) occur when the actual class of the test sample is negative and is marked correctly as negative. False Negatives (FN) occur when the actual class of the test sample is positive and is wrongly marked as negative. True Positives (TP) occur when the actual class of the test sample is positive and is marked correctly as positive.

Figure 6 demonstrates the output of the experiments in different training ratio

(50%, 60%, 70%, and 80%). Based on the output of the confusion matrix, the accuracy and F-Measure are calculated.

Precision = TruePositives / (TruePositives + FalsePositives) (1)

Recall = TruePositives / (TruePositives + FalseNegatives) (2)

Accuracy = TP+TN/TP+FP+FN+TN (3)

6. CONCLUSION

This paper presents an intelligent model for detecting phishing websites on the Internet. It provides a comparative study among four training percentages by using MLP classifiers. The main contribution of the proposed system is to build a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

real-time intelligent classifier. In addition, the proposed intelligent system reduces the computational time by applying features selection in the processing phase. The aim is to determine the most appropriate percentage of the training set using the MLP classification model for detecting phishing websites. It is observed that as the training percentage increases, the training time and computational complexity increases as well.

For future work, we intend to evaluate the performance of other machine learning classifiers and compare them to find the best one that improves the URL security.

REFERENCES:

[1] Vysakh S Mohan, R Vinayakumar, KP Soman, and Prabaharan Poornachandran, "SPOOF net: syntactic patterns for identification of ominous online factors," in 2018 IEEE Security and Privacy Workshops (SPW), 2018, pp. 258-263.

[2] Mohsen Rakhshandehroo and Mohammad Rajabdorri, "Time Series Analysis of Electricity Price and Demand to Find Cyber-attacks using Stationary Analysis," arXiv preprint arXiv:1907.11651, 2019.

[3] BB Gupta and Pooja Chaudhary, "Cross-Site Scripting Attacks: Classification, Attack, and Countermeasures," 2020.

[4] Yan Hu, Yuyan Sun, Youcheng Wang, and Zhiliang Wang, "An Enhanced Multi-Stage Semantic Attack Against Industrial Control Systems," IEEE Access, vol. 7, pp. 156871-156882, 2019.

[5] Matthijs Vos, "Characterizing infrastructure of DDoS attacks based on DDoSDB fingerprints," University of Twente, 2019.

[6] Surbhi Gupta, Abhishek Singhal, and Akanksha Kapoor, "A literature survey on social engineering attacks: Phishing attack," in 2016 international conference on computing, communication and automation (ICCCA), 2016, pp. 537-540.

[7] Brij B Gupta, Nalin AG Arachchilage, and Kostas E Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," Telecommunication Systems, vol. 67, pp. 247-267, 2018.

[8] Michael Fiermonte, "The Threat of Social Engineering to Networked Systems," Utica College, 2019.

[9] CISM Max Alexander and CISSP CRISC, "Protect, Detect and Correct Methodology to Mitigate Incidents: Insider Threats," 2018.

[10] Peng Peng, Limin Yang, Linhai Song, and Gang Wang, "Opening the blackbox of virustotal: Analyzing online phishing scan engines," in Proceedings of the Internet Measurement Conference, 2019, pp. 478-485.

[11] Routhu Srinivasa Rao and Alwyn Roshan Pais, "Detection of phishing websites using an efficient feature-based machine learning framework," Neural Computing and Applications, vol. 31, pp. 3851-3873, 2019.

[12] Silas Formunyuy Verkijika, "“If you know what to do, will you take action to avoid mobile phishing attacks”: Self-efficacy, anticipated regret, and gender," Computers in Human Behavior, vol. 101, pp. 286-296, 2019.

[13] Liaqat Ali, "Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC)," The Journal of Developing Areas, vol. 53, 2019.

[14] Sachin Kumar, "Cyber attacks & Its Security Predictions in 2020," CYBERNOMICS, vol. 1, pp. 39-43, 2019.

[15] Jason Thomas, "Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks," Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management, vol. 12, pp. 1-23, 2018.

[16] Meir Jonathan Dahan, Lior Drihem, Amnon Perlmutter, and TAM Ofir, "System and method to detect and prevent phishing attacks," ed: Google Patents, 2017.

[17] Abdul Basit and Naveed Ahmed, "Path diversity for inter-domain routing security," in 2017 14th international Bhurban conference on applied sciences and technology (IBCAST), 2017, pp. 384-391.

[18] Yehuda Binder, "System and method for routing-based internet security," ed: Google Patents, 2015.

[19] Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, and Raja Masood Larik, "Smart grids security challenges: Classification by sources of threats," Journal of Electrical Systems and Information Technology, vol. 5, pp. 468-483, 2018.

[20] Pawan Prakash, Manish Kumar, Ramana Rao Kompella, and Minaxi Gupta, "Phishnet: predictive blacklisting to detect phishing attacks," in 2010 Proceedings IEEE INFOCOM, 2010, pp. 1-5.

[21] Samuel Marchal, Jérôme François, Radu State, and Thomas Engel, "Phishstorm: Detecting phishing with streaming analytics," IEEE Transactions on Network and Service Management, vol. 11, pp. 458-471, 2014.

[22] Neda Abdelhamid, Aladdin Ayesh, and Fadi Thabtah, "Phishing detection based associative classification data mining," Expert Systems with Applications, vol. 41, pp. 5948-5959, 2014.

[23] Rami M Mohammad, Fadi Thabtah, and Lee McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, pp. 443-458, 2014.

[24] Solomon Ogbomon Uwagbole, William J Buchanan, and Lu Fan, "Applied machine learning predictive analytics to SQL injection attack detection and prevention," in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 1087-1090.

[25] Kang Leng Chiew, Choon Lin Tan, KokSheik Wong, Kelvin SC Yong, and Wei King Tiong, "A new hybrid ensemble feature selection framework for machine learning-based phishing detection system," Information Sciences, vol. 484, pp. 153-166, 2019.

[26] P PhishTank, "Join the fight against phishing," ed, 2016.

[27] Ravi Kiran Varma Penmatsa and Padmaprabha Kakarlapudi, "Web phishing detection: feature selection using rough sets and ant colony optimisation," International Journal of Intelligent Systems Design and Computing, vol. 2, pp. 102-113, 2018.

[28] K Selvakuberan, M Indradevi, and R Rajaram, "Combined Feature Selection and classification–A novel approach for the categorization of web pages," Journal of Information and Computing Science, vol. 3, pp. 083-089, 2008.

[29] Ali Asghar Heidari, Hossam Faris, Seyedali Mirjalili, Ibrahim Aljarah, and Majdi Mafarja, "Ant lion optimizer: theory, literature review, and application in multi-layer perceptron neural networks," in Nature-Inspired Optimizers, ed: Springer, 2020, pp. 23-46.

[30] Sankhadeep Chatterjee, Sarbartha Sarkar, Sirshendu Hore, Nilanjan Dey, Amira S Ashour, and Valentina E Balas, "Particle swarm optimization trained neural network for structural failure prediction of multistoried RC buildings," Neural Computing and Applications, vol. 28, pp. 2005-2016, 2017.

[31] MATLAB and Statistics Toolbox Release 2012b MathWorks, MathWorks, Natick, Mass, USA, 2012.

[32] Predictive Data Mining: A Practical Guide S. H. Weiss and N. Indurkhya, Morgan Kaufmann Publishers, San Francisco, Calif, USA, 1998.

[33] http://www.cs.waikato.ac.nz/ml/weka/. (2020).

[34] Alem Abdelkader, Dahmani Youcef, and Allel Hadjali, "On the use of belief functions to improve high performance intrusion detection system," in 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2016, pp. 266-270.

[35] Wahiba Ben Abdessalem Karaa, Amira S Ashour, Dhekra Ben Sassi, Payel Roy, Noreen Kausar, and Nilanjan Dey, "Medline text mining: an enhancement genetic algorithm based approach for document clustering," in Applications of Intelligent Optimization in Biology and Medicine, ed: Springer, 2016, pp. 267-287.

[36] Paulo Cavalin and Luiz Oliveira, "Confusion Matrix-Based Building of Hierarchical Classification," in Iberoamerican Congress on Pattern Recognition, 2018, pp. 271-278.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1. Families of Semantic Attacks

Semantic Attack	Tools
Brute-Force Attack	an end-all method to crack a difficult password
Dictionary Attack	the attacker uses a dictionary in an attempt to guess the password
Denial-Of-Service Attack	The attack focuses on the interruption of a network service.
Backdoor	Any secret method of bypassing normal authentication or security controls.
Eavesdropping	listening to a private conversation
Spoofing	falsifying data
Privilege Escalation	an attacker able to fool the system into giving them access to restricted data
Phishing	The attacker uses Email, Website, URL to crack usernames, passwords and credit card details directly from users
Clickjacking	the attacker tricks a user into clicking on a button
File Masquerading	The attacker uses the name of the file is maliciously called anything close to one that could be trusted

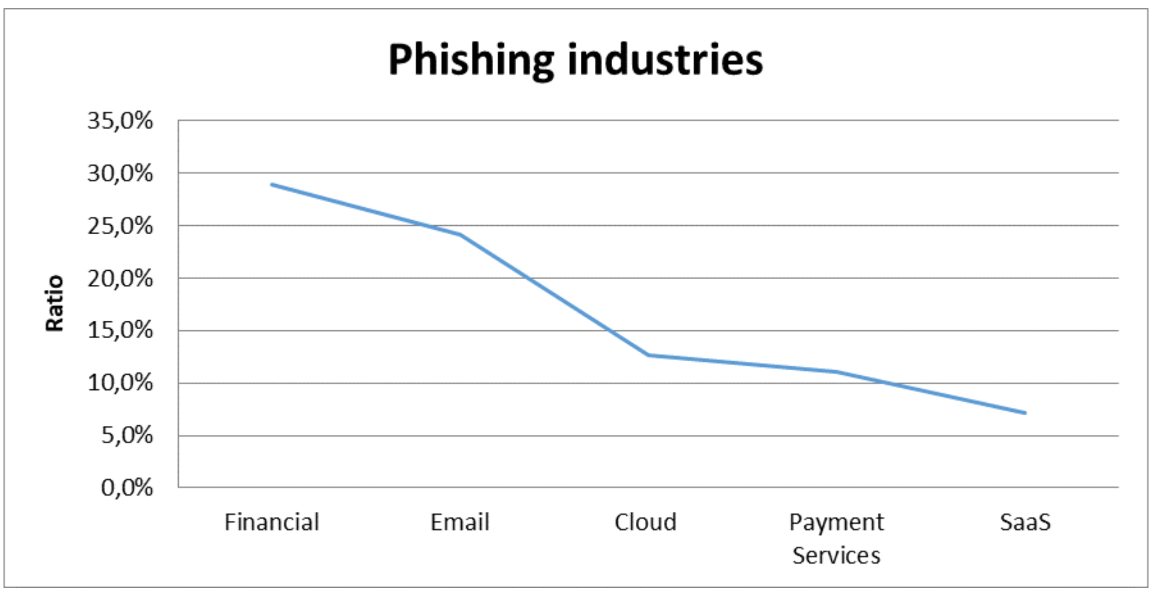

Figure 1. Top five targeted industries

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

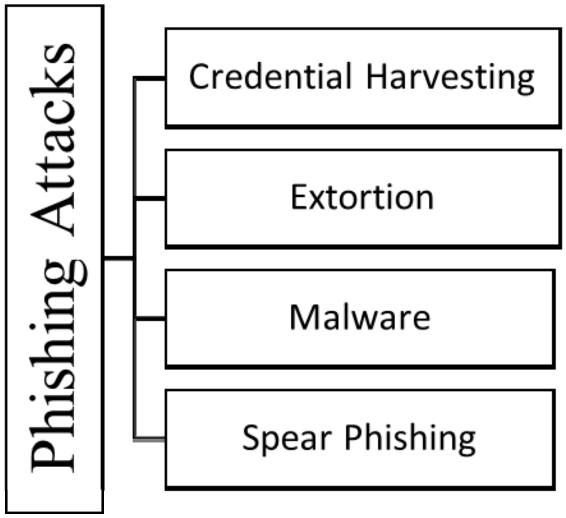

Figure 2. Phishing Attacks categories

.

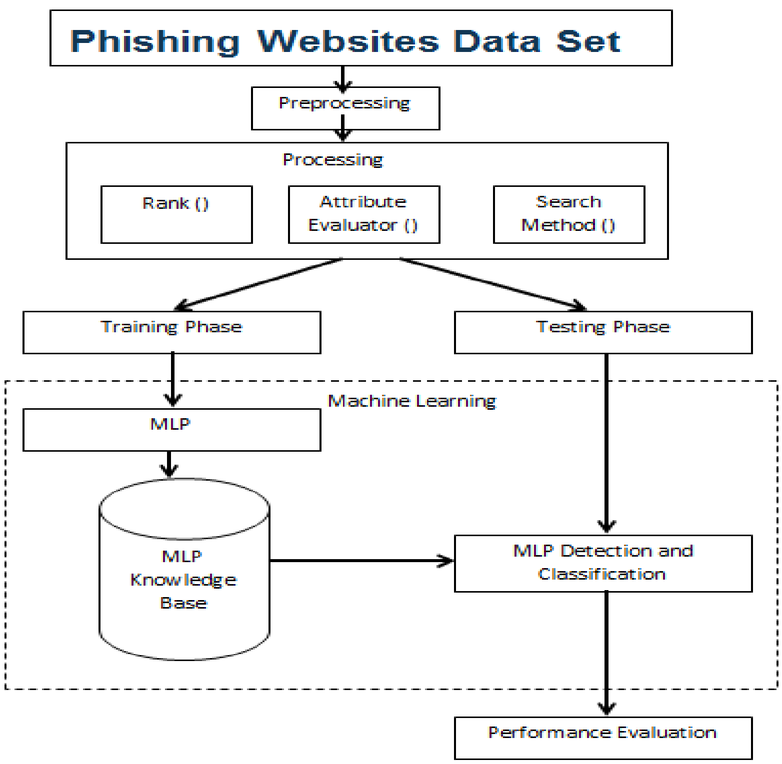

Figure 3. Block diagram of the proposed system.

Journal of Theoretical and Applied Information Technology
31st August 2020. Vol.98. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The scheme operates in five stages, which are as follows:

1. Read the dataset.
2. Preprocessing
3. Processing
   a) Select attribute [Calculate significance level of feature, Sort in descending order.]
      i. Rank
      ii. Attribute evaluator
      iii. Search method
4. Machine learning.
5. Performance evaluation.

Table 2. Experimental parameters.

Parameter	Value
Learning rate for MLP	0.3
Number of epochs for MLP	500
Number of hidden layers for MLP	1
Number of hidden neurons for MLP	1
Batch Size	100
Momentum	0.2

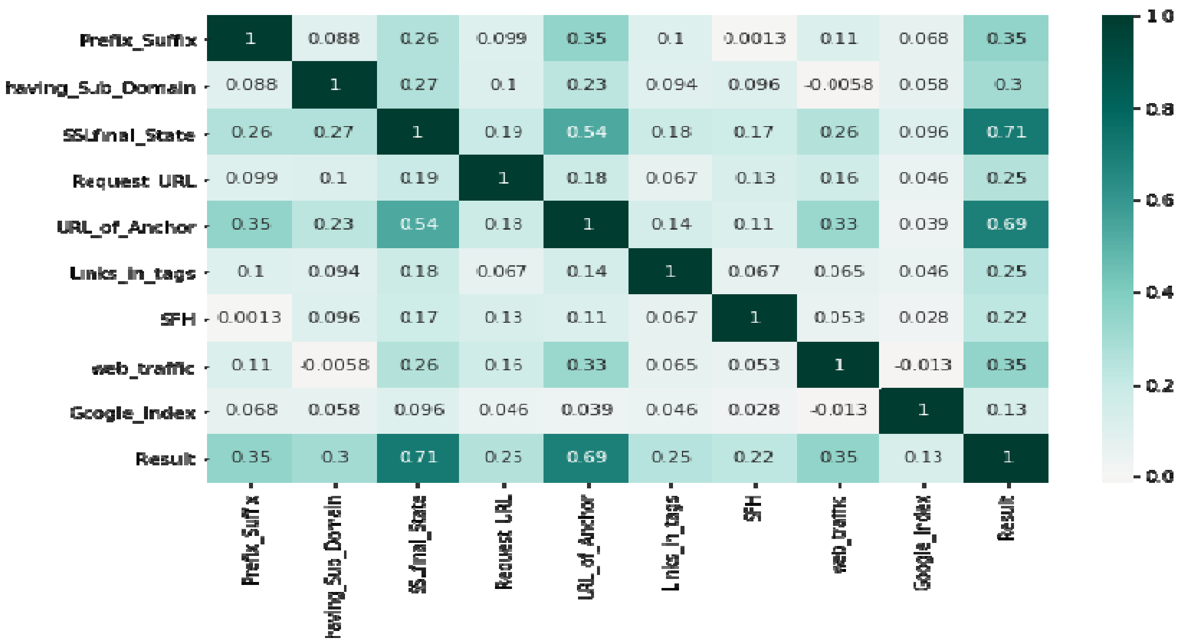

Figure 4. Heat map for features correlation

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

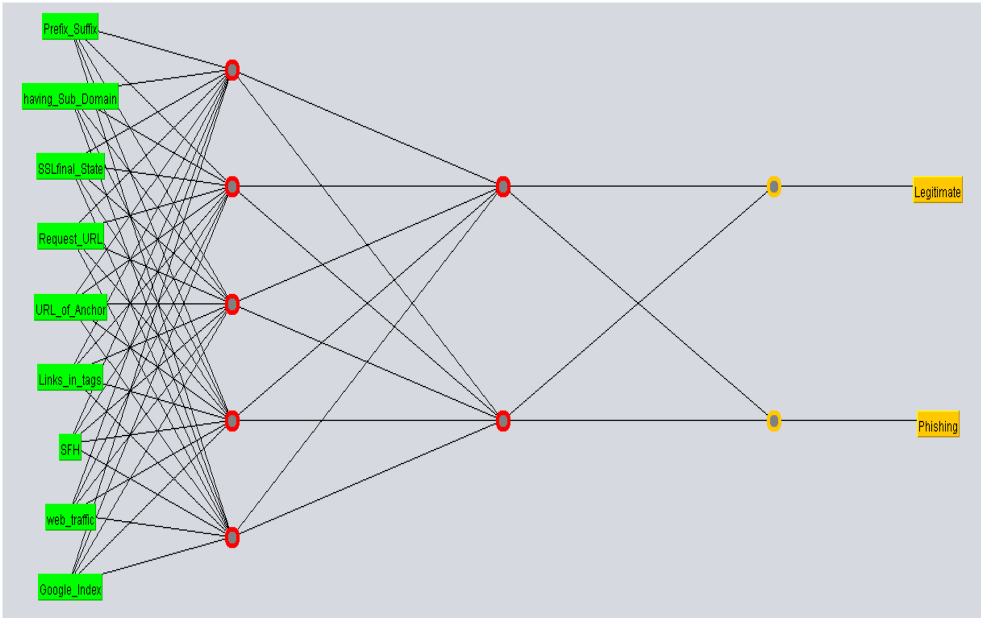

Figure 5. Structure of MLP

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 3. Confusion matrix.

		Predicted class	
		Positive	Negative
Actual class	Positive	TP	FP
	Negative	FN	TN

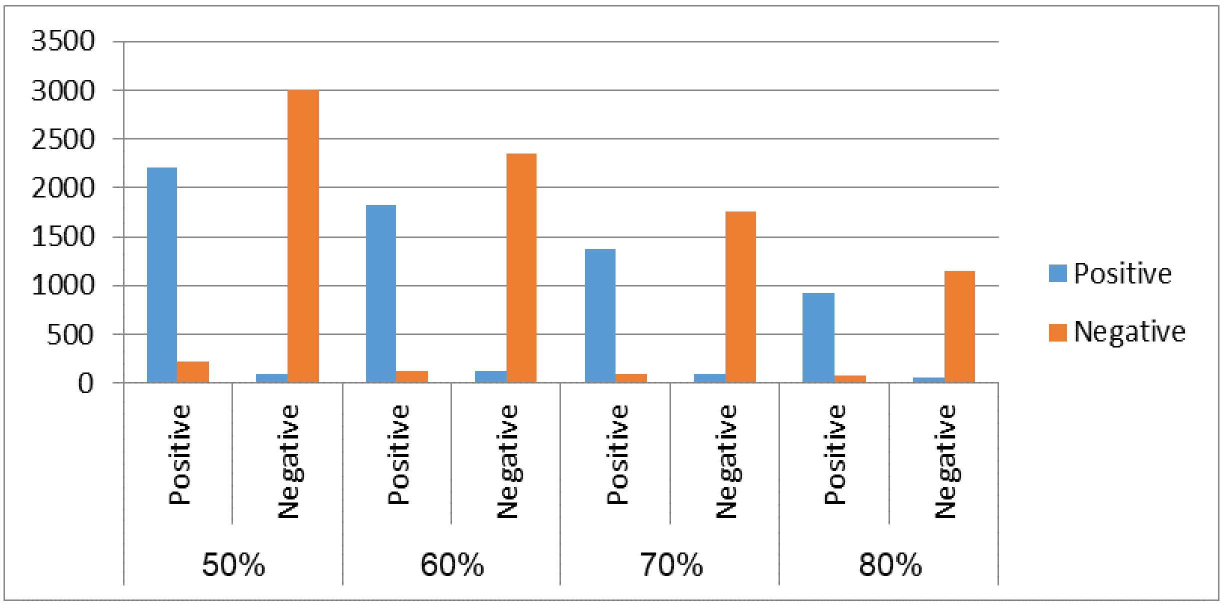

Figure 6. The output of Confusion matrix in different training Ratios

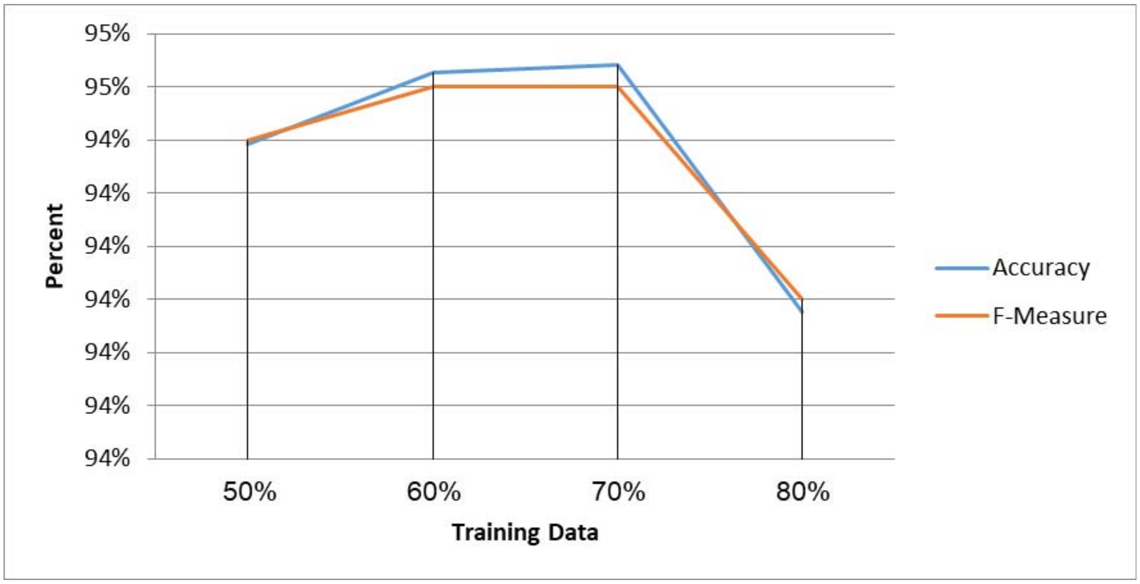

Figure 7. Percentages of the training data versus the accuracies and F-measures

Table 4. Comparison with other algorithms using 70 % training dataset

Paper	Machine Learning Algorithm	Accuracy
[18]	NN	94.07%
[19]	multi-label rule-based	94.8%
[20]	NN	84%
[21]	FFNN	87%
[22]	feed forward NN	97.40%
[23]	logistic regression classifier	98.40%
[24]	Naïve Bayesian classifier	90%
[25]	HNB and J48	96.25%
Proposed Model		99.1