


Detection of Phishing in Internet of Things Using Machine Learning Approach

Sameena Naaz, Jamia Hamdard, India

 <https://orcid.org/0000-0003-0080-5063>

ABSTRACT

Phishing attacks are growing in the similar manner as e-commerce industries are growing. Prediction and prevention of phishing attacks is a very critical step towards safeguarding online transactions. Data mining tools can be applied in this regard as the technique is very easy and can mine millions of information within seconds and deliver accurate results. With the help of machine learning algorithms like random forest, decision tree, neural network, and linear model, we can classify data into phishing, suspicious, and legitimate. The devices that are connected over the internet, known as internet of things (IoT), are also at very high risk of phishing attack. In this work, machine learning algorithms random forest classifier, support vector machine, and logistic regression have been applied on IoT dataset for detection of phishing attacks, and then the results have been compared with previous work carried out on the same dataset as well as on a different dataset. The results of these algorithms have then been compared in terms of accuracy, error rate, precision, and recall.

KEYWORDS

Decision Tree, Internet of Things, Linear Model, Logistic Regression, Neural Network, Phishing, Random Forest Classifier, Support Vector Machine

1. INTRODUCTION

Phishing attacks are growing constantly as the online transactions and digital media is growing. According to Anti Phishing Working Group (APWG) the main target of phishing are the payment system (45%), followed by the financial institutions (16%), webmail (15%) and Cloud Storage (9%). (APWG, 2010). Phishing in the IoT environment has huge impact on the organizations, individuals as well as government. According to Gartner organizations have suffered losses in millions due to phishing attacks on various devices hosting and using their applications. Apart from the financial losses these enterprises lose their credibility and brand image as well. In many cases they also have to reimburse the losses to the customer to maintain their loyalty. From the customer's perspective who were actually attacked, it will be very difficult for them to rely on these IoT devices again. They will avoid doing online transactions and this will impact the e-commerce growth in a big way (Srivastava T, 2007). Many phishing attacks have been reported recently mostly in the banking domain where the money has been siphoned either through online transactions or from the ATM ("Major Cyber Attacks," 2018). This is an example of government or a private entity falling prey to this attack.

DOI: 10.4018/IJDCF.2021030101

This article, published as an Open Access article on February 15, 2021 in the gold Open Access journal, The International Journal of Digital Crime and Forensics (IJDCF) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Another example is the access to the Aadhaar database due to the flaws in the mAadhaar app on the Google Play Store (“Aadhaar security breaches,” 2018).

A huge amount of progress in the communication technology has led to resource distribution among multiple users which in turn increases the problem of privacy, integrity, security and trust. A very attractive term called the Internet of Things has come up which makes the home automation and smart appliances very simple and exciting for us but we definitely need to strengthen the security of these IoT devices. One type of attack very common in these devices is the phishing attack in which the attacker tries to steal users personal information using different mechanisms.

A phishing attack was carried out in December 2016 in which more than 750,000 malicious emails were delivered to lakhs of gadgets including handheld and networking devices like routers etc, this report was published in egadget+. According to their report three fourth of these emails were sent by traditional computers and mobile devices, but IoT gadgets also contributed to more than one fourth of these attacks. The phishers usually carry out such attacks on SSH, telnet and SMTP (i.e. “email”) servers. These DDoS attacks if not stopped degrade the performance of these gadgets (Gorman, 2017). A mass phishing attack has been recorded on Russian business by cybersecurity experts which began in November 2018 and peaked in February 2019. In this attack the hackers posed as representatives of well-known brands and they used smart devices to send e-mails with malicious software. These emails contained encryption virus Shade/Troldesh which encoded the files on these devices and asked for money for their access. At least 50 big companies of Russia were affected due to this attack in which devices such as modem, network storage and smart home appliances were used.

Phishers are adopting different and newer techniques for phishing attacks thus making it easy for them to commit crime and difficult to spot them (Barraclough et. al, 2013). The tools which are used these days actually employ the basic rule of expert system i.e. creating particular rules in blacklist and then matching the incoming data traffic against those particular rules. One of the areas of digital forensics which monitors and inspects the network traffic for finding and interpreting the security strategy violations is called network forensics (Wang and Wang, 2010; Khan et al., 2016). Machine learning methods have been utilized to build Network forensic techniques, but two challenges which still need to be addressed are that these algorithms are generating high error rates and they are not able to determine the various ways in which attacks happen, particularly botnet events (Moustafa et al., 2017; Prakash and Krishna, 2016; Amini et al., 2015). Pattern recognition, classification, correlation statistical techniques and clustering are all included in Machine learning algorithms (Sangkatsanee et al, 2011; Amini et al., 2015).

In this paper three classification techniques, random forest, support vector machine and logistic regression are used to detect phishing in IoT devices. The rest of the paper is structured as follows. Section 2 contains the various types of phishing attacks in IoT. Section 3 and 4 gives the literature review and a description of various machine learning algorithms used in this work respectively. The methodology used in the proposed work is discussed in section 5. Experimental work and the results obtained are discussed in section 6. Section 7 gives the conclusion and future work.

2. PHISHING ATTACKS

2.1 Phishing

Being an active global network infrastructure the Internet of things (IoT) has self-configuring potential. It consists of physical as well as virtual things which have their own identities, physical properties and work on various communication protocols (Pawlick and Zhu, 2017). The Internet of Things has following features: firstly it's decentralized, and heterogeneous, and secondly it is connected to the real world. IoT is decentralized and it's nodes can configure themselves, they have local intelligence also. Since various “things” frequently go into and depart the IoT so it is heterogeneous in nature. Since these devices are connected to the real world, so they are a part of cyber-physical systems (CPS). For example an IOT device can control home lighting and can also influence behavior.

There are various ways in which phishing attacks are performed and based upon that these attacks can be classified as social engineering attacks and malware-based attacks. In social engineering-based phishing also known as deceptive phishing, the targets credentials are stolen either by sending fake emails or by using fake website (Jakobsson and Myers, 2007; Sheng et.al., 2007; Jakobsson SM, 2007). On the other hand in malware based phishing attack some malicious piece of code is somehow inserted on the victim's system.

2.2 Phishing Through Botnets

A network of systems which are purposely combined together for controlling and remotely distributing malware is called botnet. Criminals use these on large scale for many crimes like spam, phishing, stealing important information. Various devices are in danger of so called thingbots – a botnet that include autonomous linked items. Thingbots and Botnets both consist of multiple devices, which are connected to one another via smart phones, tablets, smart devices, computers and laptops. Example is the attack on Dyn in 2016 which was called Mirai botnet attack. This attack affected the domain name server of Reddit, Twitter, New York Times and Github (Meyer, 2016; Antonakakis et al, 2017). The bandwidth of the DNS was plagued due to the enormous flow of traffic.

2.3 Phishing Through Port Redirection

In this method the content is not uploaded directly, but the web requests sent to a server are redirected to some other remote web server by using port redirection services. The required information can then be stolen from the location to which the traffic was rerouted (Alliance R, 2005).

2.4 Social Engineering

Using social engineering the criminals can manipulate people so that they provide private information. Usually criminals try to trick the user in order to get bank and password information from the target. They also try to breach the computer password to install malicious software that can provide them access to personal information. This is typically done by redirecting the users to websites resembling shopping and banking sites that look valid, alluring the users to enter their details (Jagatic et al, 2007; Jagatic S, 2001; Gupta et al, 2017).

2.5 Malware-Based Phishing

Malware is a malicious piece of code installed on a system with an intent to access user's confidential data. Security gaps in the browser or the operating system aids the installation of these malwares. The most common type of malware is Trojan which constitutes 72% of all the malwares reported. Some ways in which malware infects victim's system are through key loggers and screen loggers, session hijacking, content injection and through search engines (Gruschka and Jensen, 2010; Mulazzani et al, 2011; Roberts and Al-Hamdani, 2011).

3. LITERATURE REVIEW

Some of the relevant work reported by authors in reputed journals are discussed here (Shrivastava et al, 2017) collected phishing data set from UCI repository and implemented the phishing data set on rapid miner tool and compared decision tree, random tree, random forest algorithms for classification of phishing and non-phishing. Accuracy obtained from decision tree was 91.8% which was the best as compared to other algorithms random tree 66.7%, random forest 78.8% and decision stump 84%. (Subasi et al, 2017) compared various algorithms like random forest, support vector machine, decision tree on WEKA open source tool. This work reported that Random Forest is quicker, robust and more accurate as compared to KNN, SVM Rotation forest and Decision Tree. Random forest yielded best results here based on accuracy 97.36%.

(Hodžić and Kevrić, 2016) compared the algorithms multilayer perceptron (MLP), decision tree, random forest, C4.5, rotation tree (REP tree) etc. All the experiments were conducted in WEKA tool and this work reported that Rotation tree achieved overall best accuracy of 89.1% compared to other algorithms.

In their paper (Kalaiselvan and Edwinraja, 2015) collected phishing dataset from the Phistank website and compared the algorithms C4.5, SVM, Naïve and ZeroR, to classify phishing dataset into phishing and legitimate. Here the accuracy of developed methods was assessed after applying the 10 fold cross-validation and Naïve Bayes algorithm was found to perform better than other algorithm. In their research paper Support Vector Machine, Gaussian and NMC classifiers have been employed by (Kaur and Sharma, 2015) along with fuzzy logic. Fuzzy based detection system provides effective aid in detecting phishing websites. It successfully resulted in low false positive and high true positive for classifying phishing websites. A methodology to detect phishing website based on machine learning classifiers is presented in (Ali, 2017) which uses a wrapper features selection method. Some common supervised machine learning techniques have been used by authors here to accurately detect phishing websites and they found that wrapper based algorithm performs better as compared to normal method.

In their work (Mohammad et al, 2014) proposed an Artificial Neural Network (particularly self-structuring neural networks) based intelligent model for predicting phishing attacks. The authors were able to atomise phishing website detection with frequent change in phishing websites using 17 different features. An Intelligent system to detect phishing in e-banking has been proposed by (Aburrous et al, 2010) where the authors combined fuzzy logic model with machine learning algorithms to detect phishing websites. They differentiated between different types of phishing websites using 10 fold cross validation and achieved 86.38% accuracy, which is very low.

(Chen et al, 2017) proposed a method for concocted spoof detection using different algorithms as Bayesian Network, C4.5, Logit Regression, Naïve Bayes, Neural Network and SVM (linear composite, linear, polynomial, RBF kernels). The authors achieved an accuracy of 92.56% among 900 legit concocted, and spoof e-commerce websites.

Security issues in Internet of Things have been discussed by (Hossain et al, 2015). They have mentioned that the IoT devices are very insecure due to which the data from them can be compromised very easily. Gadgets such as sensors, controllers, coordinators etc belong to the family of IoT gadgets and they do not support the traditional security methodologies. These gadgets differ from the traditional gadgets in terms of battery life, power consumption and network versatility.

Based upon the nature and type of IoT devices which are frequently scanned over the Internet (Pa et al, 2015) proposed an IoT specific Honeypot named IoT POT. In their solution the Honeypot appeared to be a genuine device. A number of attacks such as Keylogging, Distributed Denial of Service attack, Phishing, Identity Theft and Spamming can be launched by these Botnets (Amini et al, 2015).

(Roux et al, 2017) invented an intrusion detection system for IoT which considers remote transmission of information through probes. Information is collected based upon its strength and direction and anything originating from an unexpected direction, is considered to be illegitimate. Classification was done here using Neural Network. In their work (Lin et al, 2014) used Artificial Fish Swarm optimization algorithm to obtain the feature set, and then carried out classification by using Support Vector Machine. This method outperformed Genetic Algorithms for feature selection by a small amount but there was substantial improvement time-wise. Artificial Immune Systems was used by (Greensmith, 2015) for security of IoT where they combined multiple AIS to handle the heterogeneous nature of IoT.

4. MACHINE LEARNING TECHNIQUES

Machine learning algorithms Random Forest, Support vector machine and Logistic Regression are used in this work to detect phishing in IoT devices. These algorithms are explained below:

4.1 Random Forest

Random forest is a collection of large number of decision trees. Random forest can be used to solve classification as well as regression problem but mostly it is used for solving classification problem. A random forest classifier consists of a collection of tree-structured classifiers $\{h(\mathbf{x}, \Theta_k), k = 1, \dots\}$ where the $\{\Theta_k\}$ are identically distributed random vectors which are independent of each other. In this approach unit vote is casted by every tree for the best class at any input \mathbf{x}

For a collection of classifiers $h_1(\mathbf{x}), h_2(\mathbf{x}), \dots, h_k(\mathbf{x})$, and the training set taken randomly from random vector \mathbf{Y} , \mathbf{X} the margin function is calculated as $mg(\mathbf{X}, \mathbf{Y}) = av_k I(h_k(\mathbf{X}) = \mathbf{Y}) - \max_{j \neq \mathbf{Y}} av_k I(h_k(\mathbf{X}) = j)$ where $I(\cdot)$ is the indicator function.

Margin gives the measure of the variation of the average number of votes at \mathbf{X} , \mathbf{Y} for the correct class with that for any other class. Greater margin means there is more confidence in classification. The generalization error is expressed as

$$PE^* = P_{\mathbf{X}, \mathbf{Y}} (mg(\mathbf{X}, \mathbf{Y}) < 0)$$

where the subscripts \mathbf{X}, \mathbf{Y} indicate that the probability is over the \mathbf{X}, \mathbf{Y} space. In random forests, $h_k(\mathbf{X}) = h(\mathbf{X}, \Theta_k)$. For a large number of trees as the number of trees increases for all $\Theta_1, \dots, \Theta_k$ PE^* converges to $P_{\mathbf{X}, \mathbf{Y}} (P_{\Theta} (h(\mathbf{X}, \Theta) = \mathbf{Y}) - \max_{j \neq \mathbf{Y}} P(h(\mathbf{X}, \sim) = j) < 0)$. This is the reason why random forests do not over fit on addition of more trees but give a limiting value of the generalization error.

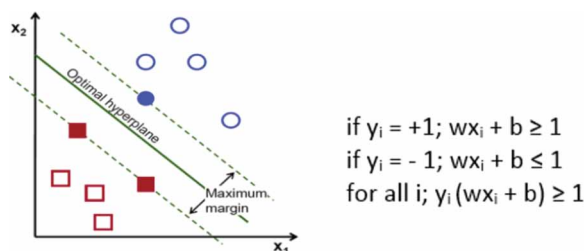
The diversity of trees is increased in RF by growing them from different training data subsets which are created through bagging or bootstrap aggregating (Breiman, L. 2001). In Bootstrap aggregating the original dataset is resampled in a random manner with replacement. Research has proven that methods which employ bagging are not sensitive to noise or overtraining in contrast to methods which are based on boosting (Briem et al., 2002; Chan and Paelinckx, 2008; Pal and Mather, 2003).

4.2 Support Vector Machine

Support Vector Machine is a supervised machine learning algorithms and one of the creating information classification system proposed by (Vapnik, 1995). SVM classifies by finding a hyperplane that divides the training dataset into distinct classes. If the dataset is two dimensional then the hyperplane is a line and the classifier is known as linear classifier. For mathematical calculations we have, Where \mathbf{x} is a vector point and \mathbf{w} is weight which is also a vector.

Several hyperplanes could exist for any dataset and the plane that maximizes the distance between two classes is known as maximum margin linear classifier. Maximum margin can be expressed as:

Figure 1. Classification using SVM



$$\text{margin} \equiv \arg \min_{\mathbf{x} \in D} d(\mathbf{x}) = \arg \min_{\mathbf{x} \in D} \frac{|\mathbf{x} \cdot \mathbf{w} + b|}{\sqrt{\sum_{i=1}^d w_i^2}}$$

4.3 Logistic Regression

Logistic Regression is a supervised learning technique that helps in performing categorization and arrangement process. Logistic Regression is an algorithms that is also used when dependent factors are binary, tertiary, ternary and quaternary (Bircan, 2004; Özdamar, 2002). The predictor variables in these cases could be categorical or numerical. But we do have multinomial logistic regression which can handle multiple outcomes for the response. For a binary response variable Y , $P(Y = 1)$ is dependent on \vec{x} , a vector of predictor values. The goal is to model

$$p(\vec{x}) \equiv P(Y = 1 | \vec{x})$$

Because the response variable Y is binary, so $p(\vec{x})$ can be modelled by modelling $E(Y | \vec{x})$.
If $p(\vec{x})$ is modelled as a linear function of predictor variables, e.g.:

$$\beta_0 + \beta_1 x_1 + \dots + \beta_p x_p$$

then there is a possibility that the fitted model gives estimated probabilities which are outside of $[0,1]$. So it is better to take:

$$p(\vec{x}) = \frac{\exp(\beta_0 + \beta_1 x_1 + \dots + \beta_p x_p)}{1 + \exp(\beta_0 + \beta_1 x_1 + \dots + \beta_p x_p)}$$

where x_1, \dots, x_p are the original explanatory variables.

Each of these algorithms have their own pros and cons and the results obtained depends upon the type of application and dataset. Although logistic regression is less predictive but is more interpretable or faster. So if the model is being used to take some decision then logistic regression is easier to explain. It is faster to train and execute for data with millions of sparse features and is also less prone to overfitting but it fails to perform when signal-to-noise is low. On the other hand random forest is versatile and works well on medium-sized dataset even in presence of noise. RF works well on categorical as well as real valued features with very little pre-processing. Support vector machines work better on linear dependencies and large feature space but can handle non-linear feature interactions also with the help of kernel.

5. METHODOLOGY

5.1 Data Collection

The dataset used in this work is UNSW-NB15 which was designed by the Australian Center of Cyber Security at UNSW Canberra (Moustafa et al, 2015) at their Cyber Range Lab. This dataset represents precise conventional traffic which may have been attacked by Botnets. IXIA PerfectStorm device was used to create this dataset which is a combination of original network traffic and attacked traffic. The dataset has 49 attributes, including the class feature and it contains 257,673 instances

(made by joining the training and testing datasets). The complete architecture of the proposed work is shown in Figure 2.

The dataset is divided into training and testing part and then both the training as well as testing dataset goes through the data pre-processing stage. Only quantitative features have been considered in this work, so the features having symbolic values such as state, protocol and services are dropped. After this stage the data goes through the feature extraction procedure for which Principal Component Analysis has been used in this work. PCA which is a linear feature extraction method requires less memory and is faster as compared to other methods. This method ranks the features based on the maximum variance for each feature and hence creates a new feature set of uncorrelated variables.

5.2 Performance Metrix

Confusion Matrix has been used to calculate different parameters such as accuracy, sensitivity or true positive rate (TPR), specificity or true negative rate (TNR), precision and f-measure and false alarm rate (Kahksha and Naaz, 2018; Kahksha and Naaz, 2019).

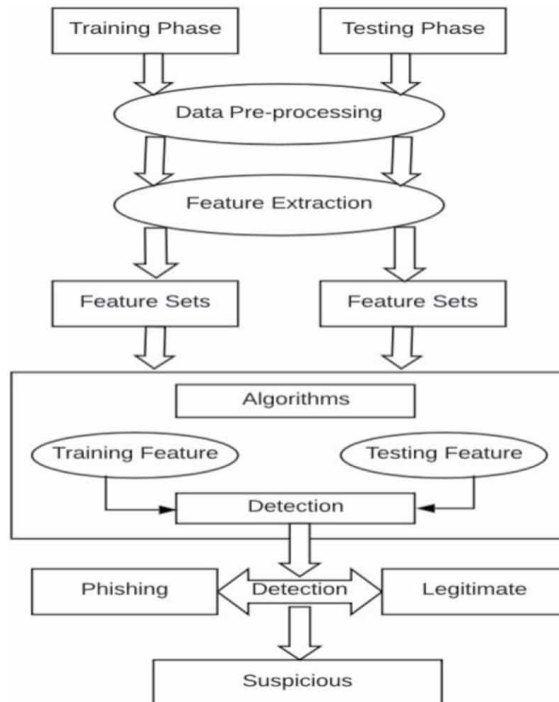
Accuracy is percentage of correct classification (true positive and negative) from overall numbers of instance:

$$\text{Accuracy (A)} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$$

Sensitivity is percentage of correct positive classifications (true positive) from instances that are actually positive:

$$\text{Sensitivity (S)/Recall/ TPR} = \text{TP} / (\text{TP} + \text{FN})$$

Figure 2. Architecture of the proposed work



Specificity is the percentage of positive records classified correctly out of all positive records:

$$\text{Specificity (SS)/ TNR} = \text{TN} / (\text{TN} + \text{FP})$$

Precision is the percentage of the correct positive classification (true positive) from instances that predicate as positive:

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP})$$

The F measure is defined as the weighted harmonic mean of the precision and recall of the test:

$$\text{F-Measure} = 2 \times \text{Precision} \times \text{Recall} / (\text{Precision} + \text{Recall})$$

False Alarm Rate /Error Rate is defined as the percentage of incorrect classification (false positive and negative) from overall numbers of instance. A false alarm rate is also known as the probability of false detection:

$$\text{False Alarm Rate (FAR)/Error Rate} = (\text{FP} + \text{FN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN})$$

$$\text{False positive rate} = \text{FP} / (\text{TN} + \text{FP}) = 1 - \text{TNR}$$

$$\text{False Negative Rate} = \text{FN} / (\text{TN} + \text{FN})$$

6. EXPERIMENTS AND RESULTS

The dataset used in this work is UNSW-NB15 which has been designed at the Australian Center of Cyber Security at UNSW Canberra in their Cyber Range Lab. The most popular technique N fold cross validation technique in machine learning has been used in this work with the value of N taken as 10. This basically means that the complete dataset was broken into 10 sets. Training takes place on 9 sets and testing is carried out on the remaining one set. This procedure is repeated 10 times and finally mean accuracy is calculated. This implementation has been done in Python. Random Forest, Support Vector Machine and Logistic Regression has been implemented on the above dataset and the results have been compared in terms of accuracy, true positive rate (TPR), true negative rate (TNR), Precision, F measure and false positive rate. These values have been calculated using formulas given in performance metrics and using confusion matrix on testing data set. The confusion matrices for the three classification methods are shown in Figure 3(a) to (c).

6.1. Results Obtained From Proposed Model

To provide a better overview of the performance of the proposed technique on the dataset, the overall accuracy, TPR, TNR, precision, F-measure and False alarm rate are presented in Table 1.

Figure 3. Confusion Matrix for the three algorithms

TP=1181	FP= 68
FN=19	TN=1496

TP=1185	FP= 64
FN=26	TN=1489

TP=1120	FP= 129
FN=84	TN=1431

Table 1. Performance of different Algorithms

	RF	SVM	LR
Accuracy	96.85%	96.74%	92.29%
TPR	98.41%	97.85%	93.02%
TNR	95.65%	95.87%	91.73%
Precision	94.55%	94.87%	89.67%
F-Measure	96.44%	96.33%	91.31%
False Alarm Rate	3.14%	3.25%	7.71%

False Alarm Rate/Error rate of different machine learning algorithms has been calculated using confusion matrix and random forest classifier has been found to have minimum error rate of 3.14%, support vector machine showed a slightly higher error rate of 3.25% whereas logistic regression has been found to perform worst with error rate of 7.71% as shown in Figure 4.

In Phishing classification, false positives (FP) is legitimate traffic which is misclassified as phishing and false negatives (FN) is phishing traffic which are misclassified as legitimate. These values are shown in Table 2

In the end all the above algorithms have been compared in terms of accuracy precision, recall, and F-measure.

As shown in Figure 5 the performance of Random Forest algorithm and Support Vector machine is almost similar in terms of all the parameters. Random forest achieved an accuracy of 96.85%, SVM is very close to it with an accuracy of 96.74% and the accuracy of logistic regression is 92.29%. The true positive rate for the three algorithms are 98.41% for RF, 97.85% for SVM and 93.02% for LR respectively. This means that 98.41% of legitimate traffic are misclassified as phishing by RF, 97.85% are misclassified as phishing by SVM and 93.02% are misclassified as phishing by LR. Random forest gives true negative rate of 95.65%, Precision of 94.55% and F-measure of 96.44%. This means that

Figure 4. Comparison of error rate

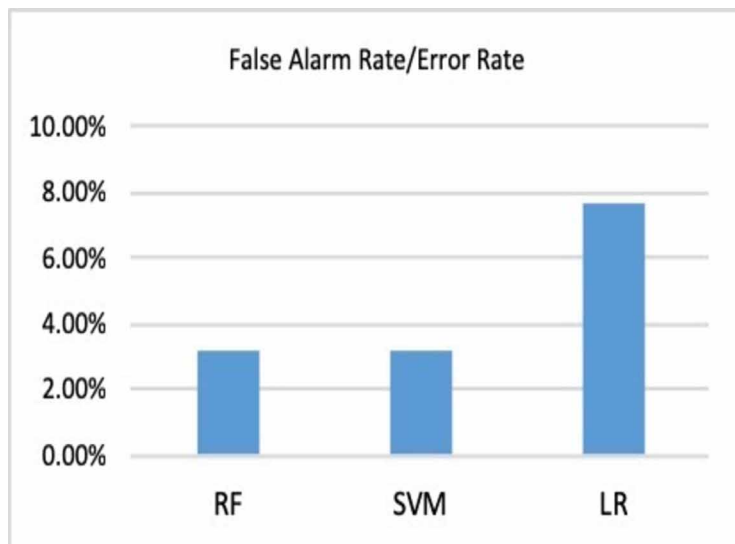
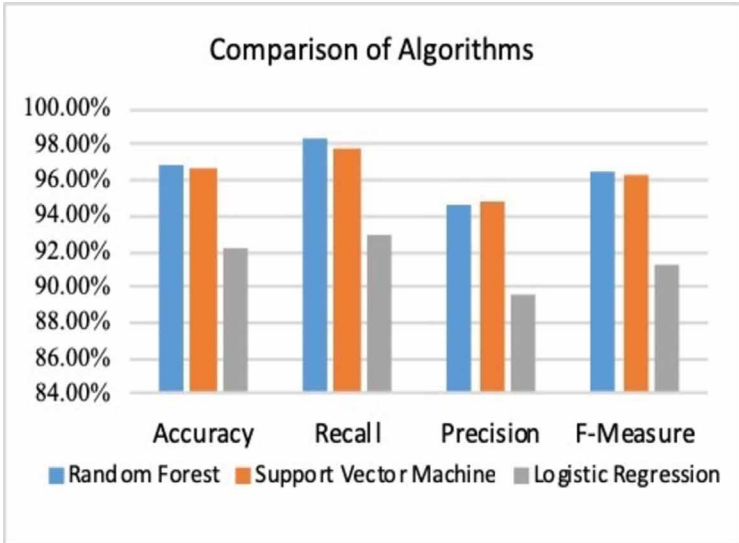


Table 2. False Positive rate (FPR) and False Negative rate (FNR)

	RF	SVM	LR
FPR	4.35%	4.13%	8.27%
FNR	1.25%	1.72%	5.54%

Figure 5. Comparison of algorithms



95.65% of phishing traffic are misclassified as legitimate 94.55% of positive identifications are actually correct. Similarly SVM yields a TNR of 95.87%, precision of 94.87% and F-measure of 96.33%.

To show the effectiveness of the proposed model, the results of existing approaches have been compared with the proposed model.

6.2 Comparison of Proposed Method With Similar Work on Different Dataset

A similar work on a dataset gathered from MillerSmiles archive, PhishTank archive and Google™s searching operators was carried out by (Kahksha and Naaz, 2019). The data set consisted of 2456 instances and 30 features. Value of attributes was in the form of integer -1, 0, and 1, -1 representing phishing, 0 denoted suspicious and 1 denoted legitimate In this work first the data set was processed to get mature data in the desired format and then it is divided into two sections as training 70% and testing 30%. The experiments were carried out using RStudio installed on windows 10.

In that work Decision tree, Random forest, Neural Network and Linear model was used and the results were obtained on the same parameters as in the proposed work. The results are given in Table 3.

Graphical representation for performance comparison based on accuracy and false alarm rate is depicted in Figure 6

6.3 Comparison of Proposed Method with Similar Work on Same Dataset

Table 4 compares the work described in this paper with the work in (Koroniotis, 2017) on the same dataset for different algorithms. As can be seen from the results all the algorithms in the current work performed better both in terms of Accuracy and False Alarm Rate except for Decision Tree for which

Table 3. Comparison of algorithms based on accuracy and false alarm rate

	RF	SVM	LR	DT	RF	NN	LM
Accuracy	96.85%	96.74%	92.29%	90.4%	95.7%	90.7%	92.1%
TPR	98.41%	97.85%	93.02%	93.2%	96.1%	84.0%	93.8%
TNR	95.65%	95.87%	91.73%	88.7%	95.2%	97.9%	90.0%
Precision	94.55%	94.87%	89.67%	83.2%	93.7%	94.0%	92.0%
F-Measure	96.44%	96.33%	91.31%	87.0%	94.0%	90.4%	92.8%
False Alarm Rate	3.14%	3.25%	7.71%	9.5%	4.3%	9.2%	8.0%

Figure 6. Comparison based on accuracy and false alarm rate

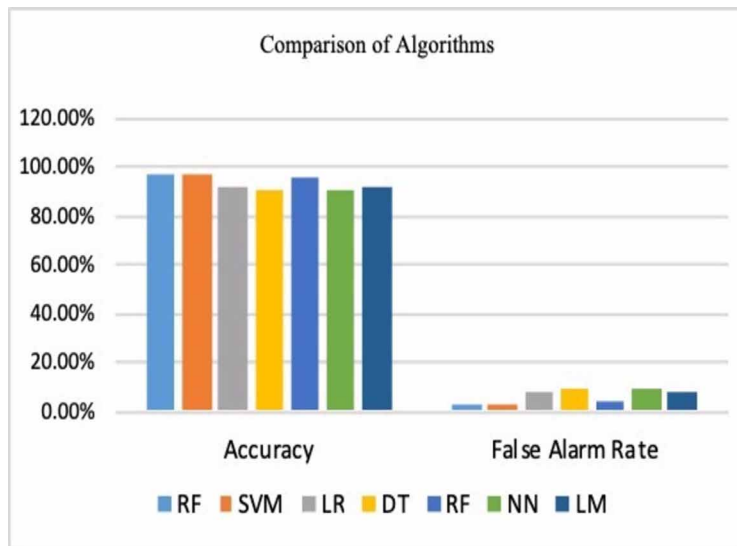
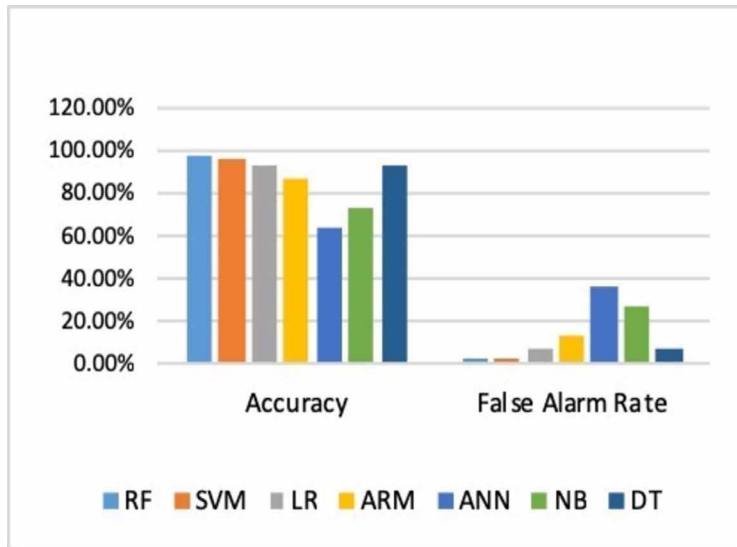


Table 4. Comparison of current work with existing work on the same dataset

	Accuracy	False Alarm Rate
Random Forest	96.85%	3.14%
Support Vector Machine	96.74%	3.25%
Logistic Regression	92.29%	7.71%
Association Rule Mining	86.45%	13.55%
Artificial Neural Network	63.97%	36.03%
Naïve Bayes	72.73%	27.27%
Decision Tree C4.5	93.23%	6.77%

Figure 7. Comparison of current work with existing work



the accuracy is slightly better than the accuracy shown by Logistic Regression. Random forest and SVM give much better performance than all the algorithms in (Koroniotis, 2017).

The same results are also depicted in Figure 7 in graphical form.

7. CONCLUSION AND FUTURE WORK

Phishing is growing continuously irrespective of intelligence and security development. There is definitely need of special care toward safeguarding of people being cheated. So the topic of phishing detection is very crucial and we have Cyber security professionals who are continuously working to make these devices more secure. Various approaches are available to detect phishing. This includes blacklisting, data mining and heuristics, soft computing and machine learning techniques. Research has shown that machine learning techniques give better accuracy as compared to the other approaches and they are also capable of handling zero-hour phishing attacks in a better manner as compared to other methods.

In this work different machine learning algorithms have been compared on phishing dataset and found that random forest works better in terms of accuracy, error rate and other parameters. The proposed algorithm has also been compared with existing similar work on same as well as different dataset. Results show that the proposed model outperforms the other work reported in literature both in terms of accuracy and false alarm rate.

In this work features that had non numeric values were simply dropped from the dataset. Some other method for feature selection can be used in the future to see if better results can be obtained. Similarly other approaches to feature extraction can also be implemented to see the effect. A combination or hybrid machine learning algorithm can also be implemented to improve accuracy and minimize false alarm rate.

REFERENCES

- Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected. (2018, September 25). Retrieved from <https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html>
- Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, 37(12), 7913–7921. doi:10.1016/j.eswa.2010.04.044
- Ali, W. (2017). Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection. *International Journal of Advanced Computer Science and Applications*, 8(9), 72–78. doi:10.14569/IJACSA.2017.080910
- Amini, P., Araghizadeh, M. A., & Azmi, R. (2015, September). A survey on botnet: classification, detection and defense. In *2015 International Electronics Symposium (IES)* (pp. 233–238). IEEE. doi:10.1109/ELECSYM.2015.7380847
- Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Kumar, D. (2017). Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 1093–1110). USENIX.
- Barraclough, P. A., Hossain, M. A., Tahir, M. A., Sexton, G., & Aslam, N. (2013). Intelligent phishing detection and protection scheme for online transactions. *Expert Systems with Applications*, 40(11), 4697–4706. doi:10.1016/j.eswa.2013.02.009
- Bircan, H. (2004). Logistic Regression Analysis: Practice in Medical Data. *Kocaeli University Social Sciences Institute Journal*, 2, 185–208.
- Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32. doi:10.1023/A:1010933404324
- Briem, G. J., Benediktsson, J. A., & Sveinsson, J. R. (2002). Multiple classifiers applied to multisource remote sensing data. *IEEE Transactions on Geoscience and Remote Sensing*, 40(10), 2291–2299. doi:10.1109/TGRS.2002.802476
- Chan, J. C. W., & Paelinckx, D. (2008). Evaluation of Random Forest and Adaboost tree-based ensemble classification and spectral band selection for ecotope mapping using airborne hyperspectral imagery. *Remote Sensing of Environment*, 112(6), 2999–3011. doi:10.1016/j.rse.2008.02.011
- Chen, H., Vasardani, M., & Winter, S. (2017). Geo-referencing Place from Everyday Natural Language Descriptions. arXiv preprint arXiv:1710.03346.
- Granger, S. (2001). *Social engineering fundamentals, part I: hacker tactics* (Vol. 2006). SecurityFocus.
- Greensmith, J. (2015, July). Securing the internet of things with responsive artificial immune systems. In *Proceedings of the 2015 Annual Conference on Genetic and Evolutionary Computation* (pp. 113–120). ACM. doi:10.1145/2739480.2754816
- Gruschka, N., & Jensen, M. (2010, July). Attack surfaces: A taxonomy for attacks on cloud services. In *2010 IEEE 3rd international conference on cloud computing* (pp. 276–279). IEEE. doi:10.1109/CLOUD.2010.23
- Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: State of the art and future challenges. *Neural Computing & Applications*, 28(12), 3629–3654. doi:10.1007/s00521-016-2275-y
- Hodžić, A., & Kevrić, J. (2016) Comparison of Machine Learning Techniques in Phishing Website Classification. *International Conference on Economic and Social Studies (ICESoS'16)*, 249–256.
- Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, June). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 IEEE World Congress on Services* (pp. 21–28). IEEE. doi:10.1109/SERVICES.2015.12
- Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. doi:10.1145/1290958.1290968

Jakobsson, M., & Myers, S. (2007). *Phishing & countermeasures: understanding the increasing problem of electronic identity theft*. Wiley.

Kahksha, , & Naaz, S. (2018). Machine Learning Algorithm to Predict Survivability in Breast Cancer Patients. *International Journal on Computer Science and Engineering*, 10(4), 97–101. doi:10.21817/ijcse/2018/v10i4/181004013

Kahksha & Naaz, S. (2019). Detection of Phishing Websites using Machine Learning Approach. *International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM 2019)*.

Kalaiselvan, O., & Edwinraja, S. (2015). Predicting Phishing Websites using Rule Based Techniques. *International Journal of Emerging Technology and Innovative Engineering*, 1(4), 180–185.

Kaur, S., & Sharma, S. (2015). Performing Efficient Phishing Webpage Detection. *International Journal on Computer Science and Engineering*, 3(7), 52–56.

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications*, 66, 214–235. doi:10.1016/j.jnca.2016.03.005

Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2017, December). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In *International Conference on Mobile Networks and Management* (pp. 30–44). Springer.

Lin, K. C., Chen, S. Y., & Hung, J. C. (2014). Botnet detection using support vector machines with artificial fish swarm algorithm. *Journal of Applied Mathematics*, 2014, 2014. doi:10.1155/2014/986428

Major Cyber Attacks on India. (2018, August 23) Retrieved from <https://www.testbytes.net/blog/cyber-attacks-on-india-2018/>

Markus Jakobsson, S.M. (2007). *Phishing and countermeasures, Microsoft's anti-phishing technologies and tactics*. Academic Press.

Meyer, R. (2016, Oct.). How a bunch of hacked dvr machines took down twitter and reddit. *The Atlantic*.

Gorman, M. [@Numeson] (2017, Jan. 14). The Internet of Things isn't safe: thousands of smart gadgets hacked to send spam and phishing emails. *egadget+*. Retrieved from <https://www.engadget.com/2014/01/17/internet-of-things-hacked-malicious-email-phishing/>

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Intelligent rule-based phishing websites classification. *IET Information Security*, 8(3), 153–160. doi:10.1049/iet-ifs.2013.0202

Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1–6). IEEE.

Moustafa, N., Slay, J., & Creech, G. (2017). Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks. *IEEE Transactions on Big Data*.

Mulazzani, M., Schrittwieser, S., Leithner, M., Huber, M., & Weippl, E. R. (2011, August). Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space. In *USENIX security symposium* (pp. 65–76). USENIX.

Özdamar, K. (1999). Statistical data analysis using package programs. *Multivariate Analyses*, 2.

Pa, Y. M. P., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2015). IoTPOT: analysing the rise of IoT compromises. In *9th {USENIX} Workshop on Offensive Technologies ({WOOT} 15)*. USENIX.

Pal, M., & Mather, P. M. (2003). An assessment of the effectiveness of decision tree methods for land cover classification. *Remote Sensing of Environment*, 86(4), 554–565. doi:10.1016/S0034-4257(03)00132-9

Pawlick, J., & Zhu, Q. (2017, October). Proactive defense against physical denial of service attacks using poisson signaling games. In *International Conference on Decision and Game Theory for Security* (pp. 336–356). Springer. doi:10.1007/978-3-319-68711-7_18

Phishing Activity trends report, Anti Phishing Working Group. (2010). (Report No. 2). Retrieved from http://docs.apwg.org/reports/apwg_report_h2_2010.pdf

- Prakash, P. B., & Krishna, E. P. (2016). Achieving High Accuracy in an Attack-Path Reconstruction in Marking on Demand Scheme. i-Manager's. *Journal of Information Technology*, 5(3), 24.
- Project, H., & Alliance, R. (2005). *Know your enemy: tracking botnets*. <http://www.honeynet.org/papers/bots/>
- Roberts, J. C. II, & Al-Hamdani, W. (2011, September). Who can you trust in the cloud? A review of security issues within cloud computing. In *Proceedings of the 2011 Information Security Curriculum Development Conference* (pp. 15-19). ACM. doi:10.1145/2047456.2047458
- Roux, J., Alata, E., Auriol, G., Nicomette, V., & Kaâniche, M. (2017, September). Toward an intrusion detection approach for IoT based on radio communications profiling. In *2017 13th European Dependable Computing Conference (EDCC)* (pp. 147-150). IEEE. doi:10.1109/EDCC.2017.11
- Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Practical real-time intrusion detection using machine learning approaches. *Computer Communications*, 34(18), 2227–2235. doi:10.1016/j.comcom.2011.07.001
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007) Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the SOUPS*, 88–99. doi:10.1145/1280680.1280692
- Shrivasa, A. K., & Suryawanshi, R. (2017). Decision Tree Classifier for Classification of Phishing Website with Info Gain Feature. *International Journal for Research in Applied Science and Engineering Technology*, 5(5), 780–783.
- Srivastava, T. (2007). *Phishing and Pharming – The Deadly Duo*. SANS Institute. Retrieved from www.sans.org/reading-room/whitepapers/privacy/phishing-pharming-evil-twins-1731
- Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T. J. (2017). Intelligent phishing website detection using random forest classifier. In *Electrical and Computing Technologies and Applications (ICECTA), 2017 International Conference on* (pp. 1-5). IEEE. doi:10.1109/ICECTA.2017.8252051
- Vapnik, V. N. (1995). *The nature of statistical learning theory*. Springer. doi:10.1007/978-1-4757-2440-0
- Wang, X. J., & Wang, X. Y. (2010). Topology-assisted deterministic packet marking for IP traceback. *Journal of China Universities of Posts and Telecommunications*, 17(2), 116–121. doi:10.1016/S1005-8885(09)60456-8

Sameena Naaz is working as an Associate Professor in the Department of Computer Science and Engineering, Jamia Hamdard, New Delhi, India. She has a total experience of more than 18 years with one-year overseas experience. She received her Bachelor of Science (Computer Engg.) from Aligarh Muslim University, in 1998 and the M.Tech. Degree in Electronics with Specialization in Communication and Information Systems from Aligarh Muslim University, in 2000. She completed her Ph. D from Jamia Hamdard in the field of distributed systems in year 2014. Sameena Naaz has published several research articles in reputed International Journals and Proceedings of reputed International conferences published by IEEE and Springer. Her research interests include Distributed Systems, Big Data, Cloud Computing, Data Mining and Image Processing. She is life member of Indian Society for Technical Education (ISTE) and a member of International Association of Computer Science and Information Technology (IACSIT). She serves as reviewer of various Journals of International repute. She is also member of program committee of various reputed International conferences. She is in editorial Board of some reputed Intentional Journals in Computer Sciences.