iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VI **Month of publication:** June 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Bird's Eye View of Anti-Phishing Techniques for Classification of Phishing E-Mails

NiharikaVaishnaw[1], S R Tandan[2]
[1,2]*Department of Computer Science and Engineering,*
Dr. C. V. Raman University, Bilaspur (C.G), India

Abstract- Today, phishing emails are considered as one of the fastest growing threat for both organizations and individuals. Internet users are heavily prone to economic deficits due to fraudulent activities performed by these phishing mails. Various approaches and techniques have been developed to filter these phishing mails from mailboxes. In this paper, we present a review of different anti-phishing techniques for classification of phishing emails. We exhibit an overview of phishing scenario, attributes required to identify phishing mails, numerous machine learning based as well as other antiphishing techniques presently used to classify phishing email. This paper gives proper perspective towards the problem, its solution space, and helps to prognosticate the future research direction.
Keyword- Phishing emails, Types of phishing, Classification, Machine Learning, Anti-phishing techniques

I. INTRODUCTION

Now days the use of Internet is increasing rapidly to access information from the World Wide Web. Every organization like bank, insurance, industries have large volume of data. To secure such information, classification of information plays a very important role. Classification is one of the most important decision making techniques in many real world problems. Anti phishing is one of the important areas to classify the phishing and normal e-mails.
[21]Phishing is an Internet-based attack in which an attacker tricks a user into submitting his or her sensitive information to a fake website mimicking a legitimate site.This sensitive information ranges from usernames and passwords to bank account numbers and social security numbers. Phishing is a serious threat to the security of internet users' confidential information. Phishing email is also a type of spam email which redirects the users to fake websites and accesses their sensitive information. Fig1 describes the steps involved in phishing process. The phishing process starts with setting up counterfeited website by the phisher which is very much similar to a legitimate website. Phisher frequently send emails to target users with embedded hyperlinks directing to their fake website. As soon as the receiver clicks on the hyperlink, it takes it to the bogus website. There it asks users for their confidential information like username, id, password etc. When the users enter their personal information, phisher steal them and spoof the users.

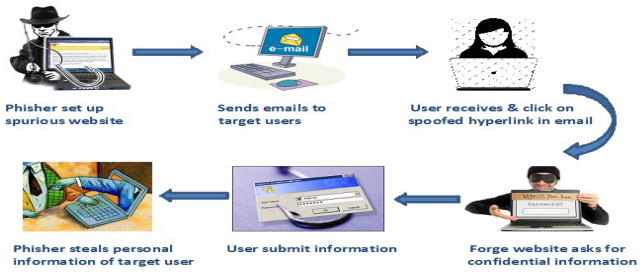


Fig 1: Process of phishing

A .Types Of Phishing Attacks
There are various types of phishing attacks, some of the conventional one are listed below [22].

1) Deceptive Phishing:This type of phishing attack broadcasts phishing emails to a wide group of recipients with the intention of acquiring their confidential information. It consists of messages related to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and

many other such scams.

2) Malware-Based Phishing: These attacks tries to inject malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from any web site, or by exploiting known security vulnerabilities—like un-updated software applications.

3) Keyloggers And Screenloggers: In this attack keyboard input are traced and relevant information is send to the hacker via the Internet. They embed themselve as small utility programs, device drivers or screen monitors that run automatically inside the system.

4) Session Hijacking: Users activity is observed until they sign in to their account or perform any transaction and establish their authentic credentials. At that point the malicious software commits unauthorized actions, like transferring funds, without the knowledge of user.

5) Web Trojans: Pop up invisibly when users attempt to log in. They retrieve legitimate informations locally and pass on to the attacker.

6) Hosts File Poisoning: Most of the users' PCs running a Microsoft Windows operating system first look up "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unawarely to a fake similar looking website where their information can be stolen.

7) System Reconfiguration: Perform alteration to settings on a user's PC for pernicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "citibank.com" to "citybank.com".

8) Data Theft: Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, and employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

9) DNS-Based Phishing ("Pharming"): Pharming is a Domain Name System (DNS)-based phishing. With this scheme, hackers manipulate a company's host's files or domain name system so that requests for URLs or name service return a forge address and further communications are directed to a fake website. The result: users unwittingly enter confidential information and get spoofed by hackers.

10) Content-Injection Phishing: It describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

11) Man-In-The-Middle Phishing: It is one of the most difficult to detect scheme. Hackers place themselves between the user and the legitimate website or system. They record the information coming from one end and continue to pass it on to the other end without influencing the ongoing transaction. Later they misuse the credentials collected when the user is not active on the system.

12) Search Engine Phishing: In this attack, phishers creates websites with appealing offers and have them indexed authenticaly with search engines. Users find these sites while surfing and are deluded by providing their information. For example, phishers set up false online shoppingwebsites offering exclusive deals at lower costs than other related sites. Victims get trapped and peforrm online transactions causing financial loss to them.

II. THE APWG REPORT Q2 2014

According to the last APWG report the intimidation of phishing is still high, the number of cyber attacks in the second quarter of 2014 is the second-highest number ever observed in a quarter since the APWG began its monitoring activity (2008)[23].“The total number of phish observed in Q2 was 128,378, a 3 percent increase over Q1 2014, when a total of 125,215 were observed. The 128,378 is the second-highest number of phishing sites detected in a quarter, eclipsed only by the 164,032 seen in the first quarter of 2012.” states the report.The APWG group detected an average of 42,793 new phishing attacks per month in Q2, the number of targets was decreased of 17 percent from same period of 2013, and the data confirms a higher concentration of attacks on more vulnerable brands.

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

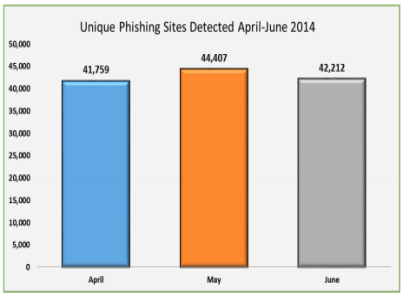


Fig.2: Phishing trend report of new phishing sites [23]

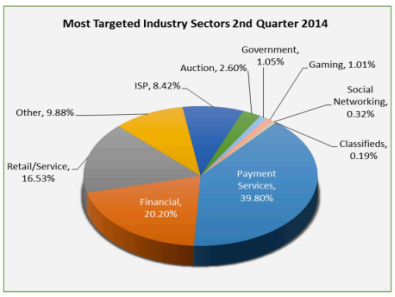


Fig.3: Industry sector area wise effects of phishing [23]

Fig2 indicates 41,759 unique sites detected in the month of April followed by 44,407 in May and 42,212 in June respectively. Fig 3 shows that Payment Services (39.80 percent) and Financial (20.20 percent) are most targeted industry sectors in Q2. The APWG report also includes data on attacks against reatail/service sites, the offensives on the industries grew, from 11.5 to 16.5 percent of all phishing attacks. According to the APWG report, Trojans are still the most common type of malware (58.20%), but experts are worried by the increase in PUPs (Potentially Unwanted Programs) such as spyware andadware. The APWG members linked the increase in PUPs to a significant increase in the creation of software bundlers, which install programs that serve PUPs [23]

III. ANTI-PHISHING TECHNIQUES

In order to guard internet users from malicious activities of phishers, several antiphishing techniques have been developed. In general the techniques can be classified as list-based, heuristic-based and machine learning-based approach.

A .List-Based Approach

This approach comprises of a black list and a white list. The black list contains numerous URLs of phishing sites reported by internet users or collected by web crawlers. The list maintainers ensure whether the reported URLs are phishing sites or not. The drawback of this approach is that it does not give 100% guarantee. There is always a possibility of unreported and uncollected URLs. On the other hand white list contains names of legitimate domains. When user tries to visit a site which is not present in the list, it gets blocked & decision is upto the user. The drawback with this approach is that it constantly asks for permission due to which the impatient user either disables the filtering mechanism or unblocks it.

B. Heuristic-Based Approach

Heuristic-based approach applies diverse criteria to find out whether a website is a phishing site. Domain names, URL, image similarity, keywords etc. are some of the respective criterias. This mechanism may use only one criterion to assess web sites. For example, the basic CANTINA filter [24] only calculates the TF-IDF score.

C. Machine learning-Based Approach

This is one of the best and widely used approaches because of its best results and high accuracy. Machine learning (ML) is a branch of artificial intelligence (AI) that employs the method of data mining to discover new or existing patterns (or features) from a dataset which is then used for the purpose of classification. Many machine learning algorithms are used as classifiers to classify phishing and non-phishig emails. This section is further discussed in detail later in this paper.

IV. ATTRIBUTES OF A PHISHING EMAIL

A phishing email consists of multimedia information, such as image and text, where the text information may contain rich/plain text, HTML, URLs, scripts, styles, etc. From this information however it is not that easy to recognize a phishing email since all these may present in a non-phishing email too. Hence, different types of features are defined manually based on observation to detect such mails which serve as input to various classifiers.After the survey of available literature, we have selected various attributes that capture the characteristics of phishing emails and consolidated them in a tabular representation (Table I).

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

TABLE I: ATTRIBUTES INDICATING THREAT OF PHISHING ACTIVITIES

S. no	Attributes	Description	Example
1	URL	-Containing IP Address	http://192.82.12.1/signin.ebay.com
		-Inclusion of @ symbol in order to redirect users to another site	www.citybank.com@123.123.123.12 instead of www.citibank.com
2	Domain Name	-Phishing site may register itself with a similar name as a legitimate site	www.snapdea1.com instead of www.snapdeal.com
		-Number of dots or periods	More than 3 dots suspect the legitimacy of site
3	Hyperlinks	-Hyperlinks in email does not route to same location as is supposed to do	
		-Unusually long hyperlinks	http://payment2.works.com/wpm/validate?code=2139877…..nvuhufyeru993fu8eu00
		-Disparity between “href” attribute and “link text”	 Bogus.com Instead of paypal.com
4	Keywords	Frequently appearing words in phishing emails	Win!; Jackpot; Update; Confirm; Click; Here; Login; User; Customer; Client;
5	Input Fields	Phishing sites usually require users to input their personal information and hence embed input fields	Enter Password, UserID, Security No. , Account No. ,Credit Card No etc.
6	HTML Content	Phishing emails consists of content-type with attribute “text/html” in order to use HTML links	Type of content- “text/html” Instead of “text/plain”
7	Embedded JavaScript	Presence of JavaScript in either body of email or in link mostly to hide information from the user	Use of <Script>tag
8	Absence of personalized information	Phishing emails does not contain personalized content about the user	Address without name of recipient, Lack of last 4 digits of recipient’s account no.
9	Disparity between domain names in email and sender’s domain name	Phishing emails have mismatch between domain names present inside email and sender’s domain(the domain name referred to by the “From” field of the same email)	
10	Ruses	Phishing emails uses different ruses to create an urgency situation to trap recipient	-The customer's account may be frozen if account details are not provided within a specified time -Fraudulent activity involving the user's account has been detected and the user must therefore provide information urgently.etc.

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. MACHINE LEARNING BASED ANTI- PHISHING TECHNIQUES

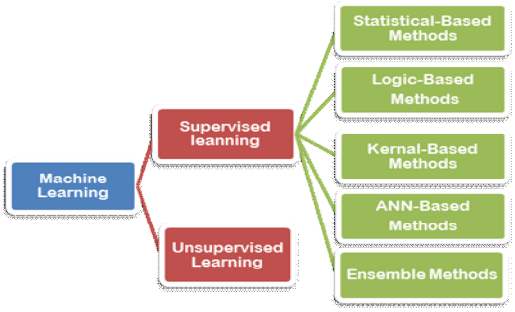


Fig 4: Classification of Machine Learning Techniques

Machine learning is one of the important subfield of computer science and classification is an important application of machine learning techniques.Machine learning focuses on the development of computer programs that can teach themselves to grow and change when exposed to new data. Maching learning, concerns the construction and study of systems that can learn from data.

Supervised Learning is the learning in which the training data is labeled with the correct answers, e.g., "spam" or "ham." The two most common types of supervised learning are "classification" (where the outputs are discrete labels, as in spam filtering) and "regression" (where the outputsare real-valued).

Unsupervised learning is the learningin which we are given a collection of unlabeled data, which we wish to analyze and discover patterns within. The two most important examples are "dimension reduction" and "clustering".

AmmarAlmomani et.al [1] proposed a survey of the protection against these phishing email attacks.This survey improves the understanding of the phishing emails problem, the current solution space, and the future scope to filter phishing emails. Most classifiers used to identify phishing email are based on: supervised learning, i.e. they must learn before they can be used to detect a new attack; unsupervised learning, which is faster, but has a low level of accuracy; or a hybrid (supervised and unsupervised) learning, which is time consuming and costly.

In this research work, we have breifed various classification techniques to classify phishing attacks. These are described below:

A. Statistical-Based Methods

Statistical approaches are characterized by having an explicit underlying probability model, which provides a probability that an instance belongs in each class, rather than simply a classification. Under this category of classification algorithms, one can find Bayesian networks and Naive Bayesian networks (NB).

1) Bayesian Networks: A Bayesian Network [25] is a graphical model for probability relationships among a set of variables (features). The Bayesian network structure *S* is a directed acyclic graph (DAG) and the nodes in *S* are in one-to-one correspondence with the features *X*. The arcs represent casual influences among the features while the lackof possible arc in S encodes conditional independencies. Moreover, a feature (node) is conditionally independent from its non-descendants given its parents.Typically, the task of learning a Bayesian network can be divided into two subtasks: initially, the learning ofthe DAG structure of the network, and then the determination of its parameters. Probabilistic parametersare encoded into a set of tables, one for each variable, in the form of local conditional distributions of a variablegiven its parents.

IsredzaRahmi A Hamid et.al [4] proposed a hybrid feature selection approach based on combination of content based and behavior-based. The study presented that hybrid features selections are able to achieve 93% accuracy rate as compared to other approaches. In addition, the quality of proposed behavior-based feature (used to detect phishing emails by observing sender behavior) using the Information Gain, Gain Ratio and Symmetrical Uncertainty is successfully tested.This hybrid feature selection approach achieved 93% accuracy.For data size of 60:40, Bayes Net outperformed other classifier and achieved the highest accuracy in set 2 which is 92% when compared to Adaboost and Random Forest. The results recommend that Bayes Net works well because of its manipulating capabilities of tokens and associatedprobabilities according to the user's classification decisions and empirical performance.

Saeed Abu-Nimeh et.al [3] developed a client-server distributed architecture to detect phishing e-mails by taking advantage of automatic variable selection in Bayesian Additive Regression Trees (BART). When combined with other classifiers, BART improves their predictive accuracy. Further the overall architecture proves to leverage well in resource constrained environments.The results demonstrated that automatic variable selection in CBART can be used to improve the predictive accuracy in other classifiers. Although the AUC decreased for the majority of classifiers (except LR), the error rate, false positive rate, and false negative rate decreased for RF, LR, and NNet after using variable selection via CBART. However, when using another variable selection technique, namely Kruskal-Wallis (KW) test, the predictive accuracy for all the compared classifiers degraded.

*2) Naive Bayes Classifiers***:** Naive Bayesian networks (NB) are very simple Bayesian networks which are composed of DAGs with only one parent (representing the unobserved node) and several children (corresponding to observed nodes) with a strong assumption of independence among child nodes in the context of their parent. The major advantage of the naive Bayes classifier is its short computational time for training. In addition, since the model has the form of a product, it can be converted into asum through the use of logarithms with significant consequent computational advantages.

Zhan, J.Thomas [2] proposed anomaly detection in dynamic social environment by using Stochastic Learning Weak Estimation (SLWE) approach. This approach is studied and implemented based on Naïve Bayes classification, for filtering phishing emails that are unpredictable in nature. Experimental results shows that the SLWE based Naïve Bayes filters are superior in performance, when compared with the MLE (Maximum Likelihood Estimation) based filter. The SLWE filters are adapted especially in environments where there are abrupt changes in the distribution of phishing and non-phishing emails. Moreover the drops in the detection rates of phishing were recovered faster by employing the SLWE filter.

B. Logic-Based Methods

In this section we will concentrate on of logical (symbolic) learning methods: decision trees, random forest and c5.0.

1) Decision Tree: Decision tree induction is the learning of decision trees fromclass-labeled training tuples.Adecision tree is a flowchart-like tree structure,where each internal node (nonleaf node)denotes a test on an attribute, each branch represents an outcomeof the test, and each leafnode (or *terminal node*) holds a class label. The topmost node in a tree is the root node.The construction of decision treeclassifiers does not require any domain knowledge or parameter setting, and therefore isappropriate for exploratory knowledge discovery. Decision trees can handle high dimensionaldata. Their representation of acquired knowledge in tree form is intuitive and generally easy to assimilate by humans. The learning and classification steps of decision treeinduction are simple and fast. In general, decision tree classifiers have good accuracy.

Ma, L.Ofoghi et.al [5] developed a method to build a robust classifier to detect phishing emails using hybrid features and to select features using information gain. The experiment was done on 10 cross-validations to build an initial classifier which performs well. The experiment also analyses the quality of each feature using information gain and best feature set is selected after a recursive learning process. Experimental result shows the selected features perform as well as the original features. The performance of five machine learning algorithms i.e decision tree, random forest, multi-layer perceptron, naive bayers and support vector machine (SVM) was compared. The result comes that decision tree generated the highest accuracy which builds a good classifier. Comparing to decision tree methods, the accuracies of other learning algorithms are random forest (-0.02%), multi-layer perceptron (-0.72%), naive bayes (-0.94%) and support vector machine (-1.92%). This result recommends that decision tree works well in discrete and small vector space data.

2) Random Forest (RF): Random forest (RF) is an ensemble learning classification and regression method suitable for handling problems involving grouping of data into classes. The algorithm was developed by Breiman and Cutler. In RF, prediction is achieved using decision trees.During the training phase, a number of decision trees are constructed (as defined by the programmer) which are then used for the class prediction; this is achieved by considering the voted classes of all the individual trees and the class with thehighest vote is considered to be the output.

Andronicus A. Akinyeluet.al [6] investigated and reported the use of random forest machine learning algorithm in classification of phishing attacks, with the major objective of developing an improved phishing email classifier with better prediction accuracy and fewer numbers of features. The study presented a content-based phishing detection approach which has bridged the current gap identified in the literature. From a dataset consisting of 2000 phishing and ham emails, a set of prominent phishing email features (identified from the literature) were extracted and used by the machine learning algorithm with a resulting classification accuracy of 99.7% and low false negative (FN) and false positive (FP) rates of about 0.06%.

Khonji et.al [7] proposed in the study that the classification accuracy of anti-phishing email filters enhance when they incorporate

the proposed lexical URL analysis technique. To evaluate the claims, a highly accurate anti-phishing email classifier is constructed and tested against publicly available phishing and legitimate email data sets. When RF was run with AdaBoostM1 [20] and using features set 3-A (the full features set without features subset selection, with Lexical URL Analysis (48 features in total), its classification model resulted in an f1 score of 99.45%. Only one classifier is known to have a higher f1 score of 99.46%however it uses additional model-based featuresand image processing techniques.

PILFERS is a proposed method to detect phishing emails byFette et.al [19]. This technique works based on 10 different features representing phishing emails. Nine features extracted from the email itself, while the tenth feature represents the age of linked-to-domain names, which can be extracted from a WHOIS query at the time the email is received. The S.A. tool (Spam assassin), was used to identify if this email has spam features or not. This technique works based on 10-fold cross-validation with random forest and SVM as classifiers to train and test the dataset. This approach is a machine-learning based approach to classification. For reference implementation of PILFER, random forest was used as a classifier. The result of the PILFER with S.A. features was 0.12% false positive rate, and 7.35% false negative rate, respectively, which means that a sizeable number of phishing and ham emails were not well classified.

3) C5.0: C5.0 [8] is one of the more recent in a family of learning algorithms referred to as decision tree algorithms. This algorithm is an improvement of the C4.5 algorithm also developedby Quinlan. The improvements are merely in efficiency, the algorithm remains the same. The algorithm is based on theconcepts of entropy, the measure of disorder in the collection,and the information gain of each attribute. Information gain isa measure of the effectiveness of an attribute in reducing theamount of entropy in the collection.

F. Toolan et.al [8] introduced an approach to classifying emails into Phishing / non-Phishing categories using the C5.0 algorithm which achieves very high precision and an ensemble of other classifiers that achieve high recall. The representation of instances used in this paper is very small consisting of only five features. Results of an evaluation of this system, using over 8,000 emails approximately half of which were phishing emails and the remainder legitimate, are presented.The F-Score of the R-Boost method was 99.31% by far the highest of the techniques that have been examined.These results show the benefits of using this recall boosting technique [8] over that of any individual classifier or collection of classifiers.

C. Kernal Method

Kernel Methods are best known for the popular method Support Vector Machines which is really a constellation of methods in and of it. Kernel Methods are concerned with mapping input data into a higher dimensional vector space where some classification or regression problems are easier to model.

1) Support Vector Machines (SVM): In formal definition, a support vector machine design a hyperplane or set of hyperplanes in a high or infinite dimensional space, which can be used for classification, regression or other tasks. A SVM is a promising new method for classification of both linear and nonlinear data. Support Vector Machines are based on the concept of decision planes that define decision boundaries. A decision plane is one that separates between a set of objects having different class memberships [9]. Support vector machine algorithms divide the n dimensional space representation of the data into two regions using a hyperplane. This hyperplane always maximizes the margin between the two regions or classes. The margin is defined by the longest distance between the examples of the two classes and is computed based on the distance between the closest instances of both classes to the margin, which are called supporting vectors [9].

M.Chandrasekaran et.al [10] proposed a novel technique to discriminate phishing emails from the legitimate emails using the distinct structural features present in them. The derived features, together with one class support vector machine (SVM) can be used to efficiently classify phishing emails before it reaches the users inbox, essentially reducing human exposure. Their prototype implementation sits between a user's mail transfer agent (MTA) and mail user agent (MUA) and processes each arriving email even before it reaches the inbox.

Bergholz et.al [11] employed statistical classification methods to classify emails as legitimate (ham) or phishing emails. Two new types of features generated by adaptive Dynamic Markov Chains (DMC) and by latentClass-Topic Models (CLTOM) were introduced. Teiradaptive DMC approach reduces the memory requirements compared to the standard DMC approach by two thirds almost without any loss in performance. CLTOM approach, which incorporates class-specific information into the topic model, outperforms the standard LDA approach for topic numbers of up to 100. Classifiers incorporating these features as input are able to substantially outperform previous approaches on publicly available benchmark corpora.Support Vector Machine (SVM) classifier

gets implemented in the libSVM-library. The RBF kernel with parameters C = 10 and gamma = 0.1 turned out to be most accurate and stable.

Wilfried N. Gansterer David et. al [12] introduced various new features for identifying phishing messages and rank established as well as newly introduced features according to their significance for classification problem. Moreover, in contrast to classical binary classification approaches (spam vs. not spam), a more refined ternary classification approach for filtering e-mail data is investigated which automatically distinguishes three message types: ham (solicited e-mail), spam, and phishing. The classification is based on a partly new designed set of features to be extracted from each incoming message. SVM classifier based on feature set *F*1 achieved an overall accuracy of 92,5% on a balanced test data set (1000 messages from each class. On a correspondingly imbalanced test set the overall accuracy improved to 95,3%. Various classifiers have been compared for assigning messages to one of the three groups. Over all three groups, a classification accuracy of 97% was achieved, which is better than solving the ternary classification problem with a sequence of two binary classifiers. Overall, the SVM achieves the highest accuracy.

D. ANN-Based Method

Artificial Neural Networks are models that are inspired by the structure and/or function of biological neural networks. They are a class of pattern matching that are commonly used for regression and classification problems but are really an enormous subfield comprised of hundreds of algorithms and variations for all manner of problem types.

1) Neural Networks: An artificial neural network, or neural network, is a mathematical model inspired by biological neural networks. Inmost cases it is an adaptive system that changes its structure during learning. There are many different typesof NNs. For the purpose of phishing detection, which is basically a classification problem, we choose multilayerfeedforward NN. In a feedforward NN, the connections between neurons do not form a directed cycle. Contrastedwith recurrent NNs, which are often used for pattern recognition, feedforward NNs are better at modeling relationships between inputs and outputs.

N. Zhang et.al [13] proposed multilayer feedforward neural networks for phishing email detection and evaluated the effectiveness of this approach. From the statistical analysis, it was concluded that NNs with an appropriate number of hidden units can achieve satisfactory accuracy even when the training examples are scarce. The multilayer feedforward NN is implemented in Java with the Encog Java Core package, which provides a powerful framework to conveniently construct NNs and perform training and testing. NN gives the highest recall while still maintaining a >95% precision, suggesting that NNs are excellent at detecting phishing emails while misclassifying only a small portion of ham emails.

ALmomani et.al [14] proposed the Detection and Prediction of unknown “zero-day” phishing Emails by provide a new framework called Phishing Evolving Neural Fuzzy Framework (PENFF) that is based on adoptive Evolving Fuzzy Neural Network (EFuNN). PENFF does the process of detection of phishing email depending on the level of features similarity between body email and URL email features. The totality of the common features vector is controlled by EFuNN to create rules that help predict the phishing email value in online mode. The proposed framework has proved its ability to detect phishing emails by decreasing the error rate in classification process. The current approach is considered a highly compacted framework. As a performance indicator; the Root Mean Square Error (RMSE) and Non-Dimensional Error Index (NDEI) has 0.12 and 0.21 respectively, which has low error rate compared with other approaches Furthermore, this approach has learning capability with footprint consuming memory.

E. Ensemble Methods

Ensemble methods or hybrid models are models composed of multiple weaker models that are independently trained and whose predictions are combined in some way to make the overall prediction. Much effort is put into what types of weak learners to combine and the ways in which to combine them. This is a very powerful class of techniques and as such is very popular. A hybrid model is a combination of two or more models to avoid the drawbacks of individual models and to achieve high accuracy. Bagging and boosting are two techniques that use a combination of models. Each combines a series of *k* learned models (classifiers), *M*1, *M*2,…..*Mk*, with the aim of creating an improved composite model, *M*.

A novel method for profiling phishing activity from an analysis of phishing emails is proposed by John Yearwood et.al [15]. Profiling is useful in determining the activity of an individual or a particular group of phishers.It is distinct from detection of phishing emails. The profiling problem is formulated as a multi-label classification problem using the hyperlinks in the phishing emails as features and structural properties of emails along with whois (i.e.DNS) information on hyperlinks as profile classes. Further, profiles based on classifier predictions are generated and classes become elements of profiles. A boosting algorithm (AdaBoost) as well as SVM to generate multi-label class predictions on three different datasets created from hyperlink information

in phishing emails is employed. These predictions are further utilized to generate complete profiles of these emails. Results show that profiling can be done with quite high accuracy using hyperlink information.

Del Castillo et.al [16] developed a system for classifying e-mails into two categories, legitimate and fraudulent. This classifier system is based on the serial application of three filters: a Bayesian filter that classifies the textual content of e-mails, a rule based filter that classifies the non-grammatical content of e-mails and, finally, a filter based on an emulator of fictitious accesses which classifies the responses from websites referenced by links contained in e-mails. The approach of this system is hybrid.A client-side system called FRALEC is proposed, which was designed and built to detect and filter phishing e-mail automatically, using different sources of information present in the content of e-mails which are handled by the processing methods most suitable for each information type.The author used 1,038 emails (10 emails as legitimate and 1,028 as phishing emails).The precision in the best result was 96%. FRALEC is an effective system for filtering fraudulent e-mails. Its good performance is reached because of integrating different classification methods that deal with all kinds of data present in e-mails.

VI. OTHER ANTIPHISHING TECHNIQUES

R. B. Basnet et.al [17] proposed a new and simple methodology to detect phishing emails utilizing Confidence-Weighted Linear Classifiers. The contents of the emails as features are used without applying any heuristic based phishing specific features and obtain highly accurate results compared to the best that have been published in the literature. Confidence-Weighted Linear classifiers achieved the best accuracy of 99.77%, with false positive rate (FPR - ham emails marked as phishing) of less than one percent across all datasets. LIBLINEAR which is a linear classifier for millions of instances and features on the other hand gave the best accuracy of 99.58% with FPR less than 1% and the worst FNR of 2.3% on Corpus2 dataset.

MadhusudhananChandrasekaran et.al [18] presented a novel approach to detect phishing attacks using fake responses which mimic real users, essentially, reversing the role of the victim and the adversary. Our prototype implementation called PHONEY, sits between a user's mail transfer agent (MTA) and mail user agent (MUA) and processes each arriving email for phishing attacks. Using live email data collected over a period of eight months we demonstrate data that our approach is able to detect a wider range of phishing attacks than existing schemes. The evaluation of the tool showed that our approach is able to detect a vast majority of the attacks, including cases where the masqueraded page is launched within the legitimate domain with no false positives

V.Shreeram et al. [20] have proposed genetic algorithm approach to detection of phishing webpages by using rule-based system and this rule set is used to match the hyperlink. An approach to detect phishing hyperlinks using the rule based system formed by genetic algorithm is proposed, which can be utilized as a part of an enterprise solution to anti-phishing. A legitimate webpage owner can use this approach to search the web for suspicious hyperlinks. In this approach, genetic algorithm is used to evolve rules that are used to differentiate phishing link from legitimate link. Evaluating the parameters like evaluation function, crossover and mutation, GA generates a ruleset that matches only the phishing links. This ruleset is stored in a database and a link is reported as a phishing link if it matches any of the rules in the rule based system and thus it keeps safe from fake hackers. Preliminary experiments show that this approach is effective to detect phishing hyperlink with minimal false negatives at a speed adequate for online application.

VII. DISCUSSION

This section presents a comparative study of techniques and mechanisms used for phish mail detection and their classification by different researchers. Table II describes the name of all the authors whose work is referred in this paper, their proposed work, result and analysis of the proposed method or system along with the name of proceeding journals and year of its publishing.

TABLE II: BRIEF SUMMERY OF PROPOSED LITERATURE

S.no	Author Name	Title of the paper	Proposed Work	Technique/ Algorithm	Results & Analysis	Name of Journal	Year
1.	Andronicus A.Akinyelu et.al	Classification of Phishing E mail Using Random Forest Machine Learning Technique	Development of an improved phishing email classifier	Random Forest(RF)	Classificati-on accuracy of 99.7%	Journal of Applied Mathematics	2014

2.	AmmarAlmomani et.al	A Survey of Phishing Email Filtering Techniques	A survey of the protection against phishing email attacks	-	-	IEEE Communications survey & tutorials	2013
3.	Khonji et.al	Enhancing Phishing E-Mail Classifiers: A Lexical URL Analysis Approach	Lexical URL analysis technique	Random Forest(RF) and AdaBoost	Accuracy 99.45%	International Journal for Information Security Research (IJISR),	2012
4.	ALmomani et.al	Evolving fuzzy neural network for phishing emails detection	PENFF to predict dynamically the zero day phishing e-mails	(EFuNN)	Decrease in the error rate in classification process	Journal of Computer Science	2012
5.	Zhan et.al	Phishing detection using stochastic learning-based weak estimators	Anomaly detection in dynamic SLWE approach	Naïve Bayes	SLWE based Naïve Bayes filters are superior in performance	Computational Intelligence in Cyber Security (CICS), IEEE Symposium	2011
6.	IsredzaRahmi A Hamid et.al	Phishing Email Feature Selection Approach	A hybrid feature selection approach	Bayes Net	Accuracy 93%	International Joint Conference of IEEE TrustCom	2011
7.	John Yearwood et.al	Profiling Phishing Emails Based on Hyperlink Information	Profiling phishing activity	SVM and AdaBoost	Profiling can be done with high accuracy using hyperlink information.	International Conference on Advances in Social Networks Analysis and Mining	2010
8.	R.B. Basnet et.al	Classifying Phishing Emails Using Confidence-Weighted Linear Classifiers	Confidence-Weighted Linear Classifiers	LIBLINEAR classifier	Accuracy 99.58%	International Conference on Information Security and Artificial Intelligence	2010
9.	V. Shreeram et.al	Anti-phishing detection of phishing attacks using Genetic Algorithm	Genetic algorithm approach to detect phishing webpages	Genetic Algorithm	Minimal false negatives at a speed adequate for online application	IEEE	2010

10.	Saeed Abu-Nimeh et.al	Distributed phishing detection by applying variable selection using Bayesian additive regression trees	A client-server distributed architecture to detect phishing e-mails	BART	Automatic variable selection in CBART improve the predictive accuracy	IEEE International Conference on Communications	2009
11.	Ma, L.Ofoghi et.al	Detecting phishing emails using hybrid features	Robust classifier Model	Decision tree algorithm, C4.5	Decision tree is a good classifier	IEEE	2009
12.	F. Toolan et.al	Phishing Detection using Classifier Ensemble.	R-Boost Mehod	C5.0	Accuracy 99.31%	E-Crime Researchers Summit	2009
13.	Wilfried N. Ganstereret. al	E-Mail Classification for Phishing Defense	Ternary classification approach for filtering e-mail data	SVM	Accuracy 97%	Springer-Verlag	2009
14.	Andre Bergholz et.al	Improved phishing detection using model-based features	Study the statistical filtering of the phishing emails	Dynamic Markov Chain and Class-Topic Models	SVM gets implemented in the libSVM-library.	Proceedings of the Conference on Email and Anti-Spam (CEAS)	2008
15.	del Castillo et.al	An Integrated Approach to Filtering Phishing Emails Computer Aided Systems Theory	FRALEC Modelconsists of three classifiers	NaveBayes Classifier, rule-based classifier, Emulator-Based classifier	Precision 96%	Springer-Berlin	2007
16.	Fette, I.Sadeh et al	Learning to detect phishing emails	PILFERS prototypes	SVM, RF	PILFER with S.A. features was 0.12% FPR, and 7.35% FNR	Proceedings of the 16th International World Wide Web Conference	2007
17.	M. Chandrasek-aran, et.al	Phishing email detection based on structural properties	Structural Features,	Support Vector Machine (SVM) classifiers	The prototype implementationsits between (MTA) and (MUA)	NYS Cyber Security Conference	2006

18.	Madhusudh-ananChandrasek-aran et.al	Phoney: Mimicking user response to detect phishing attacks	approach to detect phishing attacks using fake responses which mimic real users	PHONEY	PHONEY technique is installed between a user's MTA and MUA	IEEE Comuter Society	2006

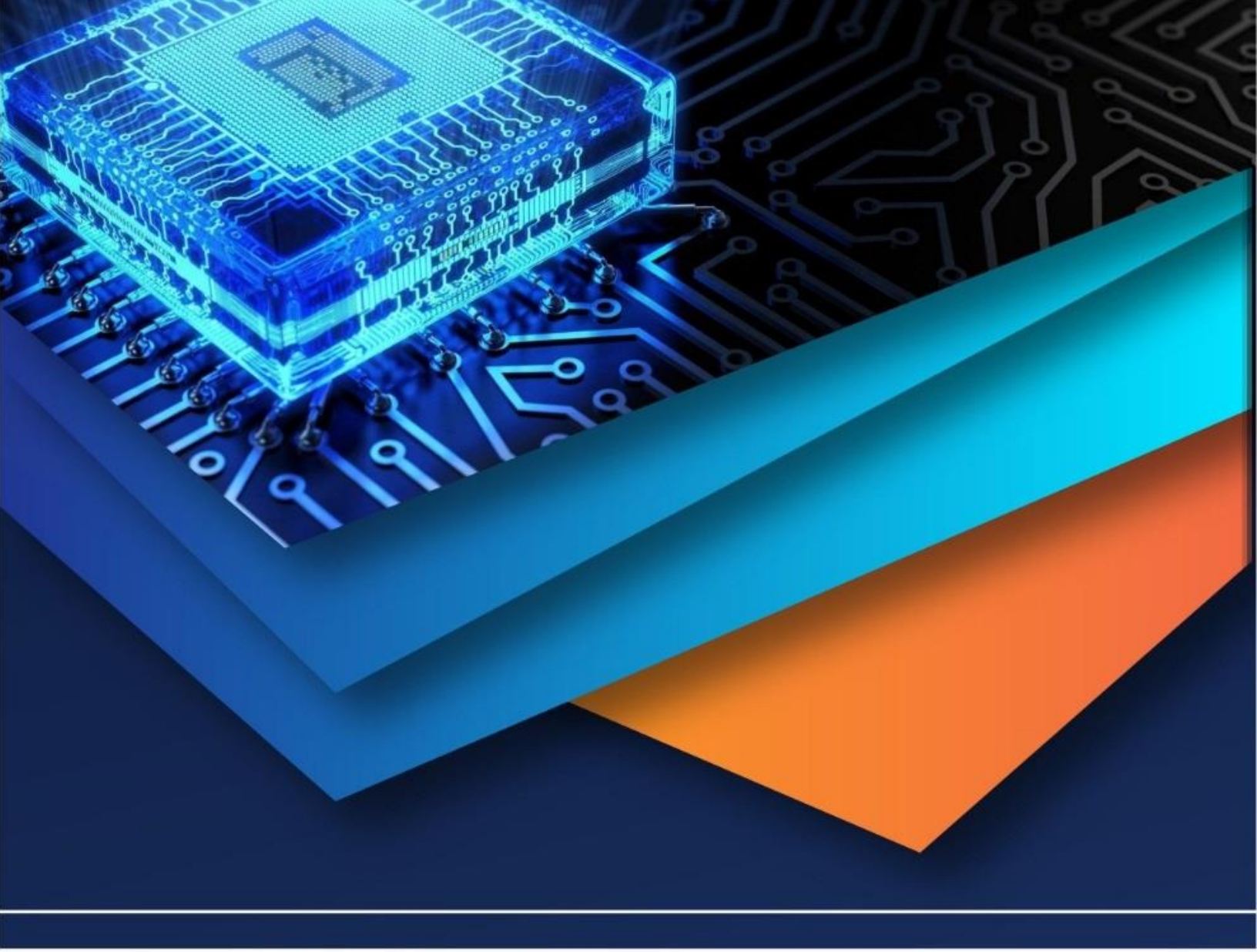
VIII. CONCLUSION

Phishing is a fraudulent activity which mostly attack through emails, websites and phone calls. Phishing emails are those emails which have wrong intentions of stealing confidential information by directing the user to their bogus website and tricking them to enter their personal information. The financial loss incurred by internet users and organizations due to phishing is growing rapidly day by day. However several approaches have been developed to protect against these phishing attacks. This survey enhances the understanding of phishing problem and helps to comprehend various anti-phishing approaches. Out of all, machine learning approaches are considered to be most affective giving satisfactory results. Approaches mentioned in the literature are able to give moderate protection against these attacks still none of them ensures 100% accuracy. Moreover many of them like hybrid techniques are costly and time consuming. Thus there is still a space for better approaches to solve drawbacks of previous ones.

REFERENCES

[1]AmmarAlmomani, B. B. Gupta, SamerAtawneh, A. Meulenberg, and EmanAlmomani, "A Survey of Phishing Email Filtering Techniques", IEEE Communications survey & tutorials, Vol.15,no.4, fourth quarter 2013.
[2] Zhan, J.Thomas, L., "Phishing detection using stochastic learning-based weak estimators," inComputational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on, pp. 55-59,2011.
[3]Saeed Abu-Nimeh1, Dario Nappa2, Xinlei Wang2, and Suku Nair1, "Distributed phishing detection by applying variable selection using Bayesian additive regression trees", in IEEE International Conference on Communications, vol.1, 2009, pp. 1-5.
[4] IsredzaRahmi A Hamid and JemalAbawajy," Phishing Email Feature Selection Approach", International Joint Conference of IEEE TrustCom-11, pp. 916-921, 2011.
[5]Ma, L.Ofoghi, B.Watters, P.Brown, S.,"Detecting phishing emails using hybrid features,",IEEE,pp.493-497, 2009.
[6]Andronicus A. Akinyelu and Aderemi O. Adewumi, "Classification of Phishing E mail Using Random Forest Machine Learning Technique", Journal of Applied Mathematics, Vol. 2014, Article ID 425731, pp. 1-6.
[7]Khonji, M.Iraqi, Y.Jones, A., "Enhancing Phishing E-Mail Classifiers: A Lexical URL Analysis Approach," International Journal for Information Security Research (IJISR), vol. 2,no.1/2, 2012.
[8]F. Toolan, J. Carthy.: Phishing Detection using Classifier Ensemble. In E-Crime Researchers Summit,2009.
[9]V. Vapnik, "The Nature of Statistical Learning Theory" ,Springer; 2 edition , 1998.
[10]MadhusudananChandrasekaran, Krishnan Narayanan and ShambhuUpadhyaya," Phishing email detection based on structural properties",NYS Cyber Security Conference, 1-7, 2006
[11]Bergholz, A.Chang, J.H.Paaß, G.Reichartz, F.Strobel, "Improved phishing detection usingmodel-based features," in Proceedings of the Conference on Email and Anti-Spam (CEAS),Mountain View,CA., 2008.
[12]Wilfried N. Gansterer David P\, et al., "E-Mail Classification for Phishing Defense,", Springer-Verlag, presented at the Proceedings of the 31th European Conference on IR Research on Advances in Information Retrieval, Toulouse, France,PP. 449-460, 2009.
[13] N. Zhang and Y. Yuan, "Phishing detection using neural network," http://cs229.stanford.edu/proj2012/ZhangYuan-PhishingDetectionUsingNeuralNetwork.pdf.
[14]ALmomani, T.-C. Wan, A. Altaher et al., "Evolving fuzzy neural network for phishing emails detection," Journal of Computer Science, vol. 8, no. 7, pp. 1099–1107, 2012.
[15]John Yearwood, Musa Mammadov and Arunava Banerjee, "Profiling Phishing Emails Based on Hyperlink Information", 2010 International Conference on Advances in Social Networks Analysis and Mining, DOI: 10.1109/ASONAM.2010.56, 2010.
[16]del Castillo, M.Iglesias, Ángel Serrano, J., "An Integrated Approach to Filtering Phishing Emails Computer Aided Systems Theory – EUROCAST 2007." vol. 4739, R. Moreno Díaz, et al., Eds., ed: Springer Berlin / Heidelberg, pp. 321-328, 2007.
[17] R. B. Basnet, A. H. Sung.: Classifying Phishing Emails Using Confidence-Weighted Linear Classifiers.2010 International Conference on Information Security and Artificial Intelligence (ISAI 2010).
[18]MadhusudhananChandrasekaran, RamkumarChinchani and ShambhuUpadhyaya, "Phoney: Mimicking user response to detect phishing attacks," in In: Symposium on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society, 2006, pp. 668-672.
[19]Fette, I.Sadeh, N.Tomasic, A.., "Learning to detect phishing emails," in Proceedings of the 16th International World Wide Web Conference (WWW 2007), ACM Press, Banff, Alberta,Canada, pp. 649-656. 2007.
[20] V.Shreeram, M.Suban, P.Shanthi, K.Manjula, "Anti-phishing detection of phishing attacks using Genetic Algorithm" 978-1-4244-7770-8/10/ ©2010 IEEE.

[21]Peter Likarish, Don Dunbar and Thomas E. Hansen, “B-APT: Bayesian Anti-Phishing Toolbar”, IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings, 2008.
[22]PCWorld, http://www.pcworld.com/article/135293/article.html
[23]Anti-Phishing Working Group, "Phishing Activities Trends REPORT," ed, apwg, http://securityaffairs.co/wordpress/27935/cyber-crime/apwg-q2-2014-report.html
[24]Zhang Y, Hong JI, Cranor LF. Cantina: a content-based approach to detecting phishing web sites. In: WWW ’07: proceedings of the 16th inter- national conference on World Wide Web. New York, NY, USA: ACM; 2007. p. 639–48.
[25]S. B. Kotsiantis,” Supervised Machine Learning: A Review of Classification Techniques”, in Informatica31, 2007, pp. 249–268.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY