A Survey of Phishing Email Filtering Techniques

Ammar Almomani, B. B. Gupta, Samer Atawneh, A. Meulenberg, and Eman Almomani

***Abstract*—Phishing email is one of the major problems of today's Internet, resulting in financial losses for organizations and annoying individual users. Numerous approaches have been developed to filter phishing emails, yet the problem still lacks a complete solution. In this paper, we present a survey of the state of the art research on such attacks. This is the first comprehensive survey to discuss methods of protection against phishing email attacks in detail. We present an overview of the various techniques presently used to detect phishing email, at the different stages of attack, mostly focusing on machine-learning techniques. A comparative study and evaluation of these filtering methods is carried out. This provides an understanding of the problem, its current solution space, and the future research directions anticipated.**

***Index Terms*—Phishing email, Filtering, Classifiers, Machine learning, Authentication, Network level protection.**

I. Introduction

PHISHING email is a special type of spam message. Such email is a criminal mechanism that relies on forged email claims purportedly originating from a legitimate company or bank. Subsequently, through an embedded link within the email, the phisher attempts to redirect users to fake Websites, that are designed to fraudulently obtain financial data such as usernames, passwords, and credit card numbers [1-5].

Phishing emails pose a serious threat to electronic commerce because they are used to defraud both individuals and financial organizations on the Internet. A survey by Gartner [6] on phishing attacks shows that, approximately 3.6 million clients in the US alone had lost money to phishing attacks and total losses had reached approximately US$ 3.2 billion Dollar. The number of victims increased from 2.3 million in 2006 to 3.6 million in 2007, an increase of 56.5%. Among all complaints received by the Federal Trade Commission in 2009 from Internet users, identity theft attributed to phishing email ranked first. It accounted for 21% of the complaints and cost consumers over 1.7 billion US dollars [7]. According to an eCrime trends report [8], phishing attacks are increasing at a rapid rate. For example, phishing in Quarter 1 (Q1) of 2011 grew by 12% over that in Quarter 1 (Q1) of 2010. Phishing emails range from very simple to very complicated messages and are capable of deceiving even the clever Internet users. Fraudulent emails can steal secret information from the victims, resulting in loss of funds. As a consequence, these attacks are damaging electronic commerce in the Internet world, resulting in the loss of trust and use of the Internet [9]. This threat has led to the development of a large number of techniques for the detection and filtering of phishing emails.

The many approaches proposed in the literature to filter phishing emails, may be classified according to the different stages of the attack flow, e.g. network level protection, authentication, client side tool, user education, server side filters and classifiers, etc. We discuss the advantages and limitation of these approaches. This survey gives an organized guide to the present state of the literature, in view of the wide scope of approaches. In the literature, the evaluation and comparison of different approaches on phishing email filtering are given a great deal of attention. This survey not only identifies and categorizes these methods, but also compares and analyzes their relative merits. For example, it lists strengths, weaknesses, and the related application scenarios for guiding the readers to design new anti-phishing detection methods in the future. This paper is not intended to cover related topics, such as spam, on which numerous studies have already been carried out. Phishing email is a different problem and, thus, needs more specific attention.

Section 2 of the paper contains a background and overview of the phishing emails. Section 3 describes proposed approaches against phishing attack. Section 4 presents the summaries and Section 5 concludes the paper.

II. Background and Overview of Phishing Emails

In this section, we discuss types of phishing attacks, the life cycle of phishing email, email-analyzing methods, phishing email evaluation methods, features to detect phishing email, and feature selection and extraction methods. In brief, we discuss zero-day phishing email attacks, and then compare this survey with existing work.

A. Various types of phishing attacks

Phishing is a particular type of spam that employs two techniques, deceptive phishing and malware-based phishing. The first technique is related to social engineering schemes, which depend on forged email claims that appear to originate from a legitimate company or bank. Subsequently, through an embedded link within the email, the phisher attempts to redirect users to fake Websites. These fake Web sites are designed to fraudulently obtain financial data (usernames, passwords, credit card numbers, and personal information) from victims. The second technique involves technical subterfuge schemes that rely on malicious code or malware after users click on a

Manuscript received February 3, 2012; revised July 9, 2012 and December 16, 2012.

A. Almomani is with National Advanced IPv6 Centre (NAV6), Universiti Sains Malaysia (USM), Malaysia (e-mail:ammarali@nav6.usm.my).

B. B. Gupta is with RSCOE, University of Pune, India (e-mail:gupta.brij@gmail.com).

S. Atawneh is with Universiti Sains Malaysia (USM), Malaysia (e-mail:satawneh@yahoo.com).

A. Meulenberg is with Universiti Sains Malaysia (USM), Malaysia (e-mail:mules333@gmail.com).

E. Almomani is with Universiti Sains Malaysia (USM), Malaysia (e-mail:eman19830@yahoo.com).

Digital Object Identifier 10.1109/SURV.2013.030713.00020

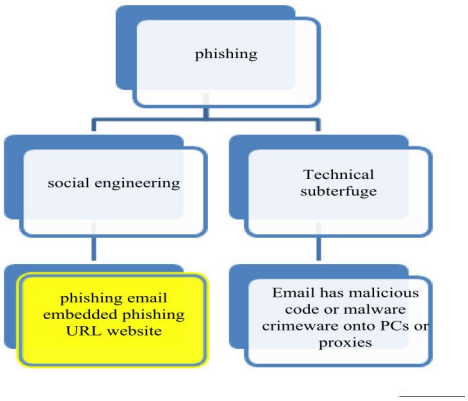

Fig. 1. Types of phishing attacks

link embedded in the email, or by detecting and using security holes in the user's computer to obtain the victim's online account information directly. Sometimes, phisher attempts to misdirect the user to a fake Web site or to a legitimate one monitored by proxies [1]. In this paper, our focus is on deceptive phishing using social engineering schemes, as it is one of the popular ways to steal victim's information by phishing. Figure 1 explains the various types of phishing attack.

B. Life cycle of phishing email

The current research focuses only on detecting phishing attacks based on emails. The phishing life cycle, as shown in figure 2, typically begins with a mass emailing that attempts to convince the reader to visit an included link in the email. This phase of phishing is much like fishing. Instead of using a fishing lure and line to catch a fish, a phisher sends out many emails in hopes that a few readers will 'bite' at the email lure by visiting the included link in the email. Typically the email looks legitimate and will include a company logo of a popular financial institution and a return address of the legitimate company. The link in the email, the 'look' will also appear legitimate at first glance. The phisher wants the lure to appear so authentic that the victim will "bite" without thinking.

Phishing emails originating from phishing Web sites have a very short life span. The Anti-phishing working group (APWG) collects and archives samples of phishing attacks. It also focuses on identifying the identity of the attacker, and any fraud resulting from phishing attacks, crime-ware, or email spoofing [10]. One example of a phishing attack is reported on March 9, 2004 when a victim received an email (Figure 3) allegedly originating from eBay [11]. This email claimed that the user's account information is allegedly invalid and must be corrected as shown.

This email had an embedded URL that appears to originate from a Web page on eBay's Website (Figure 4). This 'poisoned' Web page asked the user to enter his/her credit card number, contact information, and Social Security Number, along with the eBay username and password. The phishing email claimed to be a legitimate email from eBay. The source (appearing in the "From:" header) was S-Harbor@eBay.com, which refers to a legitimate email id of eBay Inc. Moreover, this Website appears to have a direct link to eBay.com by constantly using an encrypted channel ("https:"). Consequently, the user performed an action by clicking on the embedded URL, which was expected to direct him to eBay.com. However, the user was transferred to a different and fraudulent Website at IP address 210.93.131.250, but, this address was from Seoul, South Korea. It had no relationship with eBay.

Figure 5 shows the procedure of phishing email transfer in a computer network. It contains three components: a Message Transfer Agent (MTA), Message Delivery Agents (MDA), and a Mail User Agent (MUA).

Message Transfer Agent (MTA) is responsible for sending and receiving mail between systems using SMTP.

Message Delivery Agents (MDA) are responsible for receiving a message from an MTA and arranging for it to be received by the local system (e.g. delivered to a mailbox).

Mail User Agent (MUA) is the program that an end user uses to read and process mail. Typical examples include Microsoft outlook, Pegasus, exmh, mutt, Eudora, etc.

Therefore, as shown in Figure 5, phisher can send a phishing message to a potential victim and victim may open the phishing email.

C. Phishing email classification methods

Filtering can be defined as the automatic classification of messages into phishing and legitimate email. The process of classifying new messages is Carrie out by the phishing email filter. It can analyze messages to classify them either separately (e.g. just checking the email for presence of certain distinct words, in case of keyword filtering), or through a learning-based filter which analyses a collection of labeled training data (pre-collected messages with upright judgments), and so on [12]. An email message consists of two parts: header(s) and body. Email headers consist of a structured set of fields, such as, From, To, Subject, etc. In an email, the body is always preceded by header lines that identify particular routing information of the message, including the sender, recipient, date and subject. Email body is the part that we always see as it is the actual content of the message contained in the email. Taxonomy of email message structure is presented in Figure 6. Along with an example (Figure 7) to indicate the basis for feature selection and extraction.

D. Phishing email evaluation methods

Suppose that N_h denotes the total number of ham emails, ($n_h \rightarrow$H) is the number of ham emails classified as ham, ($n_h \rightarrow$P) is the number of ham emails misclassified as phishing, N_P denotes the total number of phishing emails, (np$\rightarrow$H) is the number of phishing emails misclassified as ham, and (np$\rightarrow$P) is the number of phishing emails classified as phishing emails. Performance of phishing email detection system can be evaluated in the following manner [14-16]:

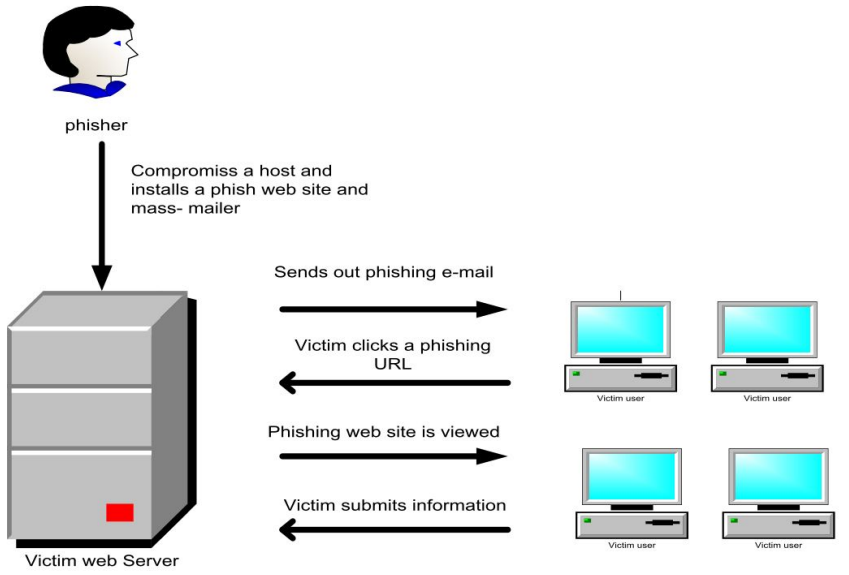

Fig. 2. Life cycle of phishing email.

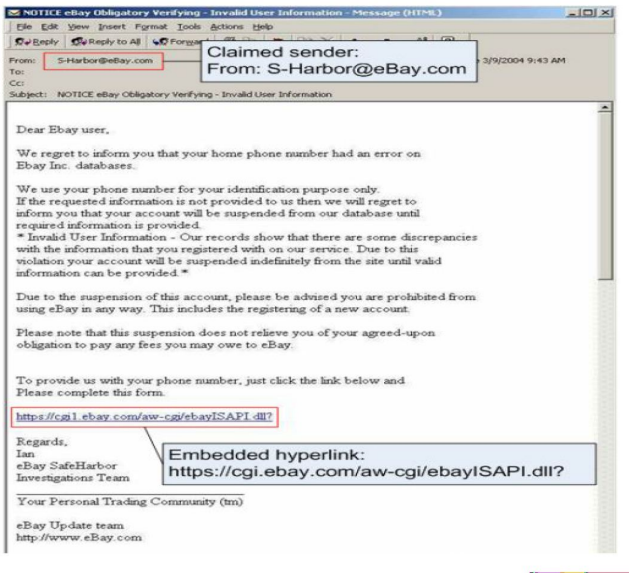

Fig. 3. Screenshot of the eBay phishing email [11]

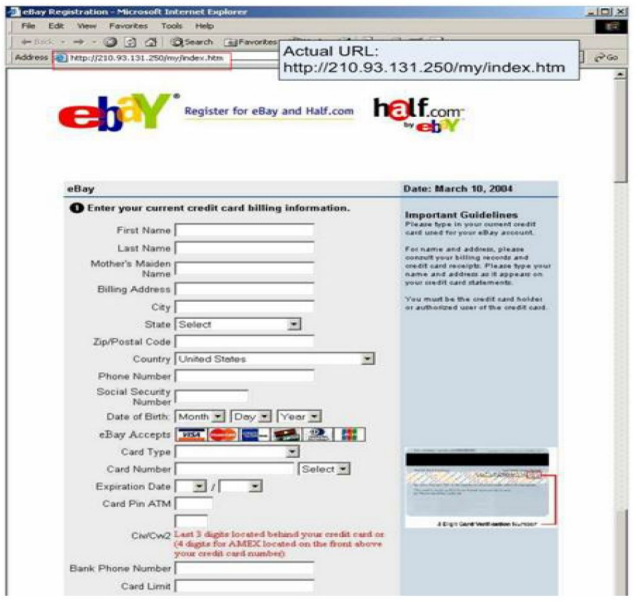

Fig. 4. Screenshot of embedded URL on the eBay phishing web page [11]

a. True Positive (TP): The number of phishing email correctly classified as phishing:

$$TP = \frac{np \rightarrow p}{Np} \tag{1}$$

b. True Negative (TN): The number of ham emails correctly classified as ham:

$$TN = \frac{nh \rightarrow h}{Nh} \tag{2}$$

c. False positive (FP): The number of ham email wrongly classified as phishing:

$$FP = \frac{nh \rightarrow p}{Nh} \tag{3}$$

d. False Negative (FN): The number of phishing emails wrongly classified as ham:

$$FN = \frac{nh \rightarrow h}{Np} \tag{4}$$

Various measures used in the literature for classification of phishing and ham email are presented in Table 1.

E. Features for phishing email detection

One of the strategies of phishing emails is to attract victims and direct them to a particular phishing Website. The phishing email asks the user to reveal confidential data using an email structure with embedded URL. In a related vein, there are

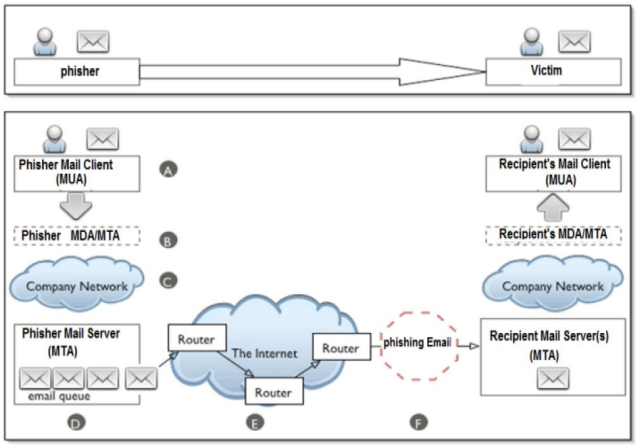

Fig. 5. Phishing email transfer procedure in the computer network

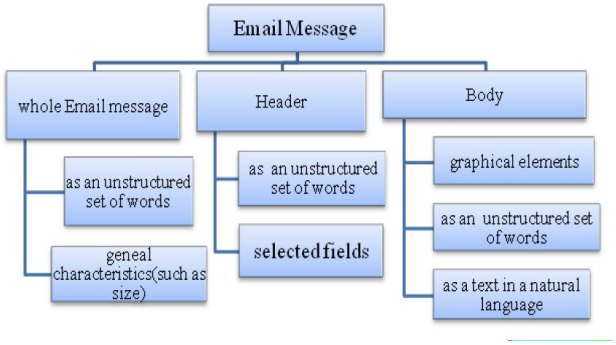

Fig. 6. Taxonomy of email message structure[13]

several sets of features to detect phishing email that are proposed in [22] and classified into three sets: basic features [22, 23], latent topic model features [14, 22, 24], and dynamic Markov chain features[22-24].

1) Basic features: Basic features are those that can be directly extracted from an email without thorough processing. Basic features can be categorized as follows:

- Structural features: Structural features can be extracted from an HTML tree, which explains the structure of email body such as the MIME standard that explains the message format number. These features include discrete and composite body parts with the number of alternative body parts.
- Link features: Link features represent different features of URL links embedded in an email, such as the number of links with IP, number of deceptive links (URL visible to the user), number of links behind an image, number of dots in a link and, so on.
- Element features: Element features represent the type of Web technology used in an email such as HTML, scripting, particular JavaScript, and other forms.
- Spam filter features: A Spam feature in general has two Boolean values (0, 1). Most of researchers use the Spam Assassin (S.A.) tool [25], which has more than 50 features to determine whether an email is classified as spam or not. By default, a message is considered as spam, if it scores more than 5.0 [26].
- Word list features: A list of words may possibly characterize a phishing email which can be classified by Boolean features, whether the words occur in the email or not. Word stems such as account, update, confirm, verify, secure, log, click, and so on [22] .

TABLE I
MEASURES USED FOR CLASSIFICATION OF PHISHING AND HAM EMAILS

Measure	Formula	Meaning
precision	$= \frac{\|TP\|}{\|TP\| + \|FP\|}$	The percentage of positive predictions that are correct
Recall Sensitivity	$= \frac{\|TP\|}{\|TP\| + \|FN\|}$	The percentage of positive labeled instances that were predicted as positive
Accuracy	$= \frac{\|TP\| + \|TN\|}{\|TP\| + \|TN\| + \|FP\| + \|FN\|}$	The percentage of correct predictions
F-Measure	$= 2 \cdot \frac{precision \cdot recall}{precision + recall}$	A measure of a test's accuracy. It considers both the precision and the recall of the test to compute the score
Total cost ratio	$= \frac{n_P \to H + n_P \to P}{\lambda \cdot n_H \to P + \lambda \cdot n_P \to H}$	λ is the relative cost of the two types of error [13, 17]
Weighted Error (W Err)	$= \frac{\lambda \cdot n_H \to H + n_P \to P}{\lambda \cdot N_H \to N_P}$	According to a specified weight λ [17]
Root Mean Square Error (RMSE)	$RMSE = \sqrt{\sum_{i=1}^{N} \frac{(y_i - \hat{y_i})^2}{N}}$	Where n is the number of emails input samples, yi is the ith actual output, yi the ith framework output,RMSE = 0 means that model output exactly matches the observed output [18]
The non dimensional error index (NDEI)	$NDEI = \frac{RMSE}{std(y(t))}$	The ratio of the root mean square error (RMSE) · It divides the standard deviation of the target data std (y (t)) [18]
ROC Curve	True positive rate plotted against false positive rate	
Objective Function	The summation of distance between all features vector and cluster center [19]	

2) Latent topic model features: Topic model features are unobservable "latent" features. It uses clusters of words that are likely to appear together in email. These features expect that in a phishing email, the words "click" and "account" often appear together. Additionally, in normal financial emails, the words "market", "plan", and "prices" can appear together [14] [22, 27].

3) Dynamic Markov Chain Features: Dynamic Markov chain features are text-based features based on the bag-of-words, which models the "language" of each class of messages, thereby capturing the probability of emails belonging

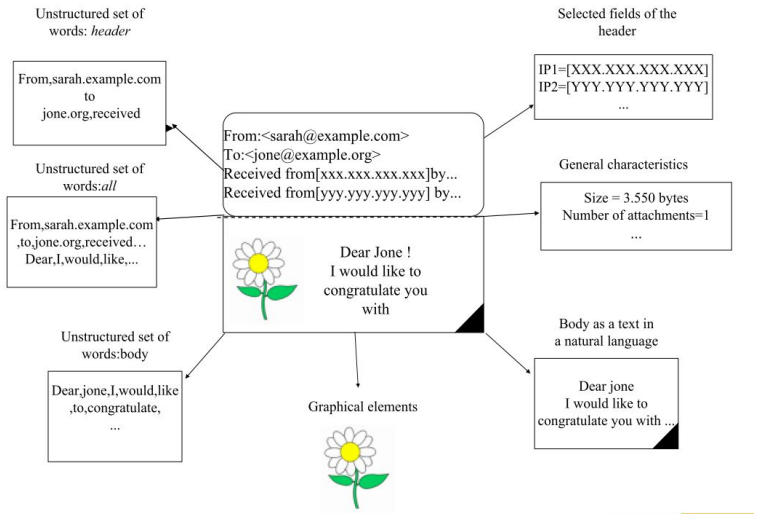

Fig. 7. An example of message structure for the purpose of feature

TABLE II
METHODS TO MEASURE THE EFFECTIVENESS, AND RANK OF FEATURES

Measure	Formula
Document frequency	$\|\{ m_j \| m_i \in \text{M and } f_i \text{ occurs in } m_j \}\|$
Information gain	$\sum_{c\in\{c_{phishingemail},Cham\}} \sum_{f\in\{fi,\neg fi\}}^{n} \hat{p}(f,c)\log\frac{\hat{p}(f,c)}{\hat{p}(f)\cdot\hat{p}(c)}$

to a specific class. These emails can be generated as basis for data analysis. For a new message, these features can compute its likelihood to belong to the different classes (e.g. phishing or ham email classes) [22-24]. However, the description of 47 phishing classification features with its evaluation can be found in [17, 28-30].

F. Features selection and extraction

Many algorithms are used to select and measure the effectiveness of the identification? Features and many methods are used for feature extraction.

The two algorithms that are most used to measure the effectiveness of features and ranking them are presented in Table 2 [13].

Where M is the set of all training message, $c_{phishingemail}$ and c_{ham} are the labels of phishing and ham email classes, respectively. f_i is a binary feature (such as "the word *click* present in the message"), and $\neg f_i$ is the negation of the feature fi (such as "the word *click* NOT present in the message"). All the probabilities are measure and estimated with frequencies.

Bag-of-word model is mostly used for feature extraction. In this model, a text (such as a sentence or a document) is represented as an unordered collection of words, disregarding grammar and even word order. This model can be adopted to characterize the whole message or any part of a message. Most algorithms depend on binary classification and some algorithms calculate the occurrences of the same word in different parts of the email message. For example, based on the number of occurrences of the tokens in the message, the model can be used as the weight of this token.

G. Zero-day phishing emails

Zero-day phishing e-mail is a new phishing email that has not been trained on the old data samples and not caught by existing filters. Similarly, zero-day attack is one that anti-phishing or spamming email tools mount using hosts that do not appear in blacklists [20, 21].

H. Comparison of this survey with existing work

To best of authors' knowledge, this paper is the first comprehensive survey focusing on phishing email analysis and its defense. A summary, comparing this paper with existing work [31, 32] is presented in the table 3.

III. CLASSIFICATION OF PROTECTION APPROACHES AGAINST PHISHING ATTACKS

Many approaches against phishing attacks have been proposed in the literature. Five defense areas are classified according to their position in the attack flow (Figure 8).Other components in the data flow, such as Simple Mail Transfer Protocol (SMTP) and IMAP server's protocols, are Internet standards for the (e-mail) transmission across Internet Protocol (IP). These protection approaches against phishing attacks are discussed below:

A. Network level protection

Network level protection is usually implemented by not allowing a range of IP addresses or a set of domains from entering the network. It allows a website administrator to block messages from those systems that usually send spam or phishing email. 'Domain name system blacklists' [34], used by

TABLE III
SUMMARY COMPARISON OF THIS SURVEY WITH EXISTING WORK

		This Work	Related Work	
			Zhang et al. [32]	Zhang et al. [32]
Scope	Network level protection	√		
	Authentication	√		
	Client side tool	√		√
	User education	√		√
	Server side filters and classifiers	√	√	
Surveyed Approaches	Comparison and evaluation	√		√
	Analysis of each techniques	√		
	Attack detection	√	√	
	Vulnerability identification	√	√	√
	Attack protection	√		

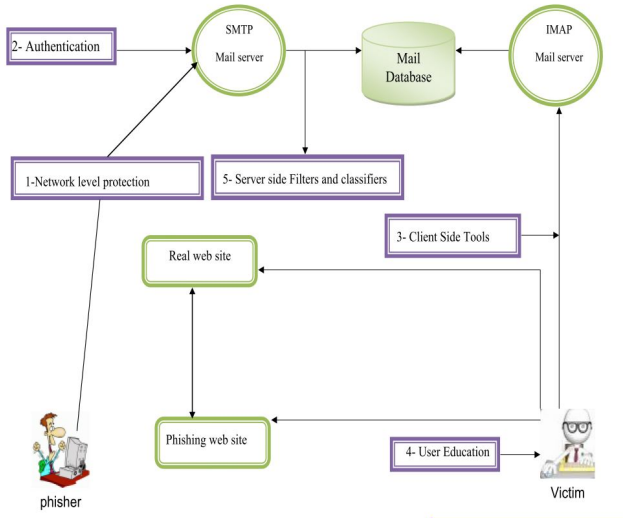

Fig. 8. Approaches to protect the user from phishing attack [33]

Internet service providers (ISP's) is generated and updated by studying traffic behavior. This approach is reactive in nature. An attacker or phisher can evade this protection technique by controlling legitimate user's PCs or by continuously changing IP addresses.

Snort [35][33] is open source software also employed at the network level. Rules in Snort are constantly updated to maintain protection.

Comparison of the two phishing attack detection tools at the network level is presented in Table 4.

Kim and Huh [36] compared the performance of four different classification algorithms to detect DNS-poisoning-based phishing attacks by collecting the routing information over a one week period. They have observed that a 'k-nearest neighbor' algorithm performed best among all the classification methods explored in the study. It had a false positive rate of about 0.7%, and a true positive rate of about 99.4%.

TABLE IV
PHISHING ATTACK DETECTION TOOLS AT THE NETWORK LEVEL

Tool	**Description**	**Advantages**	**Disadvantages**
Domain name system blacklists [34]	Database used by Internet service providers	An updated list of offending addresses	- Phisher can easily evade this protection technique
Snort [33]	Heuristic/rule engine	Good at detecting level attacks	-Rules require manual adjustments - Does not look at content of message

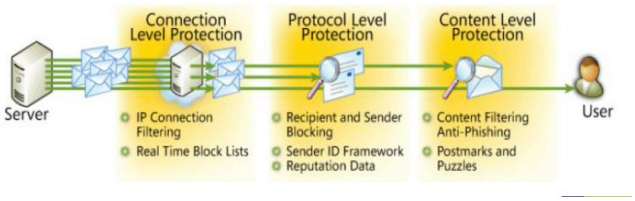

Fig. 9. Microsoft's Sender ID integration into an anti-phishing solution [39]

B. Authentication

Authentication-based approaches to filter phishing email are designed to confirm whether the email was sent by a valid path and the domain name is not being spoofed by phisher. Authentication increases the security of communication, at both the user and domain levels. User level authentication is employed by password as credentials. However, password authentication can easily be broken as evidenced by increasing phishing attacks. Domain level authentication is implemented on the provider side (e.g. from one mail server to another). Microsoft has introduced a new technology called Sender ID [37] for domain level authentication (Figure 9). A similar technology called Domain Key [38] is produced by Yahoo. However, for domain level authentication to be effective, providers on both the sender and the receiver side must employ the same technology,[33].

Other techniques are implemented in email authentication by sending the hash of the password with the domain name using digital signature and password hashing. Institutions would establish a policy whereby all high-value email communications with customers are digitally signed with an authorized private key. Upon receipt of the email, the recipient would verify the authenticity of the email using the institution's public key. There is extremely low probability that a phisher could create a valid signature on fraudulent email. PGP and S/MIME are examples of digital signature technologies. Several authors have recommended key distribution and digital signature to detect phishing email. However, at present, most users do not use email authentication [40].

TABLE V
SUMMARY OF NETWORK- AND ENCRYPTION-BASED APPROACHES

Approach	Strength	Weakness	Used in
Authentication based on user and domain level	-Increases the security of communication	- Both sender and receiver side must employ the same technology	ID [37], Domain Key [38]
Email authentication by digital signature and password hashing	-Less complexity -No need of cooperation bet ween email domains	-At present, most users do not use email authentication	Hotmail, Yahoo, Gmail [43]
Transaction Authentication Numbers (TANs)	-Less complexity -No need of cooperation between email domains	-Affected by man-in-the-middle attacks -Requires substantial infrastructure, time and cost	Bank of Austria [44]

Some banks (e.g., Bank Austria) employ user transaction authentication numbers (TANs) for filtering phishing email. The TAN is sent to the user via a short message (SMS) through mobile [41]. However, while reducing the phishing risk, this approach is still subject to man-in-the-middle attacks. The mobile TAN requires substantial infrastructure, time, and cost. Hence, at present, TAN is not appropriate for many communication scenarios, for example, social networks.

To avoid the authentification filter, a phisher can send an offer to a shopping search engine like "Froogle" with a lower price which then directs a stream of visitors to his site [42]. The search engine cannot control such transfers or the payment transactions; therefore, a new approach to filtering the content of emails and Websites is needed. Summary of the network- and encryption-based approaches is presented in the Table 5.

C. Client side tools

Tools that operate on the client side include user profile filters and browser-based toolbars. SpoofGuard [45], NetCraft [46] (shown in FIGURE10), CallingID [47], CloudMark [48], eBay toolbar[49] and IE phishing filter [50] are some of the client side tools. They include a study of phishing and attack by detecting phishing "Web browsers" directly. Other techniques also propose solutions in client side tools which include domain checks, URL examination, page content, algorithms, and community input. These tools, which are designed and trained, using typical prototypes of phishing website URLs, warn the user with a dialog box.

Figure 10 clearly shows information about accessed sites to help us evaluate fraudulent URLs (e.g. the real citibank.com or barclays.co.uk sites are unlikely to be hosted in the former Soviet Union). Usually, these tools also depend on black-listing and white-listing, which is a technique used to prevent phishing attacks by checking Web addresses embedded in emails or by checking the website directly. In the Mozilla Firefox browser, each Web page selected by a user is tested against a blacklist of well-known phishing Websites [5, 51, 52].

TABLE VI
SUMMARY OF BLACK-LISTING AND WHITE-LISTING APPROACHES

Approach	Strength	Weakness	Used in
White-listing	Accepts legitimate email only	high false positive	IE, Mozilla Firefox browsers [56, 57]
Black-listing	Good with well-known phishing Web sites	high false negatives	IE, Mozilla Firefox browsers [56, 57]

In the black-listing process, a list of the detected phishing Websites is automatically downloaded to the user machine with updates at standard intervals. Generally, sites receive a "blacklist" classification by search engines or users. For example, Google analyzes websites to ascertain their danger and then publishes results to the public. Similarly, users can flag domains they perceive as threats and report them to Google or sites (like Stop Badware.org and CyberTopCops.com [53]). The average threat time of an online phishing Website is three days and sometimes the sites are blacklisted within a few hours. However, this technique does require time for a new phishing Website to be reported and added to the blacklist.

Phishing emails are commonly hosted by the many servers on Botnets that distribute the phishing attacks [54]. Blacklisting can also produce false negatives and miss many phishing emails; therefore, it is not particularly effective. Blacklists are ineffective in protecting users from 'fresh' phishing email, as most of them blocked less than 20% of phish at hour zero [55].

White-listing is a collection of "good" URL compared to outside links in receiving incoming emails. It appears more promising, however, producing a list of trustworthy sources is time-consuming, and it is a huge task. Two problems encountered by this technique are its producing a high number of false positives, allowing phish to get through, and its filtering of ham emails. Therefore, white-listing is not effective enough to be used for detecting phishing attacks.

Black-listing and white-listing techniques (as shown in table 6) are very weak to work with technology changes (like IPV4 versus IPV6, tiny URLs, etc.) [33]. Moreover, most of users do not give attention to the warning dialogs. Due to above mentioned weaknesses; these techniques are not an effective solution to detect zero day attack.

Abu-Nimeh and Nair [58] proposed a new attack using DNS poisoning to bypass the client side security toolbars and phishing filters. Various authors have studied seven toolbars and have shown that none of them were able to detect the attack; therefore, these 'listing' tool approaches are ineffective.

Lin et al. [59] have suggested highlighting the domain name of an address in the address bar, but this approach is unable to detect and prevent phishing attacks at high level. Jain and Richariya [60] have implemented a prototype web browser, which is used to detect phishing URLs by processing each arriving email for phishing attacks. The selection criteria are

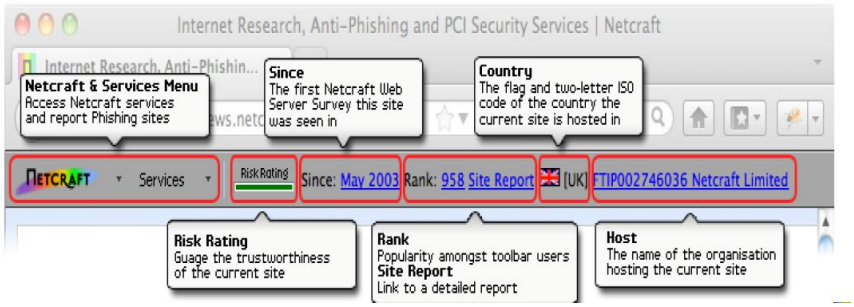

Fig. 10. NetCraft- A Client side tool [46]

based on email data collected over a period of time. However, the authors did not compare their implementation with other browser-based tools. Chen et al. [61] conducted a scientific assessment of user interface design elements (e.g. color, font type, icon type, message placement, etc) which can be used in various tools. They concluded that current tools fail to consider user preferences for displaying dialog of warning and errors. Users prefer personalization and customization of these tools.

D. User education

User education, based on social response approaches, depend on increasing the level of awareness and education about phishing attacks, in general, and about phishing emails, in particular [62-66].

The first approach offers online information about the risks of phishing attacks, and how to keep away from this attack. These materials are frequently published by the governments, non-profit organizations from trading platforms, such as eBay, Amazon, and Bank of America to financial enterprise as shown in Figure11.

The second approach, online training and testing, scores user ability to determine the phishing websites and emails such as 'Phil Game' [32]. A well-known idea from Kumaraguru et al. [67] developed two embedded training designs to teach users about phishing during their regular use of email. After such training, users can detect phishing emails by themselves. The first training system provides a warning along with active items using text and graphics. The second training uses a comic strip format to transmit the same information. The authors also proposed a game-based approach to train users on how to detect phishing email and Websites. The authors tested this technique on a group of users of different ages and found it to increase the level of knowledge about phishing attacks.
The third approach, which is implemented in real world, applies a contextual training method developed by Indiana University [68]. In this approach, a set of phishing emails are frequently sent to users by the researchers to verify the users' feedback and to find out who has been "phishing." Other working approaches on training users are included in [66, 69-72]. However, when phishers produce phishing emails with sufficient critical details, trusting users cannot distinguish them from ham. Comparison of these three approaches is listed in Table 7 [32]. Other working approaches on training users are discussed in [69, 70].

TABLE VII
COMPARISON OF TRAINING METHODS RELATED TO AWARENESS AND EDUCATION

Methods	Authority	Attractive	Impressive
Online Material	√	-	-
Online Test	-	√	√
Contextual Training	-	-	√

E. Server side filters and classifiers

Usually, server side filters, based on content-based filtering approaches, are considered as the best option to fight zero day attacks. Therefore, most researchers try to solve zero day attack from this side [21]. Usually this technique depends on an extracted set of phishing email features. These features are trained on machine-learning algorithms by adaptation to a statistical classifier to distinguish between emails labeled as ham (legitimate) email, or phishing email. After that, this classifier may be used on an email stream to predict the class of newly received emails. However, phishing email identification is different from spam classification. Spammers use the internet as an easy way to contact a huge number of users to inform them about a product. Phishers send a message that has a normal look and appears to originate from some trustworthy companies. Therefore, many techniques used in spam detection cannot be used in phishing email detection. In general, filtering of phishing emails is an application that implements a simple function in the following manner:

$$F(e,\theta) = \begin{cases} C_{phishingemail} & \text{if the email e is considered phishing email} \\ C_{hamemail} & \text{if the email e is considered ham email} \end{cases}$$

Where e is an email to be classified, θ is a vector of Parameters, and $C_{phishingemail}$ and $C_{hamemail}$ are labels assigned to the email messages.
Most phishing emails are filtered based on machine learning classification algorithms. For the learning-based technique, the parameter vector θ is the result of training the classifier on a pre-dataset. $\theta = \theta$ (E),E=(e_1, y_1), (e_2, y_2), . . .(e_n , y_n) , $y_i \in \{C_{phishing}, C_{ham}\}$, Where e_1, e_2 . . . e_n are earlier

Fig. 11. Comic strip presented to people in generic condition [64]

collected email messages, y_1, y_2 . . . y_n are the matching labels, and θ is the training function [13].

In this part, server side filters and classifiers based on machine-learning techniques for phishing email detection are divided into five sub-sections (below). Generally, each has the same techniques, and inherits the same features, but has some differences.

1) Methods based on Bag-of-Words model: This method is a phishing email filter that considers the input data to be a formless set of words that can be implemented either on a portion or on the entire email message. It is based in machine learning classifier algorithms [13, 73, 74]. For a better understanding, suppose that there are two types of messages: phishing email and ham email. Then, suppose we have a set of labeled training email messages with corresponding notes that each label contains a vector of "s" binary features and one of two values $C_{phishingemail}$ or $C_{hamemail}$ based on the class of the message. Consequently, with the training data set E, a message can be pre-processed as follows:

$$U = \{(\bar{u}_1, y_1), (\bar{u}_2, y_2), ..., (\bar{u}_n, y_n)\},$$
$$\bar{u}_i \in Z_2^s \ , \ Y_i \in \{C_{phishing} \ , \ C_{ham}\}$$

Where s is the features number used, the new input sample $\bar{u_i} \in Z_2^s$ is the classifier that provides the basis for classification, $y_i \in \{C_{phishing} \ , \ C_{ham}\}$. Some classifiers and approaches related to this method appear below.

1) *Support vector machine (SVM)* is one of the most commonly used classifier in phishing email detection. In 2006, the SVM classifier was proposed for phishing email filtering [75]. SVM worked based on training email samples and a pre-defined transformation θ: $R^s \rightarrow F$, which builds a map from features to produce a transformed feature space, storing the email samples of the two classes with a hyperplane in the transformed feature space shown in Figure 12. The decision rules

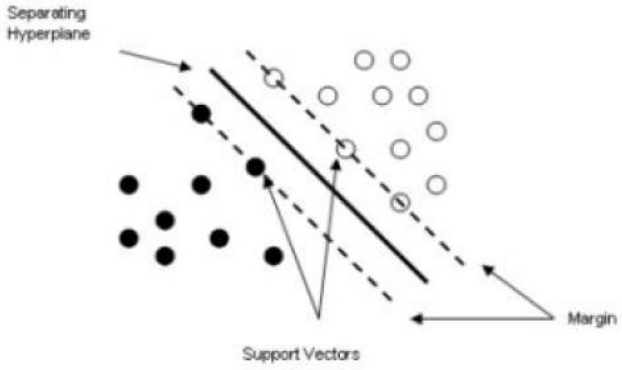

Fig. 12. Support Vector Machine [78]

appear in the following formula.

$$f(\bar{y}) = sign(\sum_{i=1}^{n}(\alpha_i x_i K(\bar{\mathrm{U}}, \bar{\mathrm{Q}}) + S))$$

Where $K(\bar{\mathrm{U}}, \bar{\mathrm{Q}}) = \theta(\bar{\mathrm{U}}).\theta(\bar{\mathrm{Q}})$, is the kernel function and αi, i = 1 …n and S maximizes margin space separate between hyperplane. The value -1 corresponds to $C_{legitemate}$ and 1 corresponds to $C_{phishing}$. SVM was proposed in particular to classify the vectors of features extracted from images [76].

2) *k-Nearest Neighbor(k-NN)* is a classifier proposed for phishing email filtering by Gansterer [77]. Using this classifier, the decision is made as follows: based on *k*-nearest training input, samples are chosen using a pre-defined similarity function; after that, the email x is labeled as belonging to the same class as the bulk among this set of k samples (Figure 13).

3) *Naive bays classifiers* are a simple probabilistic classifier, which works based on Bayes' theorem with powerful "naive" independence assumptions Ganger [90]. This classifier, used in text classification, can be a

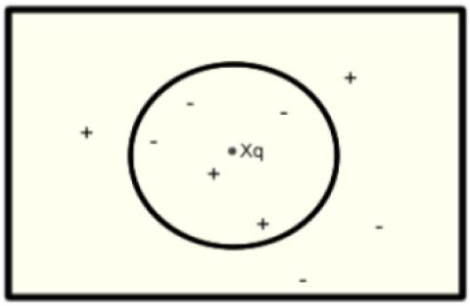

Fig. 13. K-Nearest Neighbour Algorithm [16]

learning-based variant of keyword filtering. To ensure preciseness, all features are statistically independent. The main decision rule can be explained as follows:

$$F(x)=argmax_{x=C_{phishingemail},C_{hamemail}} 7y(\hat{h}(y)\pi_{j:y^j=1} \hat{h}(y^j = 1 \mid y))$$

Where y^j is the j^{th} component of the vector $\bar{Y}$, $\hat{h}(y)$ and $\hat{h}(y^j = 1|y))$ are probabilities estimated using the training data. Naive Bayes is extremely popular and has practical software solutions [79].

4) *Boosting:* a boosting algorithm combines many hypotheses like "One-level decision trees." The main idea of this algorithm [80] depends on sequential adjustments at each phase of the classification process where a fragile (not very accurate) learner is trained. The output results of each phase are used to reweigh the data for future stages. The larger weight is assigned to the input samples that are misclassified.

5) *Term frequency-inverse document frequency (TF- IDF)* is used by Dazeley [81] for word weights, as features for the clustering. The document frequency of the word w is implemented by DF(w) which is defined as the number of email messages in the collected data set where the word w appears in the document at least once as shown in the formula [81].

$$W_{xy} = TF_{xy} \cdot \log x \frac{s}{DFi}$$

Where W_{xy} is the weight of x_{th} Word in the y_{th} document (email), TF_{xy} is the occurrences number of the x_{th} word (w) in the y_{th} document (email), DF_x is the number of email messages in which the i_{th} word (w) occurs, and S, as above, is the total number of messages in the training dataset.

Bag-of-Words model has many limitations. It is implemented with a large number of features, consumes memory and time, and mostly works with a supervised learning algorithm. Furthermore, it is not effective with zero day attack.

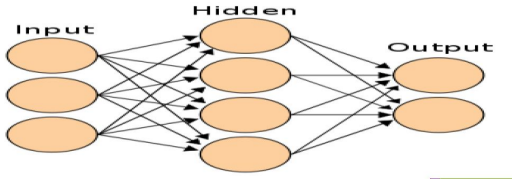

Fig. 14. Neural network

TABLE VIII
FALSE POSITIVE (FP) RATE AND FALSE NEGATIVE (FN) RATE FOR ALL SIX CLASSIFIERS

Classifiers	FP	FN
LR	04.89%	17.04%
CART	07.68%	12.93%
SVM	07.92%	17.26%
NNet	05.85%	21.72%
BART	05.82%	18.92%
RF	08.29%	11.12%

2) Multi Classifiers Algorithms: These approaches in general depend on comparison between sets of classifiers. Presently, more and more research has used new classifier algorithms like Random Forests (RF). RFs are classifiers which merge several tree predictors, where each tree depends on the values of a random Vector sampled separately, and can handle large numbers of variables in a data set. Another algorithm, Logistic Regression (LR), is one of the most widely used statistical models in several fields for binary data prediction [78]. It used because of its simplicity. Neural Networks (NNet) classifiers, which consist of three layers (input layer, hidden layer, and output layer), gains the requisite knowledge by training the system with both the input and output of the preferred problem. The network is refined until results have reached acceptable accuracy levels as shown in Figure 14. The power of NNet comes from the nonlinearity of the hidden neuron layers. Nonlinearity is important for the network learning of complex mappings. Sigmoid function is the commonly-used function in neural networks [78].

Some approaches based on the last algorithms related to phishing emails filtering appear below:

Abu-Nimeh et al. [78] compared six classifiers relating to machine learning technique for phishing prediction, namely, Bayesian Additive Regression Trees (BART), LR [82] SVM, RF, NNet, and Classification and Regression Trees (CART). He used 43 features for training and testing of the six classifiers in the data set; but the results indicated that there is no standard classifier for phishing email prediction. For example, if some classifiers have low levels of FP, they will have a high level of FN. LR whose FP is 04.9%, obtained a large number of FN at17%. The result of this technique is shown in Table 8.

Miyamoto et al. [83] performed a comparison of machine learning algorithms to detect phishing websites based on 3,000 website data. The highest observed F-measure is 85% in the case of AdaBoost. Later on, Toolan and Carthy [16] introduced an approach to classify emails based on the C5.0 algorithm. In this approach, authors have obtained an F-measure of 99.3% using a generally available dataset consisting of 8,000 samples.

Abu-Nimeh et al. [84] developed a method to detect phishing e-mail based on Bayesian Additive Regression Trees (BART) algorithm. BART algorithm improved their predictive accuracy compared with earlier work.

Ram Basnet [85] proposed a technique that works based on 16 features and has the ability to discover phishing email attacks with very limited prior knowledge. This technique adapted many machine learning algorithms to classify emails into phishing or legitimate emails. The author adapted SVM, Biased SVM, Leave One Model Out, NNet, and Self Organizing Maps (SOMs) [86]. Most of the previous algorithms were supervised learning based. Some authors have used an unsupervised algorithm implemented by SOMs. SOMs are based on analysis that can be prepared via a visualization technique called the U-matrix. Its accuracy was 90.8% based on 4,000 samples (50% legitimate; 50% phishing emails). After using all of the available techniques, the best algorithm was Biased SVM. Both Biased SVM and NNet share the same accuracy at 97.99%. However, this paper has the same machine-learning techniques which are used by other authors. NNet manifests a problem in retaining useful learning information for the future[87].

Gansterer et al. [77] made comparisons between binary (spam vs. not spam) and ternary classification approaches (ham, spam, and phishing). Some authors have used 30 features, 15 of which are taken from other researchers and 15 "online and offline" features are created by them for filtering phishing email. The results show that the new features increase the accuracy of classification with ternary classification. The accuracy reached up to 97% by adapting a support vector machine (SVM). However this technique needs large mail servers [77] and suffers from higher cost because access to the online features is based on the status of the internet connection. The extraction of too many online features may affect performance and scalability of the e-mail filtering system, especially in large-scale business e-mail servers. A summary of some multi classifiers algorithm approaches is presented in the table 9.

3) Classifiers model based features: These approaches build full models that are able to create new features with many adaptive algorithms and classifiers to produce the final results[88]. Some of the approaches appear below.

Structural features is proposed by Chandrasekaran et al. [75]. The prototype implementation sits between user's mail transfer agent (MTA) and the mail user agent (MUA). They applied simulated annealing as an algorithm for feature selection. Phishing email classifications are used in three categories. First: a number of style maker features were extracted from emails, such as the total number of words divided by the number of characters. Second: structural attributes, such as the formation of greetings implemented in the email body. Third: the frequency distribution of some selected function words such as "click." After selecting the features, they evaluate these features using Support Vector Machine (SVM) classifiers and reported an accuracy of 95%. However, the result of this technique was based on a small size dataset.

Training Smart Screen phishing filter by "Microsoft," uses the feedback data of more than 300,000 hotmail users [89]. This technique is based on the extraction of more than 100,000 email attributes using a learning algorithm based on Bayesian statistics. The expert team of Microsoft adapted the latest spamming and phishing techniques. However, after testing the technique via internet explorer, the best score of recall was 89% without false positives [90].

TABLE IX
SUMMARY OF MULTI CLASSIFIERS ALGORITHMS APPROACHES

Authors	Contribution Summary	Weakness	Mechanism	Algorithms
Abu-Nimeh et al. [84]	Prove that there is no standard classifier for phishing email prediction	More features consume more time and memory	Compared six classifiers relating to machine learning	LR, CART, SVM, NNET, BART, RF
Miyamoto et al. [83]	Comparison of machine learning algorithms to detect phishing	The observed f - measure is still low	Detect phishing website based on 3,000 website data	AdaBoost
Ram Basnet 2008 [85]	Discover phishing email attacks with very narrow prior knowledge	Using offline algorithms, it has a low level of accuracy	Compared multiple Classifiers algorithms and a clustering technique with 16 features	Adapted SVM, NNet, SOMs and NNet
Ganster et al. [77]	Established 15 new online and offline features	Higher cost because of online features	Make Comparisons between binary and ternary classification approaches	SVM

Semantic ontology concept with adaptive Naive Bayes algorithm was proposed by Bazarganigilani [42] as a new algorithm for text classification of phishing emails using a heuristic way to detect the phishing emails. The author suggests each word as an attribute and the frequency of the word represents the value. This is called the Ontology Concept to solve the problem of synonymous words; fourth step: Term Frequency Variance (TFV) [91] and Information Gain (IG) are ranking features. This model works in 5 steps as shown in Figure15. The author used 600 emails (200 as phishing email). The accuracy reached up to 94.87%. However, the size of dataset is not sufficient to fully characterize the proposed concept. Furthermore, the author depends on a single aspect of features called ontology, while many techniques to attack phishing emails used multiple aspects of features. As a result, the system cannot determine and the level of accuracy is low compared with other techniques.

PHONEY : Mimicking user response was proposed by Chandrasekaran et al. [92] as a novel approach. This technique detects phishing email attacks using sham

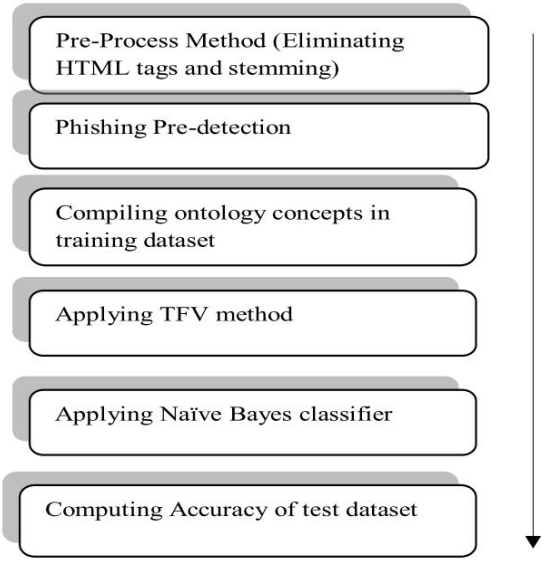

Fig. 15. Five steps in Ontology Concept proposed method [42].

responses which mimic real users, basically, reversing the character of the victim and the enemy. The PHONEY technique is installed between a user's MTA and MUA and processes all arriving emails to prevent phishing attacks. The PHONEY analyzes the incoming email contents for embedded links or attached HTML forms. Thereafter, the control is passed to the content scanner which receives the Web page for analysis, then, extracts the data from the Web page. The extracted data are compared against the entries in hash DB including all information such as password or username. The hash DB has two fields representing the token names along with their fake values. The PHONEY technique was tested and evaluated for only 20 different phishing emails over eight months. It was found that the collected data are too small to address a big problem like phishing emails. This technique requires time to reverse the characters of the victim and the phisher as shown in Figure 16.

PILFERS is a proposed method to detect phishing emails by Fette et al. [93]. This technique is based on 10 different features representing phishing emails. Nine features are extracted from the email itself, while the tenth feature represents the age of linked-to-domain names. This last can be extracted from a WHOIS query at the time the email is received [94]. The S.A. tool [25], was used to identify if this email has spam features or not. This latter technique is based on a 10-fold cross-validation with random forest and SVM as classifiers to train and test the dataset. They tested 860 phishing emails and 6,950 legitimate emails. 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.

Bergholz et al. [14] has trained a classifier by features obtained from a dynamic markov chain and class-topic models. The proposed model is able to study the statistical

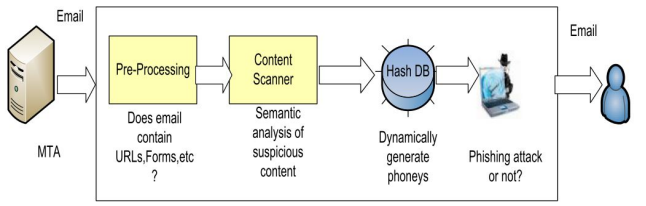

Fig. 16. Block diagram of PHONEY architecture [92]

filtering of phishing emails and train with the characteristic features of emails based on classifiers to identify new phishing emails with different content. The authors proposed new features trained by machine-learning techniques using chains algorithm with novel latent class-topic models as shown in Figure 17. First, extract a total of 27 basic features. These features include four structural features (such as the total number of body parts), eight link features (such as the total number of links), four element features (such as HTML or JavaScript code), two spam-filter features (such as Spamassassin Boolean results: spam or ham), nine word list features (such as nine-word stems: account, update, confirm, verify, secure, notify, log, click, inconvenient). Second, features extracted by dynamic markov chain depended on the likelihood of capturing a message belonging to a specific class. Third, 50 latent topic model features (clusters of words appear together in emails). Applying this algorithm on many of the phishing email features and by studying the contents of the original emails, this model was able to reduce the memory consumed compared with other research.

The authors have obtained results better than did the PILFER technique on the same dataset and proved the effectiveness of selected topic features. Furthermore, this model is developed in a real-life environment at a commercial ISP [95]. However, this technique selects a big number of features, about 81, and it has many algorithms for classification, which means it is time-consuming and, in the analytical process, a large number of dynamic Markov chain suffers from high memory requirement.

Robust classfier model is proposed by Ma Ofoghi et al. [96]. This model can detect phishing emails by hybrid features based on information-gain algorithms. The authors used seven features selected after ranking many features by the information-gain algorithm. These features represent the more powerful features in his study and include links, total number of invisible links, non-matching URLs, forms, scripts, and 'body blacklist' words. The authors used email presentation based on converting all features to numerical values on a different range. For example, the "number of invisible links" may be under five, while a body blacklist should contain hundreds of words. The values of features are normalized, before the classification process, and are limited to the range [0, 1].

To detect phishing emails, the authors proposed five stages: first, a feature generator including the seven features

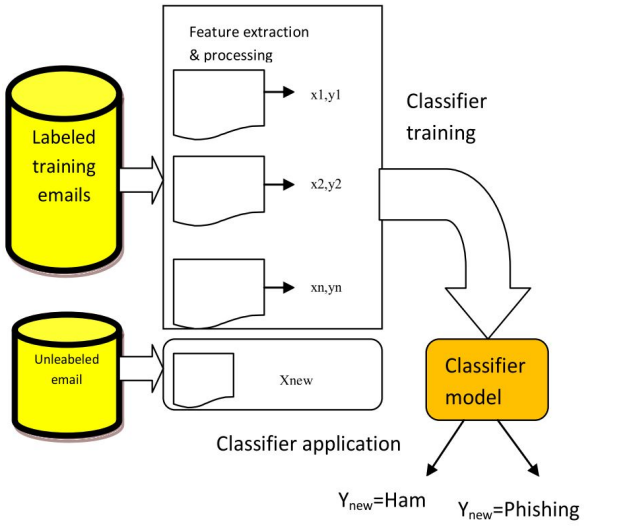

Fig. 17. The machine learning approach [14]

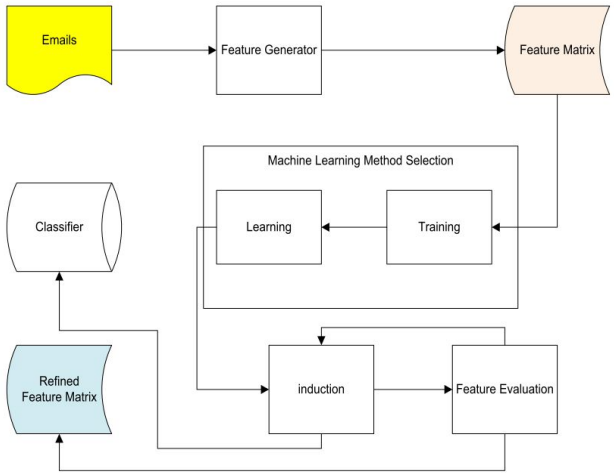

Fig. 18. Robust classifier model architecture for phishing email detection [96]

mentioned above; second: machine learning method selection by an adaptive five-machine learning algorithm; three: information gain is created by induction; four: feature evaluation selects a smaller vector space of features; and finally, a refined feature matrix to optimize feature sets (Figure 18). The accuracy of the short feature data result was best when using a decision tree algorithm for small vector space with four of the seven features. It attained an accuracy of 99.8%. However, the authors depend on a few features only, which mean several phishing attacks used other features.

The data set used by the authors related to live emails received by Westpac only; this set is not used by other authors and is not benchmarked. There is no fixed aspect of this technique because the ranking features change depending on the email streaming. Other researchers used hybrid features [97].

TABLE X
CLASSIFIERS MODELS-BASED FEATURES APPROACHES

Authors	Contribution Summary	Weakness	Mechanism	Algorithms
Chandra sekaran et al. [75]	Structural features	-Small size dataset, 200 emails only -Time consuming	The prototype implemen-tation sits between (MTA) and (MUA)	Support Vector Machine (SVM) classifiers
Ganger et al. [90]	Training Smart Screen	-Low level of recall measure-ment, -Working with fix number of features	Uses the feedback data from the Users of Microsoft	Bayesian statistics 100,000 email attributes
Bazargani gilani [42]	Semantic ontology concept , text classification of phishing emails using a heuristic way	-Level of accuracy is low compared with other techniques	Model works in 5 steps as shown in FIGURE5	Semantic ontology concept by (TFV) method Informa-tion Gain (IG), Nave Bayes algorithm classifies
Chandra sekaran , Chinchani et al.[92]	PHONEY: mimicking user response	-Collected data are so small a size,-Time consuming	PHONEY technique is installed between a user's MTA and MUA	PHONEY: Mimicking user response
Fette, Sadeh et al. [98]	PILFERS prototypes	-Sizeable number of phishing and ham emails was not well classified.	10 different features included WHOIS query	Random forest and support vector machine (SVMs) as a classifiers
Bergholz et al.[14]	Study the statistical filtering of the phishing emails	-Large number of features, -Time consuming - High memory require-ment	Trained a classifier by features obtained based on Dynamic Markov Chain and Class-Topic Models	Dynamic Markov Chain and Class-Topic Models
Ma, Ofoghi et al. [96]	Robust clas-sifier model	-Using a few numbers of features ,- Non standard dataset	7 hybrid fea-tures,model consist of five stages appear in FIG-URE13	Information gain algo-rithms,decision tree algorithm, C4.5

Comparison of classifiers model-based features is shown in the table 10.

4) Clustering of phishing email: Clustering is the process of defining data grouped together according to similarity. It is usually an unsupervised machine learning algorithm. This

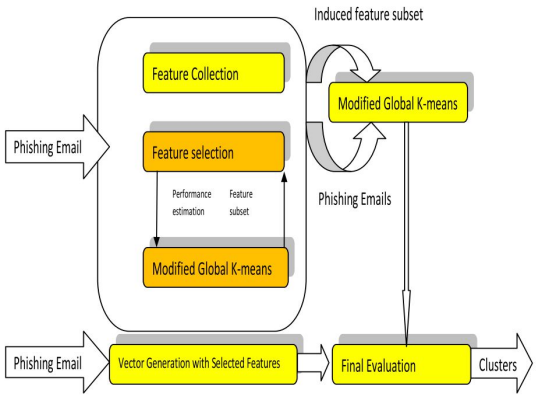

Fig. 19. Feature selection using modified global k-mean [19]

group of machine-learning techniques depends on filtering phishing emails based on clustering emails via online or offline mode. One of the most used clustering techniques is k-means clustering. K-means clustering is an offline and unsupervised algorithm that begins by determining cluster k as the assumed center of this cluster. Any random email object or features vector can be selected as initial center then the process continues:

determine the centre coordinate; determine the distance of each email object (vector) to the centre group of email objects based on a minimum distance [85].

Some approaches related with this technique appear below.

cluster phishing emails automatically proposed by Ma et al. [19] based on orthographic features that include HTML features, size of document, text content, and other elements. This is achieved by eliminating redundant features at the same time. The system collects the possible features based on examination with adaptive k-means clustering algorithm to produce the objective function values (the summation of distance between all features vector and cluster center) over a range of acceptance values across many feature subsets. The best cluster detected by the final value that determines the distribution of the objective function values is shown in Figure 19. The authors tested 2,048 emails from an Australian bank over five months, without any knowledge about the emails. Results are the efficiency of the automatic feature selection process and strong indication of correct clusters. However, this technique suffers from general emails with unknown features. The relationship between cluster value and objective function values has been explored further. So, this is not enough most especially since a k-means algorithm works offline only.

Consensus Clustering proposed by Dazeley et al. [81] depends on a combined method of unsupervised clustering algorithms and supervised classification algorithms. First, use independent clustering to randomize data. Second, build a Consensus Clustering by combining the independent clusters.

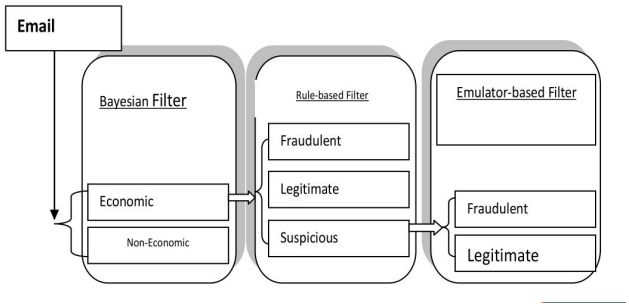

Fig. 20. FRALEC Email Classification Flow model [102]

TABLE XI
SUMMARY OF CLUSTERING APPROACHES

Authors	Contribution Summary	Weakness	Mechanism	Algorithms
Ma, Yearwood et al. [19]	cluster phishing emails automatically	-k-means algorithm works via offline technique only	13 orthographic features, produce the objective function values, clustering email	K-means clustering algorithm
Dazeley, Yearwood et al. [81]	Consensus Clustering Model	-Level of accuracy is still less than 94%	combined method of unsupervised clustering algorithms and supervised classification algorithms	TF-IDF, GKM, MSKM, NN, CSPA To build Consensus Clustering(CMSNN)

Third, train the data by Consensus Clustering, and finally, use the supervised classification algorithms to classify all clustered data. This system adapted many algorithms, including: Term Frequency Inverse Document Frequency (TF-IDF) word weights, Global k-Means algorithm (GKM) [99], Multiple Start k-Means algorithm (MSKM)[100], and Nearest Neighbor clustering (NN) . It then discovered an optimal consensus among versatile clustering by *Consensus Aggregation algorithm* again to build a full model called Consensus Multiple Start Nearest Neighbor clustering algorithm (CMSNN). This technique increased the speed of classification and improved accuracy relative to the k-means algorithm. However, because of the large number of algorithms used, the system's performance is affected and the level of accuracy is still less than 94%. Summary of clustering approaches is given in Table 11.

5) Multi-layered system: These approaches work based on combining different algorithms of classifiers working together to enhance results. Some of the authors' approaches appear below.

FRALEC is a hybrid system proposed by Castillo et al. [102] to classify e-mails into two classes, ham email and phishing email. This system consists of three filters: first,

Nave Bayes classifier which examines the textual content of e-mails to assign them to economic (legitimate) or non-economic (phishing) categories. Second, a rule-based classifier separates the non-grammatical features of emails into three categories: fraudulent, legitimate, and suspicious. Third, an emulator-based classifier-filter of virtual accesses, classifies the responses from URL Web sites referenced by hyper links enclosed in emails. The emulator filter works on two rules The first rule: the email is assigned to the fraud class if the body of an economic email includes forms. The second rule: the email is assigned to the legitimate class category if the body of an economic email does not include forms, links, or images (Figure 20). The author used 1,038 emails (10 emails as legitimate and 1,028 as phishing emails). The precision in the best result was 96%. However, from the data set, the number of legitimate emails viewed is not enough to give us clear results. This technique consumes time because it has to go through many layers before it can give us the final decision.

Multi-tier classification is a method using three classifiers proposed by, Islam et al. [103][101]. He suggests that his multi-tier method of classifying phishing emails has the best arrangement in the classification process. In his method, phishing email features are extracted and classified in a sequential fashion by an adaptive multi-tier classifier while the outputs are sent to the decision classifier process as shown in Figure 21, where c1, c2, and c3 are classifiers in three tiers. If the message is misclassified by any of the tiers of the classifiers, the third tier will make the final decision in the process. The best result came from c1 (SVM), c2 (AdaBoost), and c3 (Naive Bayes) adaptive algorithm. The average accuracy of the three tiers was 97%. However, this technique is characterized by lengthy processing times and complexity of analysis since it requires many stages. Furthermore, 3% of its test data set still was misclassified.

Profiling of phishing e-mail is a new method proposed by Yearwood et al. [80]. The authors concentrated on embedded hyperlink information by extracting structural features and WHOIS information [94] to extract 12 features representing phishing emails. Classifier algorithm SVM and a boosting algorithm were then used to generate multi-label class predictions, scheduled on three datasets formed from embedded hyperlink information in phishing emails. The classes generated are hacked site, hosted site, and legitimate site. In addition, authors tested 2,038 real emails with four-fold cross-validation. Results show that profiling can be done with quite high accuracy using hyperlink information. PhishGILLNET proposed by Ramanathan [33], is a multi-layered approach to detect phishing attacks using a system based on natural language processing and machine learning techniques that utilizes three algorithms in three layers. These algorithms are as follows: Probabilistic Latent Semantic Analysis (PLSA), which is used to build a topic model; AdaBoost, which is used to build a robust classifier; and Co-Training, which is used to build a classifier from labeled and unlabeled examples. Using this multi-layered approach, Ramanathan got a 97.7% result. However, this technique used 47 complex features that require significant processing and take more memory and computation time. Therefore, this approach is ineffective with real-world applications. Table 12 is a summary of hybrid system approaches.

TABLE XII
SUMMARY OF HYBRID SYSTEM APPROACHES

Authors	Contribution Summary	Weakness	Mechanism	Algorithms
Castillo, Iglesias et al. [51]	FRALEC model-consists of three classifiers	-Simple legitimate dataset, -consumes time	Integrated with three classifiers	Nave Bayes classifier ,rule-based classifier, Emulator-Based classifier Nave Bayes classifier ,rule-based classifier, Emulator-Based classifier
Islam, Abawajy et al. [103]	Multi-tier classification	- complexity of analysis	Three tier classification, third tier will make the final decision	(SVM), AdaBoost and Naive Bayes classifier.
Yearwood, Mammadov et al. [80]	profiling of phishing e-mail	-Using hyperlinks features only	12 binary features, WHOIS information, using Classifier algorithm to generate multi-label class	SVM and boosting algorithm
Ramanathan [33]	PhishGILLNET	Take more memory and computation time	multi-layered approach to detect phishing attacks	PLSA, AdaBoost, Co-Training algorithm

6) Evolving Connectionist System (ECOS): Evolving Connectionist System is an architecture that simplifies the evolution processes using knowledge discovery. It can be a neural network or a set of networks that run continuously and change their structure and functionality through a continuous relationship with the environment and with other systems. This system, like traditional expert systems, works with unfixed number of rules used to develop the artificial intelligence (AI) [104]. It is flexible with respect to the dynamic rule, works on either online or offline mode, and interacts dynamically with the changing environment. Such a system can solve the complexity and changeability of many real world problems. It grows throughout the process and adopts many techniques. ECOS has the following characteristics. It evolves in an open space, not fixed dimensions. This system is able to work online and with incremental, fast learning - possibly through data propagation in memory when data are passed. ECOS, in a life-long learning mode, learns as an individual system, as well as part of an evolutionary population of such systems, It has evolving structures using constructive learning and learns

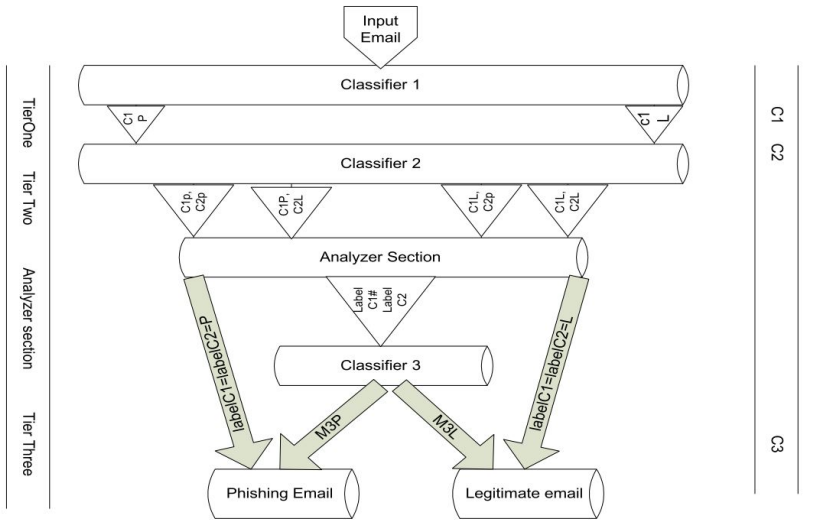

Fig. 21. Block diagram of the multi-tier classification model[103]

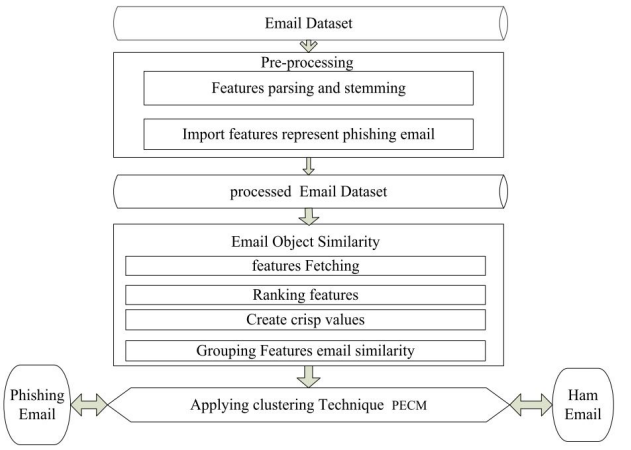

Fig. 22. Working of Phishing Email Clustering Approach (PECM)

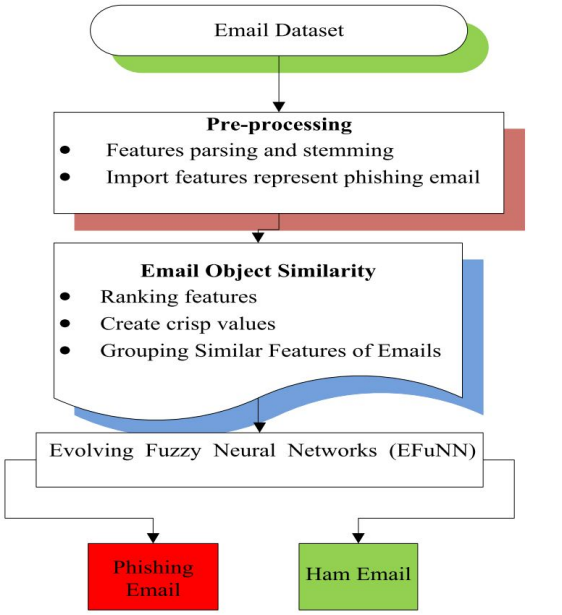

Fig. 23. Working of PENFF

locally via local partitioning from the problem space that allows fast adaptation and process tracing over time. This process simplifies demonstration and extraction of different kinds of knowledge, be it generally-memory-based, statistical, or symbolic knowledge [87, 105]. Some approaches to phishing email filtering, based on ECOS, appear below. A novel approach, proposed by ALmomani et al. [106] has used ECMC (Evolving Clustering Method for Classification) to build a new model called the Phishing Evolving Clustering Method (PECM). PECM functions are based on the level of similarity between two groups of features of phishing e-mails. PECM model is highly effective in terms of classifying e-mails into phishing e-mails or ham e-mails in online mode without consuming too much memory. It has speed because it uses a one-pass algorithm. It increases the level of accuracy to 99.7%. The PECM approach is diagrammed in Figure 22.

Detection and prediction of zero day phishing emails is provided by a new framework called Phishing Evolving Neural Fuzzy Framework (PENFF) [18] that is based on adoptive Evolving Fuzzy Neural Network (EFuNN) [107]. As a performance indicator, values of the Root Mean Square Error (RMSE) and Non-Dimensional Error Index (NDEI) are 0.12 and 0.21, respectively. This is a very low error rate compared to other approaches. Working of PENFF is indicated in Figure 23.

PDENFF proposed by ALmomani et al. [108, 112], is a novel framework that adapts the ”evolving connectionist system.” PDENFF is trained by offline learning to dynamically detect zero day phishing e-mails. Its framework is designed for high-speed ”life-long” learning with low memory footprint and complexity. Nevertheless, it provides an absolute

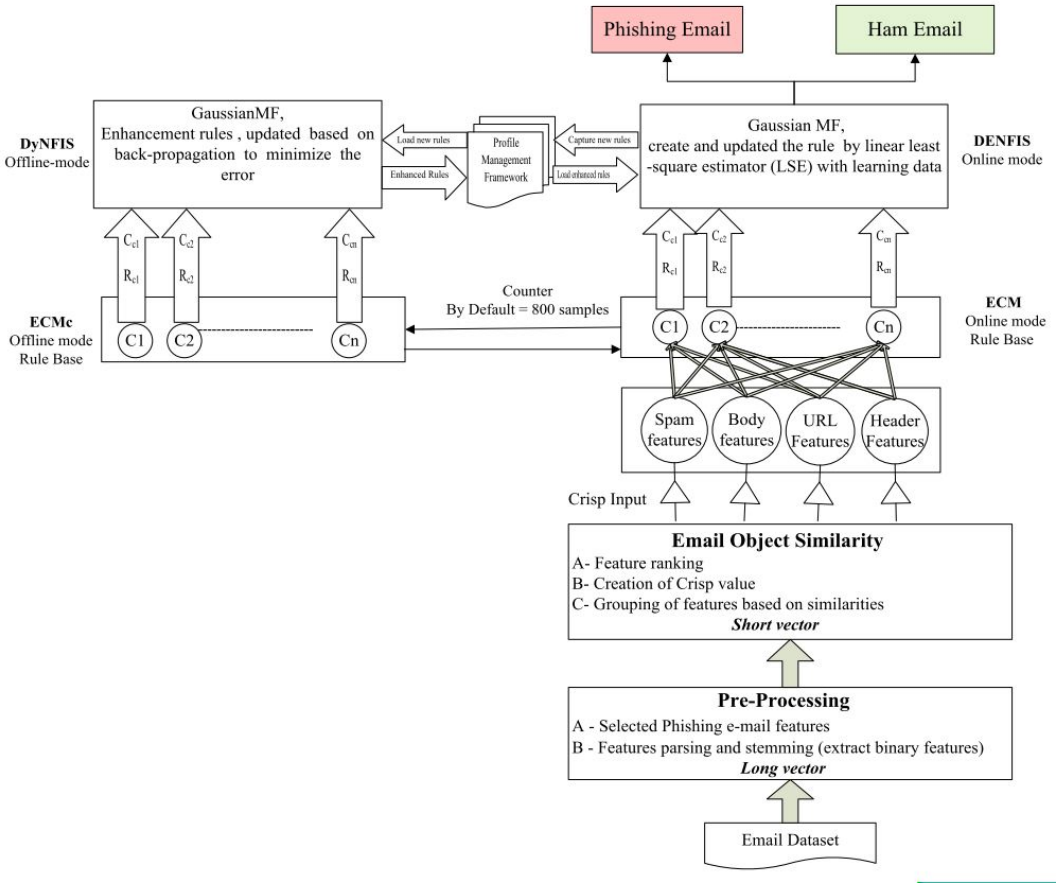

Fig. 24. Working of PDENFF

improvement of between 3% and 13% compared with prior solutions to zero-day phishing e-mail attacks. Workings of the PDENFF framework is shown in Figure 24.

Summary of evolving connectionist system approaches is presented in table 13.

7) Summary comparison of server-side filters and classifiers for phishing email filtering: Comparison of various server-side filters and classifiers techniques explored in this paper is discussed and presented in Table 14.

TABLE XIII
SUMMARY OF EVOLVING CONNECTIONIST SYSTEM APPROACHES

Authors	Contribution	Weakness	Mechanism	Algorithms
AlMomani et al. [106]	-PECM ,-with foot print consume memory-high speed	-Need continuous feeding	Similarity between two groups of features of phishing e-mails	ECMC
ALmomani et al. [18]	PENFF to predict dynamically the zero day phishing e-mails	-Need continuous feeding	adoptive Evolving Fuzzy Neural Network (EFuNN)	EFuNN
ALmomani et al.[108]	PDENFF to detect and predict dynamically the zero day phishing e-mails	-Need continuous feeding	Adaptive four algorithms from Evolving Connec-tionist System (ECOS)	ECM,ECMc,[109] DENFIS [110],DyN-FIS [111],

IV. SUMMARIES AND DISCUSSIONS

Our focus in this paper is a comprehensive survey on phishing email attacks and its solutions. Current protection techniques are unsuccessful in stopping phishing attacks, particularly zero day attack. Summaries of, and comments on various protection measures explored made from the literature survey include:

- **Network level protection:** Based on domain and IP address blacklisting, it needs updating from time to time. As it is reactive in nature, it can be updated only after pattern of abuse have been observed for some period. However, attackers can compromise legitimate user's machine to prepare phishing attack so that blacklisting may prevent legitimate user from using the Website.
- **Authentication techniques:** These operate at two levels. User level authentication, employing a password as credentials, can simply be broken as evidenced by increasingly successful phishing attacks. Domain level authentication provided by both sender and recipient

TABLE XIV
COMPARISON BETWEEN SERVER SIDE FILTERS AND CLASSIFIERS TECHNIQUES FOR PHISHING EMAILS DETECTION

No	Technique used	Advantages	Disadvantages
1	Methods based on Bag-of-Words model	-Builds good scanner between user's mail transfer Agent (MTA) and mail user agent (MUA)	- huge number of features -consumes memory -mostly working with supervised learning algorithm- fixed rules - weak detection of zero-day attack
2	Compared multi Classifiers algorithms	-Provide clear idea about the effective level of each classifier on phishing email	-Non standard classifier - mostly working with supervised learning -weak in detecting zero-day attack
3	Classifiers Model-Based Features	- High level of accuracy - create new type of features like Markov features	-huge number of features -many algorithm for classification → time consuming - higher cost -need large mail server and memory
4	Clustering of Phishing Email	-Fast in classification process	-Less accuracy because it depends on unsupervised learning - need feed continuously
5	Multi-layered system	-High level of accuracy by taking advantage of many classifiers	-Time consuming: technique has many layers working sequentially to produce final result
6	Evolving Connectionist System (ECOS)	-fast and less consumption of memory,- high accuracy,- Evolving with time,-online working,- strong in detecting zero day attack	-Need feed continuously

side. Because of lack of agreement between mail service providers, this technology is not that prevalent.

- **Client side tools and filters:** These bring the Internet user closer to the phishing attack. If the users do not pay attention to warning dialogs, they end up falling for phishing attacks.
- **User education:** Useful, but not enough. Phishers can produce phishing emails with sufficient detail that trusting users cannot distinguish them from legitimate email.
- **Server-side filters and classifiers:** These show many weak points in the use of feature sets that cannot adapt to technology changes. The results include too many misclassifications and the classifiers do not consider intentionally misspelled, conjoined, and disjointed words. Hence, attackers can make clever changes in the text based on different adaptive words, so that these filters often fail to detect phishing emails.

V. CONCLUSIONS

Phishing email is currently amongst the latest and most problematic of trends in network security threats. It is a means of obtaining confidential information through fraudulent emails that appear to be legitimate. We have presented 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. Approaches given in the literature still have much limitation on accuracy or performance, especially with zero day phishing email attack.

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. Many algorithms have been adopted, but still there is no standard technique able to stop phishing attacks in general, or zero day phishing email in particular. Moreover, most of the work is done offline. This requires data collection, data analysis, and profile-creation phases to be completed first. Offline approaches are generally 'reactive' in nature. This means that if changes are made in phishing email features, all the phases need to be repeated in order to adapt. The time lag imposed by such adaptation introduces a gap in the protection against phishing email. Thus, there is still a need for new approaches that, in an online mode, can solve the limitations associated with zero day phishing email detection and prediction.

ACKNOWLEDGMENT

This research is supported by National Advanced IPv6 Centre of Excellence (NAV6), Universiti Sains Malaysia (USM), Malaysia. Authors would like to thanks anonymous reviewers for their valuable suggestions and reviews.

REFERENCES

[1] APWG. Phishing Activity Trends Report, 2010.$Available$: $http$: $//anti-phishing.org/reports/apwg_trends_report_q2_2012.pdf$.
[2] J. S. Downs, et al., "Behavioral response to phishing risk," *presented at the Proc. anti-phishing working groups 2nd annual eCrime researchers summit, ACM Conf, Pittsburgh, Pennsylvania,* 2007,pp. 37-44.
[3] M. Aburrous, et al., "Intelligent phishing website detection system using fuzzy techniques," *IEEE Conf, Damascus, Syria. ,* 2008, pp. 1-6.
[4] M. Aburrous, et al., "Predicting Phishing Websites Using Classification Mining Techniques with Experimental Case Studies," *in Seventh International Conference on Information Technology, IEEE Conf ,Las Vegas, Nevada, USA,* 2010, pp. 176-181.
[5] J. Chen and C. Guo, "Online detection and prevention of phishing attacks," in in Proc. Fifth Mexican International Conference in Computer Science, IEEE Conf, 2006, pp. 1-7.
[6] GARTNER."Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks", December 17,2007, available:http://www.gartner.com/it/page.jsp?id=565125
[7] f. t. commission." National Data Deter Detect. Defend. Avoid ID Theft",2009,available: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html
[8] IID, "eCrime Trends Report,", vol.1, 2011,available: http://www.internetidentity.com/images/stories/docs/ecrime_trends_report-q1-2011_by_iid.pdf
[9] J. J. O. Christine E. Drake, and Eugene J. and Koontz:, "Anatomy of a Phishing Email," in First Conference on Email and Anti-Spam (CEAS),Mountain View, CA, USA, 2004.
[10] A.P. W. Group, "APWG Phishing Trends Reports Phishing Attack Trends Report - 2H 2010," Jul 31, 2011.
[11] A.P. W. Group, "eBay - NOTICE eBay obligatory verifying - Invalid user information," March 2004.

[12] P. Resnick.RFC 5322 - Internet Message Format, 2008,Available: http://tools.ietf.org/html/rfc5322

[13] E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, vol. 29, Mar, 2008 ,pp. 63-92.

[14] A. Bergholz, et al., "Improved phishing detection using model-based features," in Proc. Conference on Email and Anti-Spam (CEAS). Mountain View Conf, CA, aug 2008.

[15] H. Husna, et al., "Behavior analysis of spam botnets," in Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on, 2008, pp. 246-253.

[16] F. Toolan and J. Carthy, "Phishing detection using classifier ensembles," in eCrime Researchers Summit, IEEE Conf, Tacoma, WA, USA, 2009, pp. 1-9.

[17] M. Khonji, et al., "A study of feature subset evaluators and feature subset searching methods for phishing classification," presented at the Proc. 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, ACM Conf, Perth, Australia, 2011.

[18] A. Almomani, et al.,"Evolving Fuzzy Neural Network for Phishing Emails Detection," Journal of Computer Science, vol. 8,no.7, 2012 ,pp. 1099-1107.

[19] L. Ma, et al., "Establishing phishing provenance using orthographic features," IEEE Conf, 2009,pp. 1-10,

[20] D. L. Cook, et al., "Phishwish: a simple and stateless phishing filter," Security and Communication Networks, vol. 2,no.1, 2009, pp. 29-43.

[21] M. Khonji, et al., "Enhancing Phishing E-Mail Classifiers: A Lexical URL Analysis Approach," , International Journal for Information Security Research (IJISR),vol.2,no.1/2, March/June 2012

[22] A. Bergholz, et al., "New filtering approaches for phishing email," Journal of computer security, vol. 18,no.1,2010, pp. 7-35

[23] J. Singh, "Detection of Phishing e-mail," IJCST, vol. 2,no.1, 2011.

[24] X. Gu and H. Wang, "Online anomaly prediction for robust cluster systems," IEEE Conf , 2009, pp. 1000-1011.

[25] pop3proxy. "SpamAssassin for Win32",2010 Available: http://sourceforge.net/projects/sawin32/

[26] C. McGregor, "Controlling spam with SpamAssassin," Linux J, vol. 153,no.1, 2007.

[27] G. L'Huillier, et al., "Latent semantic analysis and keyword extraction for phishing classification," in Intelligence and Security Informatics (ISI), 2010 IEEE International Conference on, 2010, pp. 129-131.

[28] A. J. Mahmoud Khonji, Youssef Iraqi, "A Brief Description of 47 Phishing Classification Features,", 2011.

[29] F. Toolan and J. Carthy, "Feature selection for Spam and Phishing detection," in eCrime Researchers Summit (eCrime), IEEE Conf, Oct. 2010, pp. 1-12.

[30] M. Khonji, et al., "A novel Phishing classification based on URL features," in GCC Conference and Exhibition (GCC), 2011 , IEEE Conf, 2011, pp. 221-224.

[31] A. ALmomani, et al.,"Asurvay of learning-based techniques of phishing email filtering " International Journal of Digital Content Technology and its Applications(JDCTA), vol. 6,no.18, 2012. available: http://www.aicit.org/JDCTA/ppl/JDCTA1772PPL.pdf

[32] S. L. Jianyi Zhang, Zhe Gong,Xi Ouyang,Chaohua Wu,Yang Xin, "Protection Against Phishing Attacks: A Survey," IJACT: International Journal of Advancements in Computing Technology, vol. 3,no.9, 2011, pp. 155-164.

[33] H. W. Venkatesh Ramanathan, " phishGILLNETphishing detection methodologyusing probabilistic latent semantic analysis,AdaBoost, and co-training," EURASIP Journal on Information Security,springer open journal, march,Vol.1, 2012. pp.1-22.

[34] DNSBL. Information Spam Database Lookup. Accessed 28 may 2012,available: http://www.dnsbl.info/

[35] Snort Home Page. Accessed 29 May 2012, available: http://www.snort.org/

[36] H. Kim and J. Huh, "Detecting DNS-poisoning-based phishing attacks from their network performance characteristics," Electronics Letters, vol. 47,no.11, 2011, pp. 656-658.

[37] microsoft, Sender ID ,2008, available:http://www.microsoft.com/

[38] Yahoo, DomainKey Library and Implementor's Tools,accessed 29 may 2012,Available: http://domainkeys.sourceforge.net/

[39] microsoft, "Sender ID Framework Protecting Brands and Enhancing Detection of Spam, Phishing, and Zero-Day Exploits " Awhite paper, february 2008.

[40] B. Adida, et al., "Fighting phishing attacks: A lightweight trust architecture for detecting spoofed emails," 2005.

[41] R. Oppliger, et al., "SSL/TLS Session-Aware User Authentication", Computer,vol.41.no.3,2008,pp.59-65

[42] M. Bazarganigilani, "Phishing E-Mail Detection Using Ontology Concept and Nave Bayes Algorithm," International Journal of Research and Reviews in Computer Science, vol. 2,no.2, 2011.

[43] B. Adida, et al., "Lightweight signatures for email," In Proc. DIMACS Workshop on Theft in E-Commerce, April 2005.

[44] B. Austria.Bank Austria,accessed 11-jun-2012, available:http://www.bankaustria.at/de/privatkunden.html

[45] N. Chou, et al., "Client-side defense against web-based identity theft," in In Proc. 11th Annual Network and Distributed System Security Symposium (NDSS '04), San Diego, CA., 2004.

[46] Netcraft."Netcraft toolbar",2006,Available: http://toolbar.netcraft.com/

[47] CallingID. "Your Protection from Identity Theft, Fraud, Scams and Malware",accessed 29 May 2012,Available:http://www.callingid.com/Default.aspx

[48] CloudMark, accessed 29 may 2012, available: http://www.cloudmark.com/en/products/cloudmark-desktopone/index

[49] e. toolbar. accessed 29 may 2012, available: http://download.cnet.com/eBay-Toolbar/3000-12512_4-10153544.html?tag=contentMain;downloadLinks

[50] I. P. Filter. accessed 29 may 2012, available: http://support.microsoft.com/kb/930168

[51] M. D. d. Castillo, et al., "Detecting phishing e-mails by heterogeneous classification," presented at the Proc. 8th international conference on Intelligent data engineering and automated learning, Springer-Conf, Birmingham, UK, 2007.pp.296-305.

[52] Y. Wu, et al.,"Blocking Foxy Phishing Emails with Historical Information, IEEE Conf. on Communications",Cape Town, may 2010, pp. 1-5.

[53] J. Williams.. Why Is My Site Blacklisted?, 5-jun 2011,Available:http://www.ehow.com/info_12002995_blacklisted.html.

[54] A. Herzberg, "Combining authentication, reputation and classification to make phishing unprofitable," Emerging Challenges for Security, Privacy and Trust, 2009, pp. 13-24.

[55] S. Sheng, et al., "An empirical analysis of phishing blacklists," in Sixth Conference on Email and Anti-Spam,, CEAS, 2009.

[56] moicrosoft. Download Internet Explorer. accessed 26 may 2012,available: http://windows.microsoft.com/en-US/internet-explorer/downloads/ie

[57] firefox."firefox free download".accessed 11-jun 2012,available:http://www.mozilla.org/en-US/firefox/new/

[58] S. Abu-Nimeh and S. Nair, "Bypassing security toolbars and phishing filters via dns poisoning," IEEE Conf, New Orleans, Louisiana, USA,2008, pp. 1-6.

[59] E. Lin, et al., "Does domain highlighting help people identify phishing sites?," ACM Conf, CHI 2011, Vancouver, BC, Canada, 2011, pp. 2075-2084.

[60] A. Jain and V. Richariya, "Implementing a Web Browser with Phishing Detection Techniques," World of Computer Science and Information Technology Journal (WCSIT),vol.1,no.7, 2011, pp.289-291.

[61] Y. Chen, et al., "Interface design elements for anti-phishing systems," in in Proc. of the 6th International Conference on Service-Oriented Perspectives in Design Science Research, Springer Conf, Milwaukee, Wisconsin, USA, 2011, pp. 253-265.

[62] R. C. Dodge, et al., "Phishing for user security awareness," Computers and Security, vol. 26, 2007, pp.73-80.

[63] I. LUNGU and A. TABUSCA, "Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions," Informatica Economica Journal, vol. 14,no.2, 2010,pp.27-36.

[64] P. Kumaraguru, et al., "Lessons from a real world evaluation of anti-phishing training", eCrime Researchers Summit ,IEEE Conf, 2008, pp. 1-12.

[65] F. Aloul, "The Need for Effective Information Security Awareness", International Journal of Intelligent Computing Research (IJICR) , vol.1,no.3, june 2010.

[66] N. A. G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from phishing attacks IEEE International Conference on Information Society,",vol.1, 2011, pp. 485-489.

[67] P. Kumaraguru, et al., "Protecting people from phishing: the design and evaluation of an embedded training email system," *in In Proc. CHI, ACM Conf*, 2007, pp. 905-914.

[68] N. A. J. Tom N. Jagatic, Markus Jakobsson, Filippo Menczer, "Social phishing," Communications of the ACM, vol. 50, 2007, pp. 94-100.

[69] E. Bekkering, et al., "A Follow-up Study of Detecting Phishing Emails",CONISAR, vol.2 2009.pp.1-6

[70] L. A. Werner, "Analysis of an Anti-Phishing Lab Activity " Information systems Education Journal, vol. 8,no.11 2010.

[71] S. S. Tseng, et al., "Automatic content generation for anti-phishing education game," in IEEE International Conference on Electrical and Control Engineering, Yichang, China, 2011, pp. 6390-6394.

[72] T. Moore and R. Clayton, "The impact of public information on phishing attack and defense," Communications and Strategies, vol. 81,2011. pp. 45-68.

[73] R. B. Basnet and A. H. Sung, "Classifying Phishing Emails Using Confidence-Weighted Linear Classifiers, International Conference on Information Security and Artificial Intelligence,Chengdu, China," 2010, pp. 108-112.

[74] B. Biggio, et al., "A survey and experimental evaluation of image spam filtering techniques," Pattern Recognition Letters, 2011.

[75] M. Chandrasekaran, et al., "Phishing email detection based on structural properties", in New York State Cyber Security Conference (NYS) , Albany, NY ," 2006.

[76] O. Chapelle, "Training a support vector machine in the primal," Neural Computation, vol. 19,no.5, 2007,pp. 1155-1178.

[77] W. N. Gansterer, et al., "E-Mail Classification for Phishing Defense," presented at the Proc. 31th European Conference on IR Research on Advances in Information Retrieval, Springer Conf, Toulouse, France, 2009,pp.449-460

[78] S. Abu-Nimeh, et al., "A comparison of machine learning techniques for phishing detection," in Proc. eCrime Researchers Summit,, Pittsburgh, ACM Conf, Pittsburgh, PA,2007, pp. 60-69.

[79] K. P. Murphy, "Naive Bayes classifiers," Technical Report,October,2006,available:http: //www.cs.ubc.ca/ murphyk/Teaching/CS 340 - F all 06 /reading/NB.pdf.

[80] J. Yearwood, et al., "Profiling Phishing Emails Based on Hyperlink Information," in 2010 International Conference on Advances in Social Networks Analysis and Mining,IEEE Conf, Odense, Denmark,aug 2010, pp. 120-127.

[81] R. Dazeley, et al., "Consensus Clustering and Supervised Classi cation for Pro ling Phishing Emails in Internet Commerce Security," in Knowledge Management and Acquisition for Smart Systems and Services, Springer Conf, Berlin Heidelberg, vol. 6232, 2010, pp. 235-246.

[82] K. H. Shih, et al., "Financial Information Fraud Risk Warning for Manufacturing Industry-Using Logistic Regression and Neural Network," Romanian Journal of Economic Forecasting, 2011, pp. 54-71.

[83] D. Miyamoto, et al., "An evaluation of machine learning-based methods for detection of phishing sites," Advances in Neuro-Information Processing,vol.1, 2009, pp. 539-546.

[84] S. Abu-Nimeh, et al., "Distributed phishing detection by applying variable selection using Bayesian additive regression trees, in IEEE International Conference on Communications,vol.1, 2009, pp. 1-5.

[85] S. M. Ram Basnet, and Andrew H. Sung "Detection of Phishing Attacks: A Machine Learning Approach " Studies in Fuzziness and Soft Computing, springer, vol. 226, 2008 ,pp. 373-383

[86] M. Vukovic, et al., "An Intelligent Automatic Hoax Detection System," Knowledge-Based and Intelligent Information and Engineering Systems, 2009, pp. 318-325.

[87] Z. S. H. C. N. Kasabov, Q. Song and D. Greer . Evolving Connectionist Systems with Evolutionary Self-Optimisation 173. springer,vol.173, no.4, 2005.

[88] C. K. Olivo, et al., "Obtaining the Threat Model for E-mail Phishing1," Applied Soft Computing, 2011,pp.1-8.

[89] S. M. Markus Jakobsson, " Phishing and Countermeasures, Microsoft's anti-phishing technologies and tactics," 18 MAY 2007, pp. 551562.

[90] P. R. a. D. L. Ganger, "Gone phishing: Evaluating anti-phishing tools for windows. Technical report, ," September 2006.

[91] T. S. Guzella and W. M. Caminhas, "A review of machine learning approaches to spam filtering," Expert Systems with Applications, vol. 36, 2009, pp. 10206-10222.

[92] M. Chandrasekaran, et al., "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.

[93] I. Fette, et al., "Learning to detect phishing emails," in Proc. 16th International World Wide Web Conference (WWW 2007), ACM Press, Banff, Alberta, Canada, 2007, pp. 649-656.

[94] InterNIC. Whois search, InterNIC - Public information Regarding Internel Domain Name Registration Services., accessed 16-6-2012,Available:http://www.internic.net/whois.html.

[95] A. Bergholz, et al., "A Real-Life Study in Phishing Detection," in Seventh annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference Redmond, CEAS 2010, Washington, US, 2010.

[96] L. Ma, et al., "Detecting phishing emails using hybrid features,"IEEE Conf, 2009, pp. 493-497.

[97] I. A. Hamid and J. Abawajy, "Hybrid Feature Selection for Phishing Email Detection," Algorithms and Architectures for Parallel Processing, 2011, pp. 266-275.

[98] I. Fette, et al., "Learning to detect phishing emails," in Proc. 16th International World Wide Web Conference (WWW 2007), ACM Press, New York, NY, USA, May 2007, pp. 649-656.

[99] A. M. Bagirov, "Modified global k-means algorithm for minimum sum-of-squares clustering problems," Pattern Recognition, vol. 41,no.10, 2008, pp. 3192-3199.

[100] S. A. Elavarasi, et al., "a survey on partition clustering algorithms," International Journal of Enterprise Computing and Business System International Systems,, vol. 1,no.1, 2011,pp.1-13

[101] R. Islam and J. Abawajy, "A Multi-tier Phishing Detection and Filtering Approach", Journal of Network and Computer Applications,2012, In Press

[102] M. del Castillo, et al., "An Integrated Approach to Filtering Phishing E-mailsComputer Aided Systems Theory EUROCAST 2007." vol. 4739, Springer Berlin / Heidelberg, 2007, pp. 321-328.

[103] M. R. Islam, et al., "Multi-tier phishing email classification with an impact of classifier rescheduling," in the International Symposium on Pervasive Systems, Algorithms, and Networks, IEEE Conf, Kaohsiung, Taiwan 2009, pp. 789-793.

[104] L. Benuskova and N. Kasabov, "Evolving Connectionist Systems (ECOS)," in Computational Neurogenetic Modeling, ed: Springer US, 2007, pp. 107-126.

[105] P. P. Angelov, et al., Evolving intelligent systems: methodology and applications vol. 12: Wiley-IEEE Press, 2010.

[106] A. ALmomani, et al., "An Online Model on Evolving Phishing E-mail Detection and Classification Method," journal of applied science, vol. 11,issue.18, 2011, pp. 3301-3307

[107] N. Kasabov, "Evolving fuzzy neural networks-algorithms, applications and biological motivation," Methodologies for the conception, design and application of soft computing, World Scientific, 1998, pp. 271-274.

[108] A. ALmomani, et al., "An enhanced online phishing e-mail detection framework based on evolving connectionist system," International Journal of Innovative Computing, Information and Control (IJICIC), Vol.9, No.3,2013.

[109] Q. Song and N. Kasabov, "ECM- A novel on-line, evolving clustering method and its applications," in Proc. Fifth Biannual Conference on Artificial Neural Networks and Expert Systems (ANNES2001), New Zealand, 2001, pp. 87–92.

[110] N. Kasabov and Q. Song, "DENFIS: dynamic evolving neural-fuzzy inference system and its application for time-series prediction," Fuzzy Systems, IEEE Transactions on, vol. 10, 2002 pp. 144-154.

[111] Y. C. Hwang and Q. Song, "Dynamic neural fuzzy inference system," Advances in Neuro-Information Processing, vol. 5506/2009, 2009 ,pp. 1245-1250.

[112] A. ALmomani, et al., " Phishing Dynamic Evolving Neural Fuzzy Framework for Online Detection Zero-day Phishing Email, ", Indian Journal of Science and technology, vol.6, no.1. 2013.

Ammar Almomani (ammarali@nav6.usm.my) received his Bachelor of Computer Science From Mutah University in 2003 and Master in Computer information system from the Arab Academy in Banking and Financial Sciences (AABFS) in 2005, received PhD degree from National Advanced IPv6 Centre (NAV6) in Universiti Sains Malaysia (USM). In 2013. He has published more than 25 research papers in International Journals and Conferences of high repute. His research interest includes advanced Internet security and monitoring, Maleware detection.

B. B. Gupta (gupta.brij@gmail.com)received PhD degree from Indian Institute of Technology Roorkee, India. Prior to that, he has obtained Bachelor of Engineering degree in Information Technology from the Rajasthan University, Jaipur, India. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada award. He has published more than 40 research papers in International Journals and Conferences of high repute. Dr Gupta is also holding position of editor of various International Journals and magazines of high repute. He also worked as a post doctoral research fellow in University of New Brunswick, Canada. His research interest includes Information security, Cyber Security, Intrusion detection, Computer networks and Phishing.

Samer Atawneh (satawneh@yahoo.com) received his Master degree in Computer Science from University of Jordan in 2003 and a B.Sc in Computer Science from Hashemite University, Jordan in 2001. Currently, Mr. Atawneh is a Ph.D. candidate at the School of Computer Sciences at Universiti Sains Malaysia (USM), Malaysia. His research interests lie in Computer Security and Digital media fields. He has some international publications as journals and conferences' papers.

Andrew Meulenberg (mules333@gmail.com), Jr. earned a B.A. from the University of the South, Sewanee, Tenn. and a Ph.D. in Nuclear Physics from Vanderbilt University, Nashville, Tenn. He spent 27 years at COMSAT Labs (Clarksburg, MD) being responsible for predicting, monitoring, correcting, and preventing space-environmental effects on communications satellites, now Senior Lecturer at Universiti Sains Malaysia (Penang).

Eman Almomani (eman19830@yahoo.com), received her Bachelor of Science in Electrical Engineering, specialized in communication and Electronics Engineering, from Jordan University of science and technology (JUST) in 2006 and and Master in Information Technology-Technopreneurship from Universiti Sains Malaysia (USM) school of computer science in 2013.