Detecting Internet Phishing Attacks Using Data Mining Methods

Marjan Abdeyazdan[1], and Ali Rayat Pisheh[2]

***Abstract*—** Nowadays, the high rate of internet usage among cell phone users has caused many commercial and financial services to be provided through the internet. Despite the fact that internet has provided a functional platform for financial transactions of the users, it can also become challenging and dangerous. Information theft or phishing is a security challenge which is usually carried out by sending spoofed emails and spams. In this type of attacks, attackers usually try to earn the trust of the users by sending deceptive emails in order to direct them towards certain websites which contain spoofed pages for capturing user information. Phishing attacks based on spams are one of the most significant barriers for expanding online financial activities which can cause great losses for financial and credit institutions annually. Assessing the behavior of hackers in sending spam emails and carrying out phishing attacks shows that these attacks follow a particular pattern which is not discernable at the first glance. Discovering the hidden patterns of phishing attacks can be effective in developing software systems for protecting against this type of attacks. Data mining possesses a number of methods for extracting useful information from different unorganized data. This study tries to use a set of data mining tools for analyzing the data from these attacks in order to identify and detect the useful patterns of these attacks. The overall results show that compared to other methods, neural network is more accurate and more sensitive in detecting such attacks**.**

***Keywords*—** Internet Phishing Attacks, phishing, Data Mining, algorithms attacks

I. Introduction

DURING the last decade, the number of internet users has increased on a daily basis. One of the reasons behind this increase is the smartphones which provide fascinating features as well as the ease of accessing the global network. Nowadays, different generations of smartphones are getting more and more popular and widespread and using protocols related to the internet is an integral part of the lives of millions of people around the world [1]. On the other hand, businesses, financial institutions, banks and online shopping websites provide their extensive financial services on the web and the cyberspace. Performing financial transactions on the web has numerous benefits including the reduction in traffic, decrease in air pollution, saving the time and costs and so on. The expansion and spread of the internet have significantly helped expand web-based services. However, despite the benefits of using the web environment for financial transactions and internet purchases, unfortunately a number of users can endanger the financial activities of others and deceive others through phishing attacks to steal their valuable information [2]. As many users use the internet for entertainment, there are others who use the internet to obtain money, take revenge and have fun by making use of their skills and expertise in a destructive fashion. These people are called hackers, crackers, intruders, and so on [3]. Internet security is one of the security branches of computer systems. Stealing information or phishing which is mostly done through tools such as emails is categorized in the web security sphere. Nowadays, using email has become one of the integral parts of our lives so as it is present in different activities such as official, financial, and personal ones [4]. While tools such as email have a lot of functions, they play a significant role in stealing users' information. One of the emails users face almost every day is the spam emails used by phishers or hackers for different purposes such as stealing information, or advertisement. Spams can be considered one of the intrusion tools for deceiving internet users in which the intruder either introduces himself or herself as a prestigious institute or he or she uses different promises such as winning the lottery or any other tricks to direct the users towards spoofed sites so that they give away their user account and financial information. Close analysis of the content of these emails and internet spams indicates that the hackers follow a certain behavioral pattern in writing these emails out whereby the grammatical errors abound or their texts are full of words such as help, winning, visa, and so on. Data and information present in spams and emails sent by phishers provide useful insights for detecting such attacks, close analysis of which can lead to the development of security tools.

Data mining is one of the important methods for extracting hidden patterns and useful information in a huge volume of unorganized data. Data mining includes various techniques for knowledge discovery and extracting useful information such as clustering, classification, decision tree, artificial neural network, Bayesian network, and machine learning [5]. This paper aims to clarify the basic concepts of phishing attacks as well as some of the common techniques of data mining. Afterwards, a number of different data mining methods for detecting and classifying phishing attacks will be discussed and compared. Finally, the conclusions drawn from the study will be presented.

[1]Department of Computer Science, Electericity and Computer college, Mahshahr Branch, Islamic Azad University, Mahshahr, Iran.

[2]Department of Computer Science, Electericity and Computer college, Mahshahr Branch, Islamic Azad University, Mahshahr, Iran.

II. Related Works

[6] proposed a method for detecting phishing attacks based on self-structuring neural networks. In their proposed method, a data set including 17 different features and 1400 instances of legitimate, suspicious, and phishy links were used for detecting links indicating phishing attacks. In their data set, 600 legitimate links and 800 phishy links were used for training the self-structuring neural network. The important features used in their study include the following:

- Using IP address in the URL (e.g. http://91.121.10.211/~chems/webscr/verify)
- Long URL (the characteristic is binary)
- Using the @ character in the URL (the characteristic is binary)
- Using secondary or spoofed addresses in the prefixes or suffixes of the valid URL.
- Using sub-domains in the URL
- Misuse of HTTPS
- Retrieval request from another domain
- Retrieval request for a link outside the URL of anchor
- Server from handler (SFH): if the process is in a different domain, the URL of anchor is suspicious and if there is no process, the URL is a phishing one; otherwise, if the processing server is the same URL, the address is legitimate and valid.
- Abnormal URL: addresses which cannot be referenced in the WHOIS databases
- Redirecting the page: usually, in normal pages there is fewer than two page redirects, while in suspicious pages the redirects are two or three times and in phishing pages, there are more than 4 page redirects.
- Using Popup windows: if the page presents users with popup windows for logging in, it is a phishing page; otherwise, it is a normal one.
- Hiding the suspicious links: in this case, the hacker tries to hide his or her suspicious links using templates such as OnMouseOver events of JavaScript and as soon as the user moves the mouse, he or she will be redirected to that link.
- DNS record: since phishing site have a very short lifespan, these records are usually nowhere to be found.
- Website traffic: usually normal internet pages have a high volume of traffic while the phishing ones don't.
- Age of domain: since phishing pages are detected quickly, they will have a shorter age than the normal pages.
- Disabling right click: in order to prevent reading the source code of the page, phishers disable the right click action.

In the dataset used by the authors, legitimate, suspicious, and phishing addresses are shown by values of 1, 0, and -1, respectively. The results show that the amount of echo in the neural network increases the accuracy of classifying in the proposed method so that for the echo value of 1000, the accuracy of training data reaches 94.07 percent.

[7] used domain information of internet links for detecting phishing pages. One of the benefits provided by their method is the use of domain information for detecting phishing pages considering the fact that this important characteristic is neglected in other anti-phishing methods. In their proposed method, at first all the direct and indirect links to the selected website are extracted. Then, using the source code of the page, all the domains related to direct links are extracted and put in the S1 set. Afterwards, indirect links are extracted and put in the S2 set, then both S1 and S2 are combined and only general and common domains are extracted and finally by using DNS lookup, the IP address of these domains can be extracted. The results of the study show that the accuracy, FP, FN, TN, and TO of the proposed method are 99.62, 0.32, 0.5, 99.5, and 99.67 percent, respectively. Despite benefits such as accuracy and detecting phishing pages in their method, the dependency of their method on other external methods such as DNS lookup and search engines, the efficiency may be impaired.

[8] proposed a new method for detecting phishing attacks using Associative Classification (AC) as a data mining method for classifying data. Using a PHP script, they gathered the information for 601 legitimate sites and 752 phishing sites. They used 16 key features for detecting phishing attacks. They calculated the frequency of each 16 different features in the phishing pages. For instance, the frequency of phishing pages which use IP addresses in the URL is about 20.5 percent.

III. Phishing Attacks

Online phishing has recently entered into the literature of information security. It refers to a technique where hackers send deceiving emails (spams) or use telephone conversations, chat and so on to steal important information such as usernames and passwords of online users. Sending spams and spoofed emails by the hackers has become one of the common methods for stealing sensitive user information. Phishing techniques using spams vary and each day, the number of online phishing multiply. Despite the simplicity, this type of attacks are amazingly very effective and destructive and they are considered one of the recently emerged security threats in the online environment. In the information security information, the word "phishing" is used since this attack is much like fishing; however, in order to signify the concept of deceit for the users, instead of F they use Ph. Phishing means hunting for the user's password using a bait. Online phishing is an instance of social engineering techniques where the intruder uses certain social skills such as polite, official, and emotional sentences and utterances to try to connect with the victim so that through the victim they can access important user information or the information of important institutions in order to use the information for financial gain or destructive purposes. In this method, the hacker tries to earn the trust of the users by sending different messages and posing various questions in order to ask them for important and sensitive information or direct them to a spoofed website which acts as a fishing hook so that the victim enters the sensitive information in that site and the hacker can use that information for his or her destructive purposes [9].

If communication tools such as chat and online forums are not effective for phishing the information, hackers use internet spams to deceive the users and this is their favorite venue. In

this method of attack, the hacker or phisher send multiple emails to internet users impersonating an institution or another trustworthy person, in other words, he or she spoofs the identity of people or websites to invite the users to visit their websites and sign up or sign in that fake or spoofed site [9].

There are usually some links in the spam emails sent to users which direct them to certain websites. Analyzing the links present in a spam email can shed significant light on the volume of phishing attacks using these emails. Links present in spam emails usually possess some features not seen in legitimate links and using these features we can somewhat predict the probability of a phishing attack [4]. One of the methods for detecting phishing attacks is to find out the patterns present in internet links and features of the websites users are directed to through these links. As an example in Figure (1), through one of these links in an internet spam, a user is directed to a fake page resembling the login page of popular Amazon website. The tags in the source code of the page can be used as important features for detecting phishing attacks. In the source code for the page's footnotes, there are no real and outward links and this feature leads to detecting the phishing attack [10].

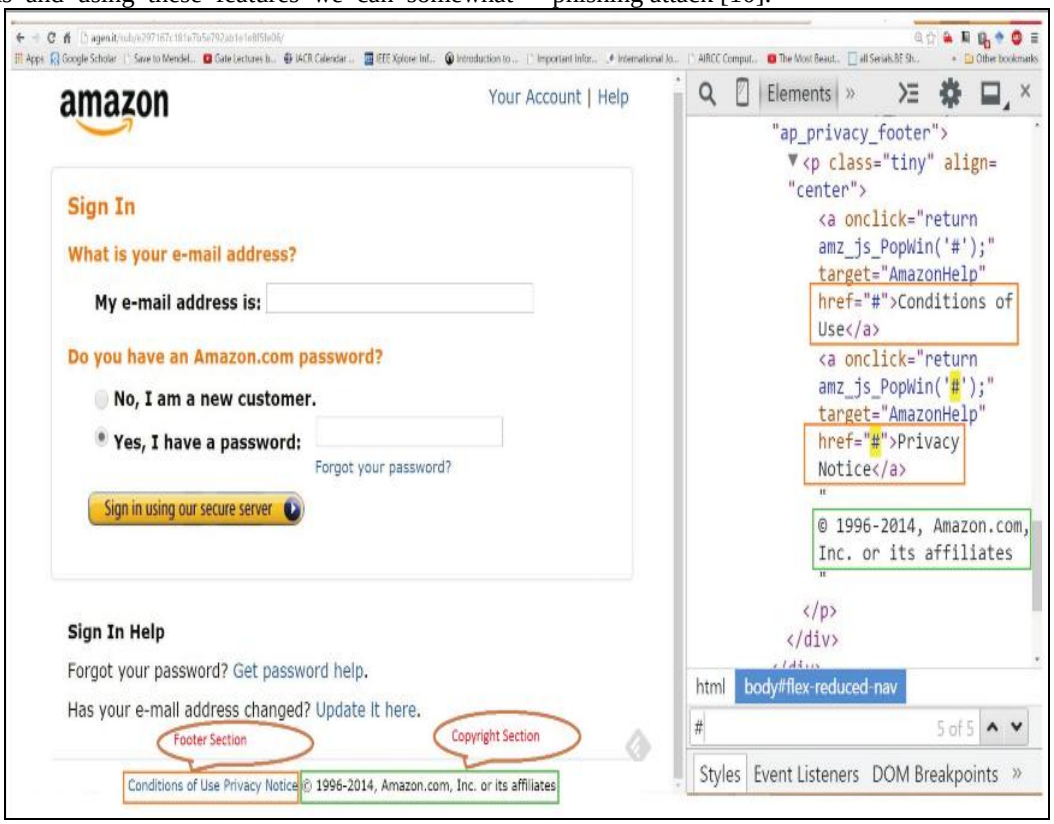

Fig. 1 Contents and the Source Code as Features for Detecting Phishing Attacks

So far, there have been important features for detecting phishing attacks including the age of the source site's domain name, the presence of IP addresses in the link, grammatical errors, the presence of @ character in the link, and the like. Detecting attack patterns based on these links is not an easy task due to the huge volume of information and its unorganized nature, so this requires special tools. In other words, the knowledge hidden in these is not of a high level and so it is not easily understandable; hence, we need methods such as data mining and its techniques to extract useful information and reach a higher level of knowledge. Discovering useful patterns in links present in spams leads to accurate detection of some internet attacks so that we can find ways to counteract them.

A. Definitions of Phishing

The phishing term is rooted in the word "fishing", not unlike many words which are used in a shortened or changed way in computer sciences. Phishing is an attack based on social engineering which is carried out in order to utilize security weaknesses in the cyberspace to deceive users to steal their usernames and passwords for financial accounts. Phishing techniques are numerous and complex, among which we can mention clicking on links to be directed to the page intended by the phisher [11]. There is no universal definition for phishing and so far there have been many definitions for phishing attacks. For instance, Figure (2) represents the number of definitions for phishing attacks in respected papers [12]. As can be seen from the figure, in 2012 about 23 different definitions for phishing were presented. The sheer number and variety of definitions for phishing indicate the complexity of this type of attacks.

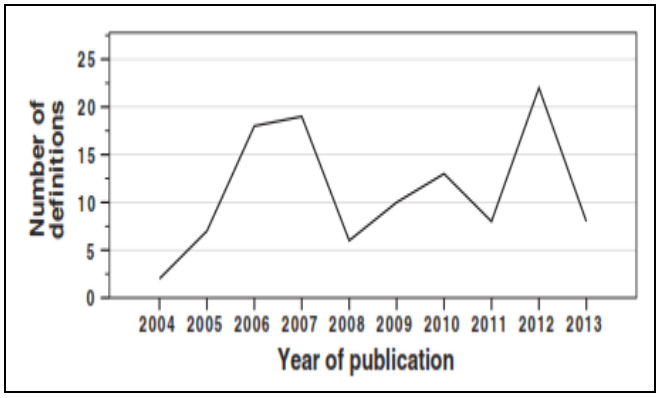

Fig. 2 The Number of Definitions Used for Phishing from 2004 to 2013

In this section, a number of definitions for phishing attacks are presented:

Definition of phishing attacks according to PhishTank Company (http://www.phishtank.com/): phishing is an attempt to steal the information of an individual using emails [13].

Sometimes phishing attack refers to websites which fake the identity and legitimacy of an institution, or a bank and claim they are that they are that organization [13].

Phishing is an internet attack using social engineering where the intruder tries to use different online or other techniques such as chat, SMS, and email to encourage users to enter certain websites to do a certain act [12].

For instance, based on the third definition, hacker might encounter a member of a shopping website and send him or her an SMS asking for his or her password. In order not to make the victim suspected of the message, hackers use official and imperative utterances.

B. Uptime for Phishing Attacks

Uptime for phishing attacks is in fact the time duration required for detection if a page is a phishing page or not. Usually, the detection is carried out by computer giants such as Google, Amazon, and the like. Figure (3) show the uptime for phishing attacks from 2011 to 2014 [14].

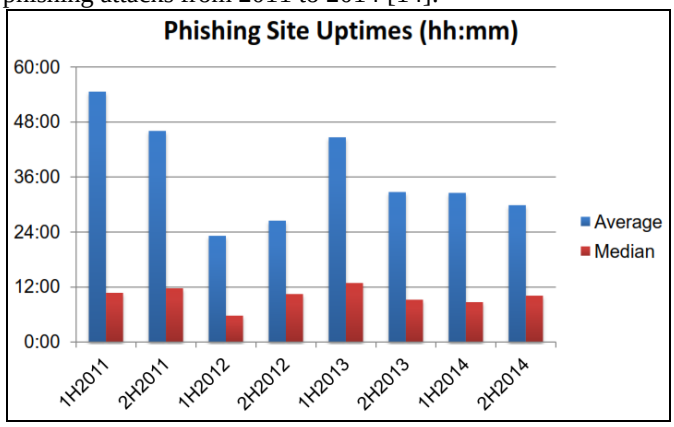

Fig. 3 Uptime for Phishing Attacks from the First Half of 2011 to the Second Half of 2014

Figure (4) shows the uptime for phishing attacks in the second half of 2014 based on domain. Based on the figure, the uptime for .com domains is the lowest and for .info domains, it is the highest [14].

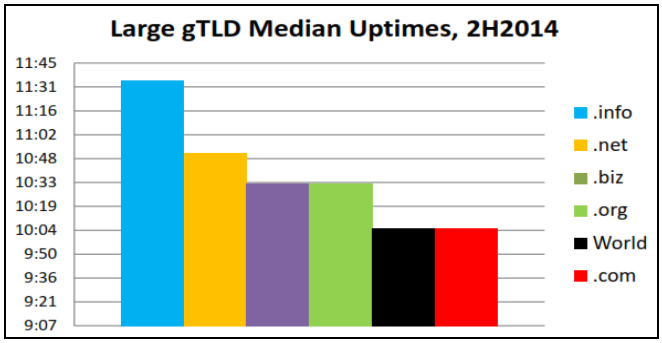

Fig. 4 Uptime for Phishing Attacks in the Second Half of 2014 Based on Domains

C. Scope of Phishing Attacks

The volume of phishing attacks is closely related to the type of the domain. Different top-level domains (TLDs) have various phishing attacks. The chart in Figure (5) shows that .com and .org domains are the domains which are most often chosen by phishers for phishing attacks [14].

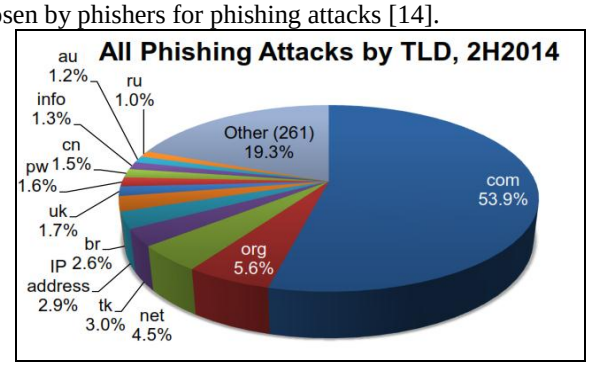

Fig. 5 Percentage of Phishing Attacks in the Second Half of 2014 Based on Domain Extensions

1) Countering Phishing Attacks

There are multiple methods for countering phishing attacks which are summarized as follows [14]:

- Training internet users for countering phishing attacks
- It is better not to click on the links sent in messages, type them instead
- Emails with general audience (without your specific name) should not be opened.
- The emails from banks and financial institutions would not ask for your account number since these institutions have your account number and they don't need to ask you for that.
- Installing anti-phishing extensions on your browser

2) Motivation and Purpose of Phishing Attacks

[15] summarize the motivations of a phisher for stealing information as follows:

- Financial gain: in this case, the financial needs of the attacker cause him or her to try to steal from institutions like banks and customer accounts
- Hiding their identity: some of the attackers need to hide themselves to be able to carry out destructive actions. Therefore, using stolen usernames and passwords they try to hide their identities while shopping on the internet (gambling, child abuse, and so on).

- Fame and notoriety: a huge number of users perform these attacks to reach fame and notoriety in the cyberspace.

3) Life Cycle of Phishing Attacks

Phishing attacks have an extensive nature. In these attacks, there is a cycle called the life cycle of phishing attacks.

Investigating the life cycle of phishing attacks can be used for developing anti-phishing techniques. Figure (6) represents the life cycle of a phishing attack using flowchart [13].

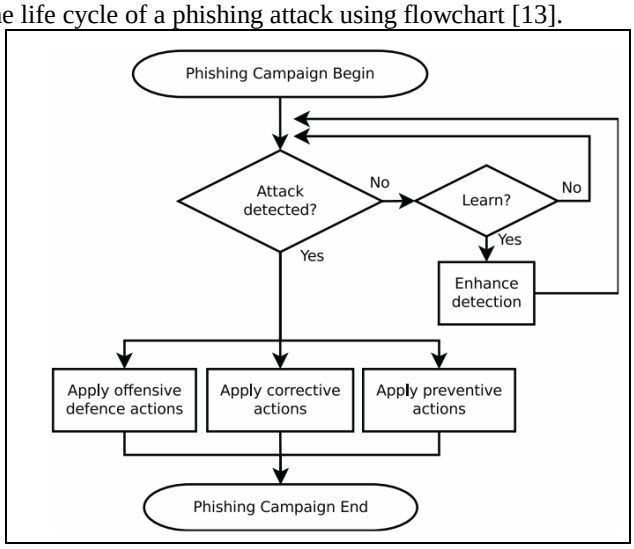

Fig. 6 Flowchart for the Life Cycle of Phishing Attacks

When a phishing attack starts (e.g. by sending phishing emails to users), the first line of defense against the attack is to detect them. In detecting phishing attacks there are two methods including end-user client software and user awareness programs. The ability to detect phishing attacks develops over time by learning, this learning can be performed through human users or machine learning algorithms. After detecting the phishing attacks, solutions must be utilized to counter them. Among the solutions that can be used after detecting the phishing attacks, the following can be mentioned [13]:

- Offensive defense: in this method, the victim of phishing attack will attack the company launching the original phishing attacks.
- Correction: in this case, the user reports the relevant hosting and deletes the files and footprints remained after the phishing attack.
- Prevention: in this method, users carry out a set of actions so that this phishing attack is erased and filtered in the future.

The above-mentioned methods only work when the phishing is accurately detected, indicating the importance of the phishing detection phase. Phishing attacks have a cycle of life including three stages: early phase, mid phishing phase, and post phishing phase, shown in Figure (7). In the early stages, the phisher prepares for the attack and creates an email or a spam and send it to the victims. In the mid phishing phases, the victims receive the fake emails and reveal their sensitive and valuable information. Finally, in the third cycle of phishing attacks, stealing information is committed [8].

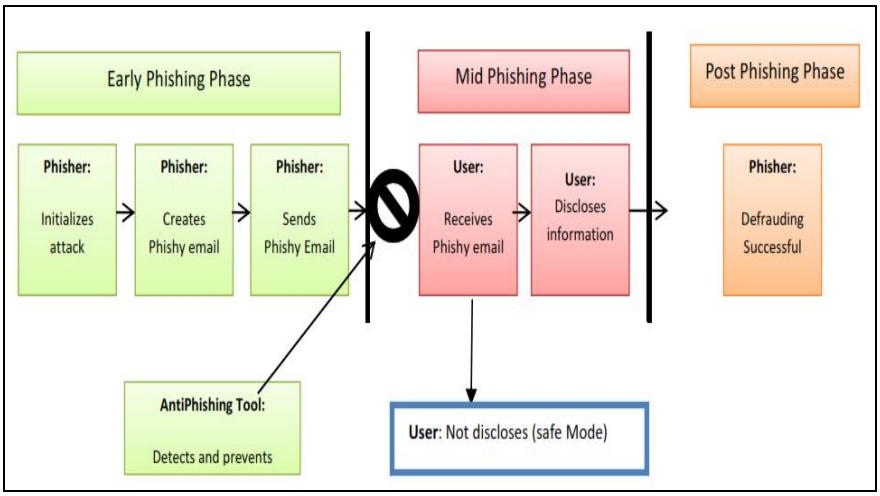

Fig. 7 Life Cycle of Phishing Attacks

IV. Analysis and Assessment

In this section, the output obtained from different methods of data mining on a phishing data set are presented and ultimately these outputs and similar experiments are used for assessing the proposed method. Therefore, before presenting the results, data mining techniques will be discussed.

A. Data Mining Techniques

Data mining is a general method for extracting useful knowledge from a set of raw and unorganized data which can provide useful patterns for better and more optimal analysis of the information. Data mining can extract useful patterns selected by the users from different types of databases. In this section, a number of important data mining techniques are briefly explained and then these techniques are used for detecting phishing attacks using Weka software application.

1) Decision Tree

Decision tree is considered a method for classification which uses data as two separate classes or parts. The first part of the data is used as training data and the second part is used as test data. Considering the fact that training data are used for learning, the main issue is the size of the decision tree; the smaller, the better. Training data must be accurately classified, leading to higher accuracy. Each node in the decision tree represents a feature. Each node has a number of edges and based on the possible values, the feature in the parent node is labelled and each edge connects two nodes or connects a node to a leaf.

2) Artificial Neural Network

Artificial decision networks are used for training different functions including functions with real values, functions with discrete values and functions with vector values. In other words, non-linear systems accept a huge number of inputs. Since neural networks consists of an arbitrary number of cells, nodes, units, or neurons and connect the input set to the output, they are designed solely based on input-output relations. Nowadays, the main goal of artificial neural networks is to reach human-like efficiency.

3) Bayesian Network

Another technique for detecting attacks is the Bayesian network which uses statistical schemes for detecting destructive behavior and it has the benefit of considering the dependency between variables. However, its main weakness is that results obtained from statistical methods require additional calculations.

4) Support Vector Machines (SVM)

While dividing the classes, support vector machine (SVM) searches for the desired separator for separating two classes and maximizing the margin between the closest points of the class. Nowadays, support vector machine has turned into a popular method for modeling, which reduces the training time. The goal of using support vector machine in attack detection systems is to separate normal patterns from attack patterns.

B. Evaluating Results in Data Mining Techniques

One of the suitable datasets for researching and developing techniques for countering phishing attacks is the set of data gathered by Rami. In the dataset used by them, the values for legitimate, suspicious, and phishy addresses are represented by 1, 0, and -1, respectively. This set includes 30 input features and 11055 records and samples. In the chart presented in Figure (8), a comparison using accuracy or precision and sensitivity or recall criteria is depicted which are calculated using Equation (1) and Equation (2), respectively:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (2)$$

In order to calculate Equations (1) and (2), the following parameters have been used:

- True positive (TP): the number of phishing samples correctly detected by the proposed method.
- True negative (TN): the number of non-phishing samples correctly classified as normal by the proposed method.
- False positive (FP): the number of phishing samples incorrectly classified as normal by the proposed method.
- False negative (FN): the number of non-phishing samples incorrectly classified as phishing samples by the proposed method.

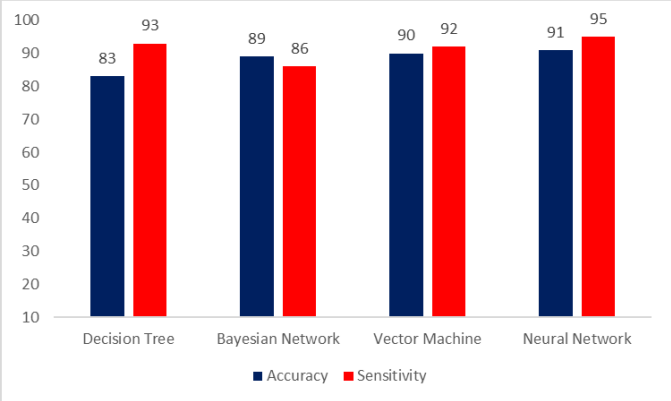

Fig. 8 Comparing Data Mining Techniques in Detecting Phishing Attacks Using the Two Evaluation Criteria of Accuracy and Sensitivity

As the chart indicates, the neural network technique detects these attacks with higher accuracy and sensitivity compared to other methods followed by support vector machine.

V. Conclusion

Spams are an important tool for phishers in phishing attacks to steal valuable information. Despite the fact that spams are used for different purposes including advertisement, financial issues, drugs, and so on, a certain percentage of the spams are used for sending the links of fake websites to users. These destructive links direct users to fake versions of generally legitimate websites. Investigating the subject matter of the spams and phishing attacks reveals that these two issues are almost always related since sending fake links in phishing attacks using destructive emails or spams does not require a lot of capital and time on behalf of the phisher. Detecting different spams and the methods for countering them on the one hand and detecting internet phishing attacks using different methods particularly data mining on the other were the main points of the current paper. In this study, we used different data mining techniques such as decision trees, artificial neural network, Bayesian network, and support vector machine to try to detect these attacks. The results of the experiments show that the neural network technique detects these attacks with higher accuracy and sensitivity compared to other methods, followed by support vector machine technique.

Considering the accuracy and sensitivity of artificial neural network in detecting phishing attacks compared to other data mining methods, in the next study we will try to propose a combined version of artificial neural network method and evolutionary algorithms in order to improve the accuracy and sensitivity of the neural network in detecting internet phishing attacks.

REFERENCES

[1] S. Mansfield-Devine, "Interview: Joe Ferrara–fighting phishing," *Computer Fraud & Security*, vol. 2013, pp. 17-20, 2013. http://dx.doi.org/10.1016/S1361-3723(13)70064-2

[2] G. Aaron, "The state of phishing," *Computer Fraud & Security*, vol. 2010, pp. 5-8, 2010. http://dx.doi.org/10.1016/S1361-3723(10)70065-8

[3] E. Shein, "The gods of phishing," *Infosecurity*, vol. 8, pp. 28-31, 2011. http://dx.doi.org/10.1016/S1754-4548(11)70023-7

[4] T. A. Almeida and A. Yamakami, "Facing the spammers: A very effective approach to avoid junk e-mails," *Expert Systems with Applications*, vol. 39, pp. 6557-6561, 2012. http://dx.doi.org/10.1016/j.eswa.2011.12.049

[5] S.-H. Liao, P.-H. Chu, and P.-Y. Hsiao, "Data mining techniques and applications–A decade review from 2000 to 2011," *Expert Systems with Applications*, vol. 39, pp. 11303-11311, 2012. http://dx.doi.org/10.1016/j.eswa.2012.02.063

[6] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," *Neural Computing and Applications*, vol. 25, pp. 443-458, 2014. http://dx.doi.org/10.1007/s00521-013-1490-z

[7] G. Ramesh, I. Krishnamurthi, and K. S. S. Kumar, "An efficacious method for detecting phishing webpages through target domain identification," *Decision Support Systems*, vol. 61, pp. 12-22, 2014. http://dx.doi.org/10.1016/j.dss.2014.01.002

[8] N. Abdelhamid, A. Ayesh, and F. Thabtah, "Phishing detection based Associative Classification data mining," *Expert Systems with Applications*, vol. 41, pp. 5948-5959, 2014. http://dx.doi.org/10.1016/j.eswa.2014.03.019

[9] M. Aburrous, M. A. Hossain, K. Dahal, and F. Thabtah, "Intelligent phishing detection system for e-banking using fuzzy data mining," *Expert systems with applications*, vol. 37, pp. 7913-7921, 2010. http://dx.doi.org/10.1016/j.eswa.2010.04.044

[10] R. S. Rao and S. T. Ali, "PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach," *Procedia Computer Science*, vol. 54, pp. 147-156, 2015. http://dx.doi.org/10.1016/j.procs.2015.06.017

[11] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators," *Computers & Security*, vol. 58, pp. 39-46, 2016. http://dx.doi.org/10.1016/j.cose.2015.12.001

[12] E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science*, vol. 3, pp. 1-10, 2014. http://dx.doi.org/10.1186/s40163-014-0009-y

[13] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 2091-2121, 2013. http://dx.doi.org/10.1109/SURV.2013.032213.00009

[14] P. Kumaraguru, P. Dewan, and R. Clayton, "2014 APWG Symposium on Electronic Crime Research (eCrime)."

[15] W. D. Yu, S. Nargundkar, and N. Tiruthani, "A phishing vulnerability analysis of web based systems," in *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*, 2008, pp. 326-331. http://dx.doi.org/10.1109/iscc.2008.4625681