SCOPE OF VISUAL BASED SIMILARITY APPROACH USING CONVOLUTIONAL NEURAL NETWORK ON PHISHING WEBSITE DETECTION

[1]Reshma R, [2]Dr. R. Vijayakumar, [3]Dr. Sindhu S

[1] Mtech Student, School of Computer Sciences Mahatma Gandhi University, Kottayam
[2] Professor, School of Computer Sciences, Mahatma Gandhi University, Kottayam
[3] Associate Professor, NSS Engineering College, Akathethara, Palakkad.

Abstract: *Phishing website is an illegitimate websites that is designed by dishonest people to mimic a real website. Those who are entering in such website may expose their sensitive information to the attacker whom might use this information for financial and criminal activities. In this technological world, phishing websites are created using new techniques allows them to escape from most anti-phishing tool. So that, the white list and blacklist based techniques are less effective when compared with the recent phishing trends. Advanced to that, there exists some tools using machine learning and deep learning approaches by examining webpage content in order to detect phishing websites. Along with the rapid growth of phishing technologies it is needed to improve effectiveness and efficiency of phishing website detection. This work reviewed many papers those proposed different real time as well as non real time techniques. As the result this study suggests a Convolutional Neural Network (CNN) framework with 18 layers and scope of transfer learning in AlexNet for the classification of websites using screenshot images and URLs of phishing and legitimate websites . CNN is a class of deep, feed-forward artificial neural networks (where connections between nodes do not form a cycle) & use a variation of multilayer perceptrons designed to require minimal preprocessing.*

***IndexTerms* - *Phishing, Character level CNN, Deep learning, transfer learning, APWG, AlexNet*.**

1. INTRODUCTION

In recent years, the most spreading online fraud activities are from the result of phishing and malware-based attacks. Recent study from RSA Security, a Dell Technologies business reported that the US, the Netherlands and Canada are the top three countries targeted by phishing attacks. It is shocking that India serves fourth place in that report. The Phishing concept came into existence at the early 1990s via America Online, or AOL. A group of hackers and pirates together named the warez community are the first “phishers.” They developed an algorithm to generate random credit card numbers, which they would then attempt to use to make fraudulent AOL accounts in trial and error manner. If there was a match found with any real card, they were able to create an account and spam others in AOL’s community. By 1995, AOL halted those generators, but contradicts to that the warez group moved on to other methods, specifically behaved as AOL employees and messaging people using AOL Messenger for their information. On January 2, 1996, the word “phishing” was first broken away in a Usenet group dedicated to American Online. Then AOL eventually included warnings on all its email and messaging software to alert users of potential phishing abuse. But phishing attacks moved on the different approaches [1].

Phishing is an attack that involves both social engineering research and deception to steal user's personal and financial information. Techniques targeted at using spoofed e-mails purporting will be from businesses and legal entities, to obtain sensitive information from the victim through third-party fraud. Technical deception schemes work directly on computers on steep credentials, which often use user-friendly user names and password tracking systems - and to corrupt local navigation infrastructure to attract false websites to consumers [2]. Attacks using phishing websites growing drastically in internet world since web surfing became inevitable to individuals now days. Phishing websites are a similar web site for legitimate websites to swindle web users in order to obtain their personal and financial information. Detection and protection of phishing websites must be carefully done by predicting the trends of attackers for doing so. According to quarterly based APWG Phishing Activity Trends Report 2018, the total number of phishing websites was 138,328, reduced around 50% within one year. Phishing that targeted SaaS/webmail services (29.8%) doubled in Q4 and most targeted sector is the payment service with 33 percent of phishing attacks. The total count of phishing attacks hosted on web sites that have HTTPS and SSL certificates decreased in that period [3].

There are different forms of phishing attacks in theory [1] as listed below:

- Phishing Attack by Fraud
- Phishing Attack by Infectious software
- Phishing Attack by MITM approach
- Phishing Attack by DNS spoofing
- Phishing Attack by Inserting harmful content
- Phishing Attack by Search Engine indexing

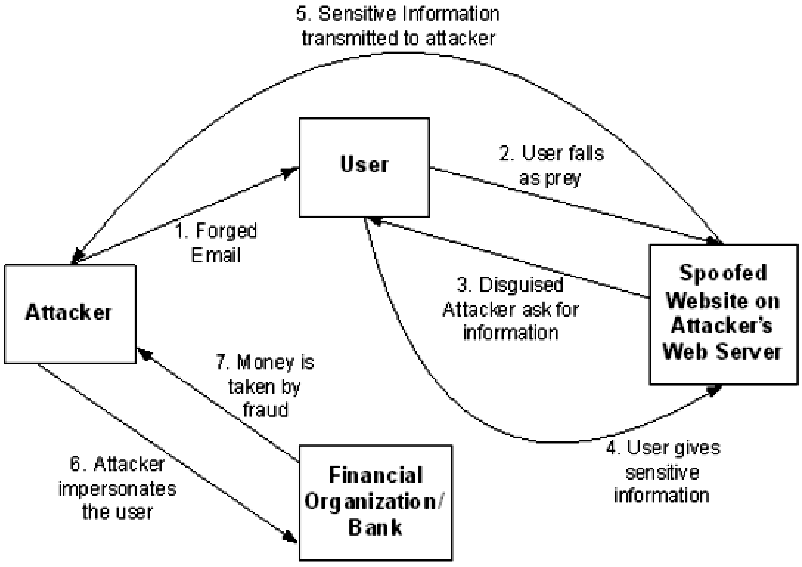
5. Sensitive Information transmitted to attacker
User
2. User falls as prey
1. Forged Email
Attacker
Spoofed Website on Attacker's Web Server
3. Disguised Attacker ask for information
7. Money is taken by fraud
6. Attacker impersonates the user
Financial Organization/ Bank
4. User gives sensitive information

Fig 1.1 Stages of phishing [1]

In phishing attack by fraud, the user is fooled by fraudulent emails to disclose personal or confidential information. While phishing attack by infectious software such as key loggers and screen loggers, the attacker succeeds in running dangerous software on user's computer. The DNS spoofing is used by phishers compromises the domain lookup process so that the user's click would lead him or her to a fake website. Another way of phishing is the attacker puts malicious content into a normal website in order to extract personal or sensitive information. In phishing attack by MITM approach, the attacker stays in between the user and the legitimate site to taps sensitive information. The fake web pages created by attacker give attractive offers to be top indexed by a search engine, so that a user would easily fall in it. Similarly, there are many ways for phishing attack detection and prevention. The stages of a general phishing attack are summarized in figure 1.1. Many researchers found different techniques against phishing but counter wards phishing experts developed many other practical way of spoofing. Researchers in advanced technology domain are worked hard to prevent phishing in real time by inventing many tools for detection and prevention of websites. Out of many domains, upcoming technology called Deep Learning has significant role in handling phishing attacks.

1.1 DEEP LEARNING

Deep learning is advancement to the machine learning concept; a model learns itself to perform classification tasks directly from images, text, or sound. Deep learning is usually implemented using neural network architecture [4]. Traditional neural networks contain solely a pair of or three layers, while deep networks can have hundreds. Computer programs that use deep learning bear a lot of an equivalent method. Each algorithm in the hierarchy applies a nonlinear transformation on its input and uses what it learns to create a statistical model as output. The characteristics of deep learning are

- Easy access to large volumes of named text files:

Data sets are freely available, and are useful for training on many different types of objects.

- Increased computing power:

High-performance GPUs in deep learning speed up the training of the massive amounts of data needed for deep learning, which reduces training time from weeks to hours.

- Pretrained models built by experts:

Pretrained models such as AlexNet can be used to perform new recognition tasks using a technique called *transfer learning* with highest accuracy.

A deep neural network combines multiple nonlinear process layers, using simple elements operating in parallel and inspired by biological nervous systems. It consists of associate input layer, several hidden layers, and an output layer. The layers are interconnected over nodes, or neurons, with each hidden layer using the output of the previous layer as its input. With the use of these features, real time phishing detection became more accurate as compared with traditional approach [4].

Phishing website detection tools can be developed by using the features of websites such as text, frames and images. Many researchers introduced phishing detection scheme based on text features only, some introduced detection scheme with the use of image features only, some based on text and frame features only, and based on text and image features only. Author M.A. Adebowale et al, 2019 introduced a scheme called intelligent phishing website detection and protection scheme (IPDPS) with the use of ANFIS architecture by looking into integrated features of images, frames and text [5]. Further details about this scheme are included in the later section.

2. LITERATURE REVIEW

Detecting and preventing the phishing attack is an important step towards securing phishing attacks on websites. There are some approaches to detecting these attacks. There are several phishing-related review papers available currently. From those papers, it is noted that there are different techniques for detection phishing attack. Generally they are classified as follows [6]:

- Attribute Based Anti-phishing Techniques
- Genetic Algorithm Based Anti-phishing Techniques
- Identity Based Anti-phishing Techniques
- Content Based Anti-phishing Approach

- Character Based Anti-phishing Approach
- Visual Similarity Based Anti-phishing Approach

2.1 ATTRIBUTE BASED ANTI-PHISHING TECHNIQUES

Attribute-based anti-phishing strategy applies both reactive and proactive anti-phishing defenses. This technique has been implemented in PhishBouncer tool [7]. An important aspect of the PhishBouncer approach is the plug-in framework, which provides a flexible way of applying personal adaptive and reactive logic to HTTP (S) streams. All anti-phishing logic was implemented as a set of plug-ins. They divided the plug-ins into three broad classes based on their role in the overall control flow and threading logic. The three classes were as follows: Dataplugins; called on every HTTP request and associated response to perform analysis on header and payload data. Checks; sequentially execute when HTTP requests entering the proxy and decide whether to accept the request, reject the request, or set a numeric value to indicate the confidence and choice selection. Probes; allow embedding proactive behavior into the proxy. PhishBouncer contains a set of nine anti-phishing checks and their supporting dataplugins including Suspected by Image Attribution check, Domain Too Young check, HTML Crosslink check, False Info Feeder check, Certificate Suspicious check, URL Suspicious check, Leaking User Data check, Phish Signature Match check, and Referred by Webmail check. PhishBouncer combines the outcome of individual checks to detect phishing attack.

Advantages:

- More phished sites were detected than traditional approaches
- Unknown attacks also be detected

Disadvantage:

- Slow response time due to multiple checking of authentication

2.2 GENETIC ALGORITHM BASED ANTI-PHISHING TECHNIQUES

In this approach [8], the genetic algorithm (GA) is applied to develop rules that discern the phishing link from the legal link. In order to assessing the parameters, such as the evaluation function, crossing and mutation, GA generates a set of rules that only adapts to phishing links. Those rules are stored in a database and a hyperlink activates as a phishing link if it matches any of this system rules and, therefore, is kept safe from the false hackers. The genetic algorithm not only useful for detecting phishing attacks, but also protects users from malicious or unwanted links to web pages. The rules preserved in the rule base are in the following general form [9]:

If {condition}
    Then {act} [9]

This rule can be explained with an example as follows: if there exists an IP address of the URL in the received e-mail and it does not match the defined Rule Set for White List then the received mail is reported as phishing mail and denoted as follows:

If {IP address of the URL in the received e-mail matches the Rule set}
Then {E-mail is Phishing mail}

Advantages:

- Before the user enters into the mail, it notifies the feature of malicious status
- Not only phishing detection but also malicious web link detection

Disadvantages:

- Need multiple rules set for each URL type to detect phishing
- It is to be needed to write new rules set which leads to more complex algorithm for other parameters

2.3 IDENTITY BASED ANTI-PHISHING TECHNIQUES

The identity based anti-phishing exploits the non-technical / inexperienced users who cannot identify spoofed emails or web sites and the relative ease of masqueraders. Authors H. Tout and W. Hafner [10] present Phishpin, an approach that uses mutual authentication concepts, requires online elements to prove their identities. This anti-phishing approach that combines client based filtering and domain-based identity techniques and integrates partial credentials and filtering to enforce bi-directional authentication without revealing sensitive information. By doing mutual authentication, users do not need to re-enter their credentials. Thus, the passwords between users and individuals through the Internet have changed only through the initial account setup method.

Advantages:

- Provide mutual authentication for both client side and server side
- Client password disclosure is not needed for each session

Disadvantages:

- If a hacker disabled the browser plug-in after gaining access permission to the client computer and then method will not detect phishing attack.
- When the session is initialized for the first time, it is compulsory to disclose the password

2.4 CONTENT BASED ANTI-PHISHING APPROACH

This approach identifies the similarity between the legitimate web page and suspicious/phishing web pages with respect to textual as well as visual contents. A content-based approach to detecting phishing sites CANTINA [11], examines the content of a webpage to determine whether or not it is legitimate, rather than looking at the surface characteristics such as URL and domain name of a web page. CANTINA uses the well-known TF-IDF (document term / inverse frequency) algorithm used to retrieve information. Experiments result that CANTINA was good at detecting phishing sites with accuracy approximate to 95%. CANTINA was implemented as a Microsoft Internet Explorer extension. Similarly another tool named GoldPhish [12] implemented this approach and used Google as its search engine. This tool protects against zero day phishing attacks with high accuracy. The procedure is as follows: First it captures an image of a page, and then uses optical character recognition to convert the image to text, and grasps the Google PageRank algorithm to reach decision on the validity of the site.

Advantages:

- Both CANTINA and GoldPhish provides zero day phishing and very low false positive results

Disadvantages:

- Time lag entangled in querying Google degrades the performance of CANTINA
- CANTINA: No dictionary for languages other than English
- GoldPhish delays webpage login
- GoldPhish may the webpage vulnerable to attacks on Google's PageRank algorithm and Google's search service

2.5 CHARACTER BASED ANTI-PHISHING APPROACH

Phishers always try to steal information of users by misleading them by clicking on the hyperlink that embedded into phishing email. The format of a hyperlink is as follows:

<ahref="URL"> Anchor text<\a>

The 'Universal Resource Locator' (URL) an unique identifier which provides the web link where the user will be re-directed and 'Anchor text' is the hypertext represents the visual link [6]. The unique characteristics or features of hyperlink were used in the character based anti-phishing technique especially to detect phishing links. LinkGuard [13] tool implements this technique which extracts the DNS names from the actual and the visual links and then compare with each other, if these names have matched, then said to be a legitimate otherwise phishing. Authors [13] considered the different possibilities of mismatch and rectified with respect to it. If IP address in the actual DNS is in the form of dot-decimal, then suspicious. If the actual link or the visual link is in encoded form, then the link is decoded first and then analyzed. When there is no destination information (DNS name or dotted IP address) in the visual link then the hyperlink is analyzed. During the period of analysis, LinkGuard searches the DNS name in blacklist as well as whitelist, if it is present in either of the list then classify accordingly. If it is not contained in either whitelist or blacklist, pattern matching will be done. During pattern matching the sender email address is extracted and then it is searched in a list of address is maintained that are manually visited by the user. URLNet [32] is the deep learning technique proposed to character based anti-phishing technique. This network uses character level CNN as well as word level CNN to URL classification.

Advantage:

- More Effective; not only for known attacks, but also to the unknown ones
- LinkGuard can detect up to 96 percent unknown phishing attacks in real-time

Disadvantage:

- The dotted decimal IP addresses may be relevant in some special situations even though LinkGuard results it as phishing (False Positives)

2.6 VISUAL SIMILARITY BASED APPROACH

Phishers always try to design a website that looks exactly as corresponding legitimate website, but the reality is they always keep a minor difference between them. So the visual similarity cannot be omitted when thinking about anti-phishing method. The two key points of visual similarity based approaches are follows: [31]

(1) Attackers usually insert ActiveX, images, Java Applet, and Flashes in place of HTML text to get hidden from anti-phishing detection. Visual similarity based detection approaches easily detect such embedded objects

(2) Techniques based on visual similarity use a signature to identify phishing web pages. The signature is created with common site-wide features rather than a single web page. Therefore, a signature is needed enough to detect multiple web pages targeted from a single site or from different versions of a site.

Author Dhamija et al. [26] conducted a survey on the visual similarity based approach on phishing detection, as the result they found the phishing intelligence of attackers using the visual similarity. In their study it was noted that about 23% of the experienced users missed to verify the URLs of the phishing websites. So it is evident that even experienced users may fooled by phishing attackers. Sadia Afroz et al. [27] presented a new approach called PhishZoo to handle this attack with similar accuracy to blacklisting approaches. It was used the profiles of trusted website's appearances to detect phishing. Chen et al. used screenshot of web pages to detect phishing sites [28]. They used Contrast Context Histogram (CCH) to describe the images of web pages and k-mean algorithm to cluster nearest key points. Finally Euclidean distance between two descriptors is used to find matching between two sites. Their approach has 95-99% accuracy with 0.1% false positive. Fu et al. [29] used Earth Mover's Distance (EMD) to compare low resolution screen capture of a webpage. Images of web pages are represented using color of a pixel in the image (alpha, red, green, and blue) and the centroid of its position distribution in the image. They used machine learning to select different threshold suitable for different web pages. Shuichiro Haruta et al. [30] proposed visual similarity-based phishing detection scheme using image and CSS with target website finder which results an accuracy of 72.1%. Since CSS contains the website visual contents, they used this feature to detect the website which plagiarizes appearance or CSS of legitimate website.

2.7 INTELLIGENT PHISHING DETECTION SYSTEM

All the above anti-phishing techniques have many features as well as limitations. Those techniques can be integrated in many ways to phishing detection. Intelligent phishing detection can be developed in different ways; Using Artificial Neural Network (ANN), Neuro-Fuzzy logic, Machine Learning algorithms, and Convolutional Neural Network of Deep Learning approach.

2.7.1 ARTIFICIAL NEURAL NETWORK ARCHITECTURE

An artificial neural network is an interconnected group of nodes, inspired by a simplification of neurons in a brain [15]. In other words, neural networks are a set of algorithms, modeled loosely after the human brain, that are designed to recognize patterns. Author Ramy M Mohammad [16] et al introduced an Artificial Neural Network model with back propagation to phishing detection. They studied many NNs to determine required NN parameters, such as "the number of hidden layers, the number of hidden neurons, learning speed etc"; which results better prediction accuracy. This technique in predicting phishing websites with reduced training time gives out as the automation of the process of NN building. They shown the result on different number of neurons 8,5,4,3,2 but better result obtained when number of hidden neurons set to 2; used 18 features to classify and trained the neural network. Many researchers made advancement in this ANN to improve accuracy. Reference [17] presented an ANN-MLP based phishing website classification model instead of single layered ANNs. This results the accuracy of 98.23% at the test phase. Reference [18] presented another variant ANN with Particle Swarm Optimization (PSO) algorithm instead of Back Propagation to classify the Uniform Resource Locator (URL) into Phishing URL or Non phishing URL. Dataset with 31 attribute was used for PSO-ANN modeling and achieved better accuracy with different number of hidden layer and output layer than back propagation neural network. Most of the research on this was based on text features only which gives the new scope.

2.7.2 NEURO-FUZZY SYSTEM

Neural networks have strong learning capabilities at numerical level, but users have difficulty understanding it. On the other hand, Fuzzy systems have good ability to explain vague arguments and integrate knowledge of skills. Both paradigms provide the ability to learn hybridization, include good interpretation and insight knowledge. Thus the concept of Neuro-Fuzzy systems evolved. This model was developed by inputting the fuzzification layers on neural network for learning practice. Neuro-fuzzy models describe the systems by using fuzzy *if-then* rules, such as '*If x is small then y is large*' represented in a nested manner, to which learning algorithms known from the area of artificial neural networks can be applied [19]. A paper on Neuro-Fuzzy Methods for Modeling and Identification refers that this model can be named as a graybox technique on the boundary between neural networks and qualitative fuzzy models [19]. Many anti-phishing tools were developed using this model or system so far. Author P.A. Barrowclough [20] et al presents a solution for inadequacy faced by online transactions. They claims that the inputs used for their study were not considered before in a single protection platform as hybrid way. They extracted total of 288 features from these five input sources. Neuro-Fuzzy systems with five inputs offers better accuracy and also be effective in detecting phishing sites in real-time.

A drawback of neuro-fuzzy modeling is that the current techniques for constructing and tuning fuzzy models are rather complex, and their use requires specific skills and knowledge. Modeling of complex systems will always remain an interactive approach [19].

2.7.3 MACHINE LEARNING APPROACH

Machine learning is the concept comes after the artificial intelligence as subset of itself. This technology provides an ability of self learning and self improving without any external instructions but with explicit feature engineering. Machine learning (ML) algorithm allows software applications to become more accurate in predicting outcomes without being explicitly programmed. This type of approaches focuses on applying machine learning and data mining techniques to phishing detection. These related techniques are classified into three main categories: Classification, Clustering, and Anomaly Detection [21]. Classification techniques try to map inputs (features or variables) to desired outputs (response) using a specific function. In the case of classifying phishing emails, a model is created to categorize an email into phishing or legitimate by learning certain characteristics of the email. Phishing classifiers can be grouped into three main categories: Classifiers based on URL features, Classifiers based on textual features, Classifiers based on hybrid features. Clustering-based countermeasures partition a set of instances into phishing and legitimate clusters. The objective of clustering is to group objects based on their similarities. If each object is represented as a node, and the similarities between different objects are measured based on their shared common features, then a clustering algorithm can be used to identify groups (of nodes) of similar observations. The anomaly-based approaches to phishing detection essentially treat phishing attempts as outliers. Every website claims a unique identity in the cyberspace either explicitly or implicitly. Anomaly detection methods assign a score to the suspicious material under analysis by comparing the features of phishing material with those of one or more nearest neighbors. If the anomaly score goes above a cut-off point, the webpage would be classified as phishing [21].

A classification model based on Extreme Learning Machine [22] for phishing website features classification achieved better performance than other machine learning methods (Support Vector Machine (SVM), Naive Bayes (NB)). ELM model can be defined as the Feed-forward artificial neural network (ANN) model with a single hidden layer [22]. To activate cells in a hidden ELM layer, a linear function was used, as well as non-linear (sigmoid, sinus, Gaussian), non-derivable or discrete activation functions and achieved highest accuracy of 95.34% [22]. But this classification model restricted to text features only and need more effectiveness in its performance.

2.7.4 DEEP LEARNING APPROACH

Deep learning (also known as deep structured learning or hierarchical learning) is an advanced concept of Machine Learning research that gives the capability of learning from unsupervised data that is unstructured or unlabeled to the networks. That is any designed model itself learns to perform classification tasks directly from images, text, or sound, usually implemented using neural network architecture. The term "deep" refers to the number of layers in the network—the more layers, the deeper the network. Traditional neural networks contain only 2 or 3 layers, while deep networks can have hundreds [23]. Online Malicious URL and DNS Detection Scheme proposed by Jiang J., Lin X [24] considered two common attack vectors URL and DNS in malicious activities for phishing detection with the help of character based Convolutional Neural Network framework. CNN framework automatically extracts the malicious features hidden within the URL strings and trains the classifying model. CNN network has been widely used in image recognition due to its ability to directly perform some convolution operations on the original pixel binary data to find hidden features hidden between pixels. CNN can also be used in word sequence feature mining with Neural Language Processing (NLP) [23]. In Reference [24] evaluated this approach using real-world datasets to demonstrate that this approach is both accurate and efficient. Fig 2.1 shows that the online malicious URL detection approach proposed in it.

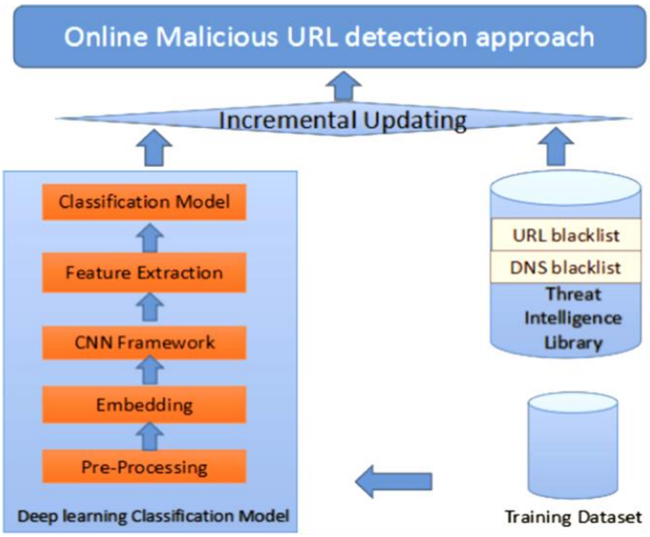

Fig 2.1: online malicious URL detection approach [24]

3. RESULTS AND DISCUSSIONS

Deep learning was developed to understand and analyze text using a multi-layered deep neural network, limiting natural language processing (NLP) capabilities to traditional machine learning algorithms using raw machines. The approach described here uses a deep learning network called the Convolutional Neural Network to train the classification model. Over the network, every output of the previous layer turns to the next level of input. Particularly deep learning techniques have the potential for language analysis, and distributed vectors trained under text-based vector representation for words are widely used in linguistic analysis systems.

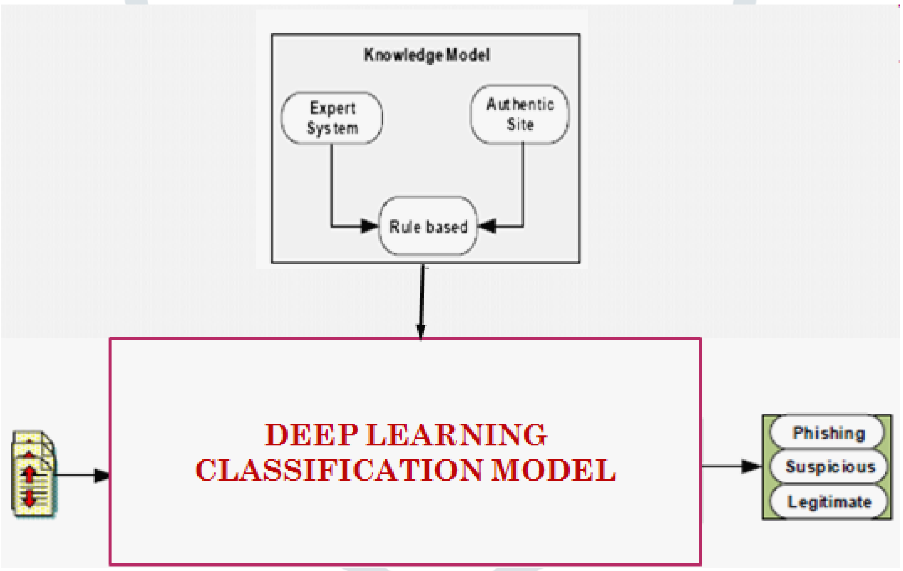

Fig 3.1 Conceptual diagram of smart phishing detection system using deep learning

In our proposed approach (see Fig. 3.1) consists of two main components, as follows:

(1) Dataset: The real-world dataset of phishing websites with URLs, screenshots, and webpage content from PhishTank, 2017. Another dataset was Phish-IRIS with screen shots of phishing and legitimate websites.

(2) Deep learning classification model, which consists of three processes such as preprocessing the input data, embedding, feature extraction and training a classification model using deep learning method.

A Convolutional neural network (CNN or ConvNet) is one of the most popular algorithms for deep learning with images as well as texts. Like other neural networks, a CNN is composed of an input layer, an output layer, and many hidden layers in between. The CNN framework mainly divided into two layers:

Feature Detection Layers:

These layers perform one of three types of operations on the data: convolution, pooling, or rectified linear unit (ReLU). Convolution puts the input data through a set of Convolutional filters, each of which activates certain features from the input datasets. Pooling simplifies the output by performing nonlinear down sampling, reducing the number of parameters that the network needs to learn about. Rectified linear unit (ReLU) allows for faster and more effective training by mapping negative values to zero and maintaining positive values. These three operations are repeated over tens of layers, with each layer learning to detect different features.

Classification Layers:

After feature detection, the architecture of a CNN shifts to classification. The next-to-last layer is a fully connected layer (FC) that outputs a vector of K dimensions where K is the number of classes that the network will be able to predict. This vector contains the probabilities for each class of any image being classified. The final layer of the CNN architecture uses a softmax function to provide the classification output.

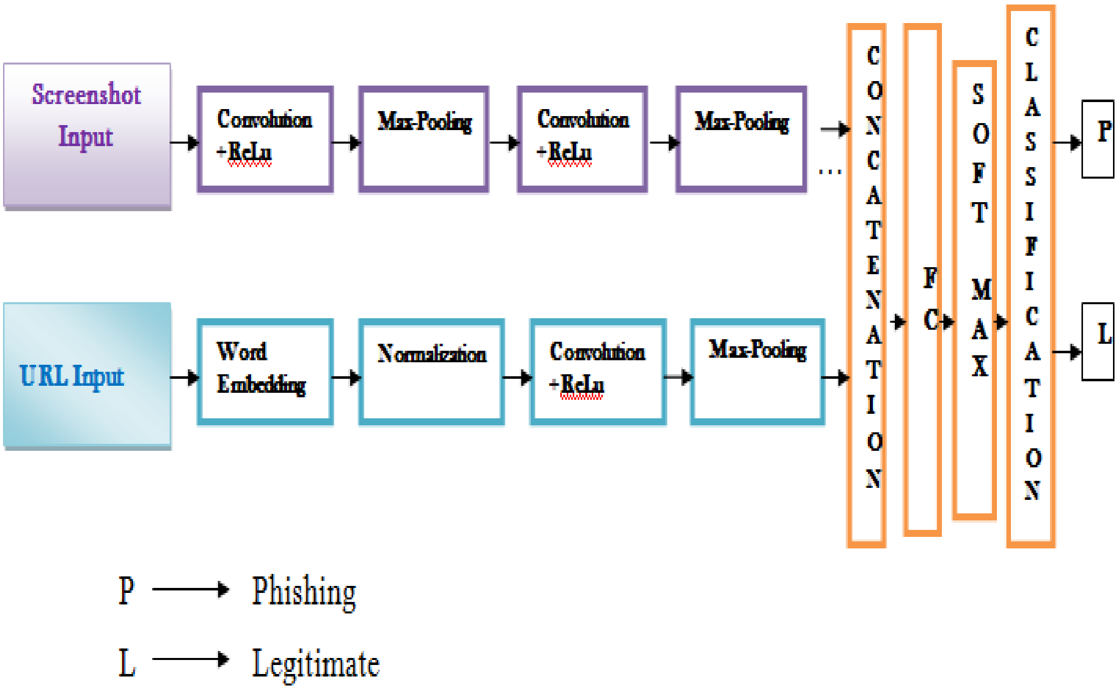

Fig 3.2: Proposed CNN architecture

The above architecture takes the input as screenshot of a website along with its corresponding URL and then passes this data to respective layers. Screenshot image passes through 8 layers of convolution, ReLu and max-pooling. The URL input passes through embedding layer which quantizes the URL into unique words and then batch normalization applies to convert it into images. Then these can be easily passed through the convolution layers to make it as CNN model. The outputs from both the Max-pooling layers are to be concatenated and then send to classification layers. The detailed description is follows:

Convolutional Layer: In the Convolutional layer, the first argument is filterSize, which is the height and width of the filters the training function uses while scanning along the images. In this example, the number 3 indicates that the filter size is 3-by-3. You can specify different sizes for the height and width of the filter. The second argument is the number of filters, numFilters, which is the number of neurons that connect to the same region of the input. This parameter determines the number of feature maps. Use the 'Padding' name-value pair to add padding to the input feature map. For a Convolutional layer with a default stride of 1, 'same' padding ensures that the spatial output size is the same as the input size. You can also define the stride and learning rates for this layer using name-value pair arguments of convolution2dLayer.

Batch Normalization Layer: Batch normalization layers normalize the activations and gradients propagating through a network, making network training an easier optimization problem. Use batch normalization layers between Convolutional layers and nonlinearities, such as ReLU layers, to speed up network training and reduce the sensitivity to network initialization. Use batchNormalizationLayer to create a batch normalization layer.

ReLU Layer: The batch normalization layer is followed by a nonlinear activation function. The most common activation function is the rectified linear unit (ReLU). Use reluLayer to create a ReLU layer.

Max Pooling Layer: Convolutional layers (with activation functions) are sometimes followed by a down-sampling operation that reduces the spatial size of the feature map and removes redundant spatial information. Down-sampling makes it possible to increase the number of filters in deeper Convolutional layers without increasing the required amount of computation per layer. One way of down-sampling is using a max pooling, which you create using maxPooling2dLayer. The max pooling layer returns the maximum values of rectangular regions of inputs, specified by the first argument, poolSize. The 'Stride' name-value pair argument specifies the step size that the training function takes as it scans along the input.

Fully Connected Layer: The Convolutional and down-sampling layers are followed by one or more fully connected layers. As its name suggests, a fully connected layer is a layer in which the neurons connect to all the neurons in the preceding layer. This layer combines all the features learned by the previous layers across the image to identify the larger patterns. The last fully connected layer combines the features to classify the images. Therefore, the OutputSize parameter in the last fully connected layer is equal to the number of classes in the target data. The output size is 2, corresponding to the 2 classes (Phishing and Legitimate). Use fullyConnectedLayer to create a fully connected layer.

Softmax Layer: The softmax activation function normalizes the output of the fully connected layer. The output of the softmax layer consists of positive numbers that sum to one, which can then be used as classification probabilities by the classification layer. Create a softmax layer using the softmaxLayer function after the last fully connected layer.

Classification Layer: The final layer is the classification layer. This layer uses the probabilities returned by the softmax activation function for each input to assign the input to one of the mutually exclusive classes and compute the loss. To create a classification layer, use classificationLayer.

4. CONCLUSION

Phishing is a significant problem involving fraud email and web sites that mislead unsuspecting users into disclosing private information. Among the different anti-phishing approaches, integration of visual similarity based approach and character based anti-phishing approach was not yet considered. The objective of the work was to identify the scope of developing such phishing website detection scheme to detect phishing websites more accurately with the help of deep learning algorithm called Convolutional Neural Network (CNN) classification model. The CNN framework was suggested to automatically extract the malicious features and train the classifying model. Thus it avoids manual hand crafted feature engineering method needed for real world phishing detection schemes. The integration of hybrid features extracted from URL texts and screenshot images may lead to betterment of existing phishing detection schemes.

REFERENCES

[1] Biju Issac, Raymond Chiong and Seibu Mary Jacob "*Analysis of Phishing Attacks and Countermeasures"* IBIMA, Bonn, Germany, Jan 2006, ISBN 0-9753393-5-4,pp.339-346

[2] W. Ali, "*Phishing Website Detection based on Supervised Machine Learning with Wrapper Features Selection,*" International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp. 72-78, 2017.

[3] APWG report [Online] Available at: https://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf

[4]https://www.mathworks.com/content/dam/mathworks/tagteam/Objects/d/80879v00_Deep_Learning_ebook.pdf

[5] M.A.Adebowale, K.T.Lwin, E.Sánchez, M.A.Hossain "*Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text*" Expert Systems with Applications,Volume 115, January 2019, Pages 300-313

[6] Deshmukh, M., Popat, S. K. and Student, U. (2017)"*Different Techniques for Detection of Phishing Attack*", International Journal of Engineering Science, 10201

[7] Michael Atighetchi, Partha Pal "*Attribute-based prevention of phishing attacks*" Eighth IEEE international symposium on network computing and application, 2009

[8] V. Shreeram, M. Suban, P. Shanthi and K. Manjula, "*Anti-phishing detection of phishing attacks using genetic algorithm,*" 2010 International Conference On Communication Control And Computing Technologies, Ramanathapuram, 2010, pp. 447-450.

[9] AmmarAlmomani, B. B. Gupta, SamerAtawneh, Meulenberg, and EmanAlmomani "*A Survey of Phishing Email Filtering Techniques*" IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, 2013

[10] H. Tout and W. Hafner, "*Phishpin: An Identity-Based Anti-phishing Approach,*" 2009 International Conference on Computational Science and Engineering, Vancouver, BC, 2009, pp. 347-352.

[11] Y. Zhang, J. I. Hong, and L. F. Cranor. "*CANTINA: a content-based approach to detecting phishing web sites*" In WWW '07: Proceedings of the 16th international conference on World Wide Web, pages 639–648, New York, USA, 2007. ACM.

[12] Matthew Dunlop, Stephen Groat, and David Shelly "*GoldPhish: Using Images for Content-Based Phishing Analysis*", in proceedings of internet monitoring and protection (ICIMP), Fifth International Conference, Barcelona, Pages 123-128, 2010.

[13] Lokesh M R, Vishwa Lalit, Jeeth Nair, Sura Sannith and Pradeep D "*Link Guard Algorithm Approach On Phishing Detection And Control*" International Journal of Advance Foundation and Research in Computer (IJAFRC)

[14] Jiang J., Lin X., Ghorbani A., Ren K., Zhu S., Zhang A., *"A Deep Learning Based Online Malicious URL and DNS Detection Scheme"* Communication Networks SecureComm, Springer, Cham 2017., vol 238

[15]www.wikipedia.org

[16] Mohammad, Rami, McCluskey, T.L. and Thabtah, Fadi Abdeljaber (2013) "*Predicting Phishing Websites using Neural Network trained with Back-Propagation*" In: Proceedings of the 2013 World Congress in Computer Science, Computer Engineering, and Applied Computing. WORLDCOMP 2013 . World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, Nevada, USA, pp. 682-686. ISBN 1601322461

[17] Ferreira, R. , Martiniano, A. , Napolitano, D. , Romero, M. , De Oliveira Gatto, D. , Farias, E. and Sassi, R. (2018) "*Artificial Neural Network for Websites Classification with Phishing Characteristics*" Social Networking, 7, 97-109.

[18] S. Gupta and A. Singhal, "*Phishing URL detection by using artificial neural network with PSO*," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-6.

[19] Babuška R.,In: Abraham A., Jain L.C., Kacprzyk J. "*Neuro-Fuzzy Methods for Modeling and Identification*", Recent Advances in Intelligent Paradigms and Applications. Studies in Fuzziness and Soft Computing, (2003) vol 113. Physica, Heidelberg

[20] Barraclough, P. A., Hossain, M. A., Tahir, M. A., Sexton, G. and Aslam, N. (2013)
"*Intelligent phishing detection and protection scheme for online transactions*" (Report), *Expert Systems With Applications*, 40(11), pp. 4697.

[21] Ahmed Aleroud, Lina Zhou, "*Phishing environments, techniques, and countermeasures: a survey*", *Computers & Security* (2017)

[22] Yasin Sönmez, Türker Tuncer, Hüseyin Gökal, Engin Avcı, *"Phishing web sites features classification based on extreme learning machine"* 6th International Symposium on Digital Forensic and Security (ISDFS) Conference, 2018, Page(s): 1-5

[23]https://www.mathworks.com/content/dam/mathworks/tagteam/Objects/d/80879v03_Deep_Learning_ebook.pdf

[24] Jiang J. et al. (2018) In: Lin X., Ghorbani A., Ren K., Zhu S., Zhang A. (eds) "*A Deep Learning Based Online Malicious URL and DNS Detection Scheme"* Security and Privacy in Communication Networks. SecureComm 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 238. Springer, Cham