**CHAPTER – 2**

**LITERATURE SURVEY**

**2.1 INTRODUCTION**

The Phishing sometimes referred to as criminal activity, will create a security threat to internet users. Soon every device that one owns IP address and nearly everyone has credentials to be connected to the Internet. Whether it's through a phone, laptop, or every device which has email and browser, the phishing attack will be happening in ways we cannot even imagine yet. Phishing has its impact in every field of life which everyone experiences it in one or the other way. This literature survey illustrates how the detection of phishing attacks can be done by the use of to transform an ordinary software to "Phishing Alerts" which will enhance the better accuracy to the detection of phishing URL. There is an alarming increase in morbidity and mortality due to attacks happen to normal internet users. In India, it is estimated that one attack happens every day. The normal has also been shown to have a maximum phishing attack. The victim involved in the attack needs to be taken care of and immediately give alert to the internet user. But there is a lag in handling the aftermath of attacks in the browser. The victim needs to be notified instantly about the attacks so that they can be stop access the phishing website immediately before they lose their credentials.

# 2.2 RELATED WORKS

A literature survey in a project report is that section which shows the various analyses and research made in the field related to our project work. The purpose of a literature survey is to gain an understanding of the existing research and relevant to our work and particular to the topic phishing URL detection using features of the URL or area of study. From these literature works below mentions which are related to our work helps to build knowledge in our field of work. These are some of the literature survey works, which include classifying URL, detection, predicting the phishing URL, machine learning, approach of phishing URL detection and etc.

**2.2.1 CLASSIFYING PHISHING URLs USING RECURRENT NEURAL NETWORKS**

As the technical skills and costs associated with the deployment of phishing attacks decrease, they are witnessing an unprecedented level of scams that push the need for better methods to proactively detect phishing threats. In this work, they explored the use of In this way, they compared a feature-engineering approach followed by even without the need for manual feature creation, beating by 5% the random forest method. This means it is a scalable and fast-acting proactive detection system that does not require full content analysis. Phishing attacks are a growing problem worldwide. Ac- cording to the Anti-Phishing Working Group (APWG), phishing sites increased by 250% from the last quarter of 2015 to the first quarter of 2016, targeting more than 400 brands each month [1]. This is the most the APWG has ever seen since they began tracking and reporting on phishing in 2004. Nowadays, phishing attacks can be launched from anywhere in the world at insignificant costs by people with little to no technical skills. Organizations trying to protect their users from these attacks are having a hard time dealing with the massive amount of emerging sites, which must be identified and labeled as malicious or harmless before users can access them. In this work, they focused on using machine learning techniques for the classification of phishing sites using only their URLs. Specifically, they compared the combination of lexical and statistical analysis of URLs as input for random forest (RF) classifier against a novel approach that employs recurrent neural networks, more particularly, a long/short term memory network (LSTM). The results show that despite using the URLs as sole input, the RF and the LSTM methods achieved an accuracy rate of 93.5% and 98.7%.

**2.2.2 PHISHING SITES PREDICTION USING CLASSIFICATION TECHNIQUES**

Phishing is an important issue that faces cybersecurity. This paper exploits the capabilities of classification techniques on Phishing site Prediction (PWP) and introduces a methodology to protect users from the attackers. The blacklist procedure isn't a strong enough way to stay safe from cybercriminals. Therefore, phishing site indicators have to be considered for this purpose, with the existence and usage of machine learning algorithms. Five different classification techniques have been used to evaluate their efficiency (PWP) in terms of accuracy and the Relative Absolute Error (RAE) value for each one of them, with and without the feature selection process. The tool was used for the implementation of these classifiers on a public dataset from the NASA repository. The motivation behind this investigation is to employ a number of Data Mining (DM) algorithms for the prediction purpose of phishing sites and compare their effectiveness in terms of accuracy and RAE. Where DM classifiers have proved their goodness in this kind of problem. The classification technique has significant performance in Phishing site Prediction. Five algorithms have been used and compared in terms of accuracy and RAE [2]. The feature selection preprocess was considered to observe the performance of classifiers with a minimal number of features. The obtained results of the classifiers are doing good without eliminating features in the tested dataset. But there is a tradeoff in the accuracy and the consumed time in the prediction process. Where if more accuracy was required, it's better to use the classification techniques without feature selection. And if the best performance was the target it's better to use the feature selection process in this dataset. Without applying the feature selection, it was found that the Random Forest classifier had the highest accuracy and the Naïve Bayes had the least one, while the Multilayer Perceptron and Prism had the least RAE value and Naïve Bayes had the highest one. In the future, more classification techniques can be compared, with different measures, and more datasets can be used, in addition to the feature extraction from a number of phishing sites then they could apply many classification techniques for the prediction process.

**2.2.3 PROTECT SENSITIVE SITES FROM PHISHING ATTACKS USING FEATURES EXTRACTABLE FROM INACCESSIBLE PHISHING URLs**

Phishing is the third cyber-security threat globally and the first cyber-security threat in China. There are 61.69 million phishing victims in China alone from June 2011 to June 2012, with the total annual monetary loss more than 4.64 billion US dollars. These phishing attacks are highly concentrated in targeting at a few major sites. Many phishing pages had a very short life span. In this paper, they assume that the sites to protect against phishing attacks are known, and study the effectiveness of machine learning-based phishing detection using only lexical and domain features, which are available even when the phishing pages are inaccessible. they propose several novel highly effective features, and use the real phishing attack data against Taobao and Tencent, two main phishing targets in China, in studying the effectiveness of each feature, and each group of features. they then select an optimal set of features in our phishing detector, which has achieved a detection rate better than 98%, with a false positive rate of 0.64% or less. The detector is still effective when the distribution of phishing URLs changes. In this paper, they investigated the effectiveness of machine-learning-based phishing detection when the targeted phishing sites are known. The actual phishing data targeted at Taobao and Tencent have been used in our studies. This is a position paper for an ongoing project to develop an effective phishing detector to protect the users of the aforementioned major sites targeted by phishing attacks. The detector can be deployed to these users as a browser plugin. Browser plugins have been widely used by online banks and online retailers in China to protect their users. A major challenge is that many phishing pages are short-lived, typically less than 20 hours, and URLs may change Protect Sensitive Sites from Phishing Attacks Using Features Extractable from Inaccessible Phishing URLs [3]. For example, they received regular (they likely initially and then daily) reports of phishing URLs from Taobao. Upon receiving the report, they immediately access the phishing pages but more than 80% of the phishing URLs are inaccessible. As a consequence, the discriminative features obtained from live sites such as page features and network features used in existing phishing detectors can no longer be used. Only lexical and domain features are used since many phishing URLs had a short life span, and these features are typically still available even when phishing pages are inaccessible. they proposed several novels, highly effective features. they studied the effectiveness of each feature and selected an optimal set of features in our detector, which achieved a detection rate better than 98%, with a false positive rate of 0.64% or below. The detection rate with the changed distribution of phishing URLs was still above 91%.

**2.2.4 DETECTION OF PHISHING ATTACKS**

Phishing is a form of cybercrime where an attacker imitates a real person by promoting them as an official person or entity through e-mail or other communication mediums. In this type of cyber attack, the attacker sends malicious links or attachments through phishing e-mails that can perform various functions, including capturing the login credentials or account information of the victim. These e-mails harm victims because of money loss and identity theft. In this study, a software called "Anti Phishing Simulator" was developed, giving information about the detection problem of phishing and how to detect phishing emails. With this software, phishing and spam emails are detected by examining mail contents. Classification of spam words added to the database by the Bayesian algorithm[4] is provided. Anti Phishing Simulator was developed to check the text content and determine whether the related message contained phishing elements. Today, an e-mail can be found in primitive ways whether it is a phishing message or not. For this are looked where this e-mail came from, whether a link with the message matches the actual site, whether the email or referrer site is using some emotional or exciting words to get a response, whether it is spelling or grammar errors in the email or on the site. However, many people pay attention to this point unconsciously entering the links given to other accounts. Anti Phishing Simulator aims to control the security of information and to prevent infringements, to check whether spam is available from the current database, to enable the user to create his own spam list, and to check whether the incoming mail has dangerous content. The inclusion of the mail account to be protected in the system. With this module, the user will also control and communicate without having to open the mail. With this module, it is possible to determine the classification results of keywords and passages in the database by the Bayes algorithm. The simulator collects phishing and spam messages at a common point. In addition to getting spam messages in the spam box, it allows you to control the "spam box" whenever you want. Those who are technically qualified by the "URL Control" feature will be able to examine the link address in the mail in more detail. In the future, it is aimed to analyze mail content more thoroughly with basic text mining by increasing the spam keyword database much more. It is also aimed to obtain more accurate results and classification with artificial neural networks.

**2.2.5 INTELLIGENT PHISHING URL DETECTION USING ASSOCIATION RULE MINING**

Phishing is an online criminal act that occurs when a malicious page impersonates as a legitimate page so as to acquire sensitive information from the user. Phishing attack continues to pose a serious risk for users and annoying threat within the field of electronic commerce. This paper focuses on discerning the significant features that discriminate the legitimate and phishing URLs. These features are then subjected to associative rule mining—apriori and predictive apriori. The rules obtained are interpreted to emphasize the features that are more prevalent in phishing URLs. Analyzing the knowledge accessible on phishing URL and considering confidence as an indicator, the features like transport layer security, unavailability of the top-level domain in the URL and keyword within the path portion of the URL are found to be sensitive indicators for phishing URL. In addition to this number of slashes in the URL, dot in the host portion of the URL and length of the URL is also the key factors for phishing URL. The proposed method consists of two phases URL search phase and feature extraction phase. In the URL search phase, once the user requests an URL, a search is carried out to check whether the given URL is in the repository of legitimate URLs. If a match is found in the repository, then the URL is considered to be a legitimate URL. Otherwise, the URL is not a legitimate URL and it undergoes the next phase. The main reason for carrying out the search phase before the feature extraction phase is it reduces the unnecessary computation during the feature extraction phase and improves the overall response time of the system. In the Feature extraction phase, they have defined heuristics to extract 14 features from the URL and are subjected to association rule mining to determine the legitimate and phished URL. mining—apriori and predictive apriori. The rules obtained are interpreted to emphasize the features that are more prevalent in phishing URLs. The results obtained from rule mining have highlighted the useful features available in the phished URL. Analyzing the information available on phishing URL and considering confidence as an indicator, the features such as transport layer [5] security, unavailability of the top-level domain in the URL and keyword within the path portion of the URL are found to be sensitive indicators for phishing URL. In addition to this number of slashes in the URL, dot in the host portion of the URL and length of the URL is also the key factors for phishing URL.

**2.2.6 ONLINE DETECTION AND PREVENTION OF PHISHING ATTACK**

Phishing is a new type of network attack where the attacker creates a replica of an existing page to fool users (e.g., by using specially designed e-mails or instant messages) into submitting personal, financial, or password data to what they think is their service provides' site. In this paper, they propose a new end-host based anti-phishing algorithm, which they call LinkGuard, by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the Anti-Phishing Working Group (APWG). Because it is based on the generic characteristics of phishing attacks, LinkGuard can detect not only known but also unknown phishing attacks. they have implemented LinkGuard in Windows XP. Our experiments verified that LinkGuard [6] is effective to detect and prevent both known and unknown phishing attacks with minimal false negatives. LinkGuard successfully detects 195 out of the 203 phishing attacks. In these experiments, the LinkGuard can detect and prevent phishing attacks in realtime. They first analyze the common characteristics of the hyperlinks in phishing e-mails. Our analysis identifies that the phishing hyperlinks share one or more characteristics as listed below: 1) the visual link and the actual link are not the same; 2) the attackers often use a dotted-decimal IP address instead of DNS name; 3) special tricks are used to encode the hyperlinks maliciously; 4) the attackers often use fake DNS names that are similar (but not identical) with the target site. they then propose an end-host based anti-phishing algorithm which they call LinkGuard, based on the characteristics of the phishing hyperlink. Since LinkGuard is character-based, it can detect and prevent not only known phishing attacks but also unknown ones. they have implemented LinkGuard in Windows XP, and our experiments indicate that LinkGuard is light-weighted in that it consumes very little memory and CPU circles, and most importantly, it is very effective in detecting phishing attacks with minimal false negatives. LinkGuard detects 195 attacks out of the 203 phishing archives provided by APWG without knowing any signatures of the attacks. In this paper, they have studied the characteristics of the hyperlinks that are embedded in phishing e-mails. they then designed an anti-phishing algorithm, LinkGuard, based on the derived characteristics. Since PhishigGuard is characteristically based, it can not only detect known attacks but also is effective to the unknown ones. they have implemented LinkGuard for Windows XP. In this experiment that LinkGuard can detect up to 96% unknown phishing attacks in real-time. they believe that LinkGuard is not only useful for detecting phishing attacks but also can shield users from malicious or unsolicited links in pages and Instant messages. Our future work includes further extending the LinkGuard algorithm so that it can handle CSS (cross-site scripting) attacks.

**2.2.7 LARGE SCALE AUTOMATIC CLASSIFICATION PHISHING URL**

Phishing sites, fraudulent sites that impersonate a trusted third party to gain access to private data, continue to cost Internet users over a billion dollars each year. In this paper, they describe the design and performance characteristics of a scalable machine learning classifier they developed to detect phishing sites. they use this classifier to maintain Google's phishing blacklist [7] automatically. Our classifier analyzes millions of pages a day, examining the URL and the contents of a page to determine whether or not a page is phishing. Unlike previous work in this field, they train the classifier on a noisy dataset consisting of millions of samples from previously collected live classification data. Despite the noise in the training data, our classifier learns a robust model for identifying phishing pages which correctly classifies more than 90% of the phishing page. This paper describes such an automatic phishing classifier that they built and currently use to evaluate phishing pages and maintain our blacklist. Since its activation in November 2008, this system evaluates millions of potential phishing pages every day. To evaluate each page, the classifier considers features regarding the page's URL, content, and hosting information. they retrain this classifier daily using approximately ten million samples from classification data collected over the last three months. To provide training labels for this data, they use our published blacklist, the most complete listing of known phishing pages they have available. Since the coverage of our published blacklist is not perfect, the training labels contain a number of misclassifications. Nevertheless, our process develops classification models that demonstrate excellent performance, maintaining a false positive rate well below 0.1% while maintaining high recall. During the first six months of 2009, our classifier evaluated hundreds of millions of pages, automatically blacklisting 165,382 phishing pages. For comparison, PhishTank evaluated 139,340 potential phishing pages, finding only 47,203 actual phishing pages, during the same timespan. In this large-scale system for automatically classifying phishing pages which maintains a false positive rate below 0.1%. Our classification system examines millions of potential phishing pages daily in a fraction of the time of a manual review process. By automatically updating our blacklist with our classifier, they minimize the amount of time that phishing pages can remain active before they protect our users from them. Even with a perfect classifier and a robust system, they recognize that our blacklist approach keeps us perpetually a step behind the phishers. they can only identify a phishing page after it has been published and visible to Internet users for some time. However, they believe that if they can provide a blacklist complete enough and quickly enough, they can force phishers to operate at a loss and abandon this type of Internet crime.

**2.2.8 AUTOMATIC CLASSIFICATION OF CROSS SITE SCRIPTING URL**

The structure of dynamic sites comprised of a set of objects such as HTML tags, script functions, hyperlinks, and advanced features in browsers lead to numerous resources and interactiveness in services currently provided on the Internet. However, these features have also increased security risks and attacks since they allow malicious codes injection or XSS (cross-site Scripting). XSS remains at the top of the lists of the greatest threats to applications in recent years. This paper presents the experimental results obtained on XSS automatic classification [8] in pages using Machine Learning techniques. they focus on features extracted from document content and URL. Our results demonstrate that the proposed features lead to highly accurate classification of the malicious page. This paper focuses on the automatic classification of XSS attacks on pages by extracting and analyzing predictive features of the document content and URL, using Naive Bayes and SVM classifiers. To this end, experiments are performed using Dmoz and Clue09 datasets as non-XSS pages, while XSSed pages are used as malicious samples. Moreover, a brief comparison with the features described by Likarish et al, in terms of performance, is also presented. The classification rates achieved by both classifiers using the proposed features presented stable values and helped the whole set of features to outperform the baseline features. As contributions, this paper presented, The definition and analysis of features to classify patterns of XSS attacks in pages, The presentation of a method which employ machine learning techniques to detect XSS attacks in pages, A comparative analysis the Naive Bayes and SVM classifiers, in order to show the overall performance of the XSS attacks classification. With regard to future work and considering the magnitude of XSS attacks, it is clear that the search for features that represent new attacks is a good opportunity for new experiments seeking for extending knowledge and conclusions. Moreover, the experiments conducted are limited to two classifiers and manipulation of its parameters. Thus, there are other classifiers that can fit the problem and obtain good results. Finally, even though they tried to deal with large databases, this work does not reach all attack possibilities.

**2.2.9 Detecting Phishing sites, a Heuristic Approach**

Phishing is a site forgery technique with an intention to track and steal the sensitive information of online users. The hacker fools the user with social engineering techniques such as SMS, voice, email, site, and malware. Various approaches have been proposed and implemented to detect a variety of phishing attacks such as the use of blacklists and whitelists to name a few. In this paper, they propose a desktop application called PhishSaver, which focuses on the URL and site content of the phishing page. they aim at detecting phishing sites with the help of a desktop application named PhishSaver. PhishSaver uses a combination of the blacklist and a number of heuristic features to detect a number of phishing attacks. For blacklist, they have used GOOGLE API SERVICES [9] that is Google safe browsing blacklist as this list is constantly updated and maintained by Google. It is also possible to run PhishSaver as a daemon process that means it is able to detect phishing attacks in real-time as a user browses the internet. PhishSaver takes URL as an input and outputs the status of the URL as a phishing or legitimate site. The heuristics used to detect phishing are footer links with a null value, zero links in the body of the HTML, copyright content, title content, and site identity. PhishSaver is able to detect zero-hour phishing attacks that may have not been blacklisted and is faster than visual-based assessment techniques that are used in detecting phishing. they observe that PhishSaver has obtained a higher accuracy rate and covers a wider range of phishing attacks that results in less false negative and false positive rates.

**2.2.10 Detection and Prevention of Phishing Attack Using Dynamic Watermarking**

Nowadays phishing attacks are increasing with the rate which is highly problematic for social and financial sites. Many antiphishing mechanisms currently focused to verify whether a site is genuine or not. This paper proposes a novel anti-phishing approach based on the Dynamic watermarking technique. According to this approach, the user will be asked for some additional information like watermark image, its fixing position, and secret key at the time of user registration and these credentials of a particular user will be changed at per login [10]. During each login phase, a user will verify the authentic watermark with its position and decide the legitimacy of the site.

Today all organizations are using the internet for sharing the message and the communication must be secure. This attack treated as a deceptive phishing attack that targets the financial organization. Many anti phishing tools exist to protect the attack. According to their idea, they have proposed a new end-host based anti-phishing algorithm, which is called Link Guard, which works by utilizing the generic characteristics of the hyperlinks in phishing attacks. In this paper, they are proposing an approach for the prevention of phishing attacks based on dynamic position watermarking techniques. This approach is divided into three modules viz. The registration process, Login verification process, and site closing process. Different positions for watermark image can be top left, bottom left, top right, bottom right, center.

**2.2.11 Phishing URL Detection Using URL Ranking**

The openness of the exposes opportunities for criminals to upload malicious content. In fact, despite extensive research, email-based spam filtering techniques are unable to protect other services. Therefore, a countermeasure must be taken that generalizes across services to protect the user from phishing host URLs. This paper describes an approach that classifies URLs automatically based on their lexical and host-based features. Clustering is performed on the entire dataset and a cluster ID (or label) is derived for each URL, which in turn is used as a predictive feature by the classification system. Online URL reputation services are used in order to categorize URLs and the categories returned are used as a supplemental source of information that would enable the system to rank URLs [11]. The classifier achieves 93-98% accuracy by detecting a large number of phishing hosts while maintaining a modest false positive rate. URL clustering, URL classification, and URL categorization mechanisms work in conjunction to give URLs a rank.

**2.2.12 Phishing sites Detection Using Machine Learning**

Phishing is a common attack on credulous people by making them disclose their unique information using counterfeit sites. The objective of phishing site URLs is to purloin the personal information like user name, passwords, and online banking transactions. Phishers use the sites which are visually and semantically similar to those real sites. As technology continues to grow, phishing techniques started to progress rapidly and this needs to be prevented by using anti-phishing mechanisms to detect phishing. Machine learning is a powerful tool used to strive against phishing attacks. This paper surveys the features used for detection and detection techniques using machine learning.

Phishing is the most unsafe criminal exercise in cyberspace. Since most of the users go online to access the services provided by the government and financial institutions, there has been a significant increase in phishing attacks for the past few years. Phishers started to earn money and they are doing this as a successful business. Various methods are used by phishers to attack vulnerable users such as messaging, VOIP, spoofed links, and counterfeit sites. It is very easy to create counterfeit sites, which looks like a genuine site in terms of layout and content. Even, the content of these sites would be identical to their legitimate sites. The reason for creating these sites is to get private data from users like account numbers, login id, passwords of debit and credit card, etc. Moreover, attackers ask security questions to answer to posing as a high-level security measure providing to users. When users respond to those questions, they get easily trapped into phishing attacks. Many kinds of research have been going on to prevent phishing attacks from different communities around the world. Phishing attacks can be prevented by detecting the sites and creating awareness for users to identify the phishing sites. Machine learning algorithms [12] have been one of the powerful techniques in detecting phishing sites. In this study, various methods of detecting phishing sites have been discussed.

**2.2.13 A Proposal on Phishing URL Classification for Web Security**

Data mining and machine learning are some of the most essential tools in new generation technology. That is used in a number of applications i.e. security, banking, and decision making. In this paper, the data mining application of web data security is described in detail. In this context, the domain of phishing URL detection and classification is a key aim of the proposed work. This paper includes the different aspects of phishing and recently made contributions to the accurate classification of phishing URLs. In addition to that, a data mining based model is also proposed that is helpful to classify the phishing URLs more accurately. Finally, the paper provides a future extension of the work. The main aim of the proposed study is to explore the domain of web security more specifically phishing detection and their identification approaches. In this context, a rich literature is explored for obtaining the relevant methodologies and techniques of classification. Finally, some relevant techniques are obtained and on the basis of available literature, an accurate classification model [13] is proposed for design and implementation. The proposed data model is based on the concept of rule mining and rule-based classification technique. Therefore two popular rule mining techniques namely apriori algorithm and FP-Tree is proposed for system employment. This model is implemented and their performance evaluation is demonstrated in the near future.

**2.3 SUMMARY**

Various dimensions of Phishing Alerts were briefed in the survey paper. The smartness of the detection of attack depends on the extension added to the browser and also on the safety of the victim credentials. Out of all the papers that were referred, the efficient one was with the browser extension as it is human independent. However, this proposal does have some disadvantages. The rest of the papers were all similar to the same features which might bring a sure change when designed. The cause of an attack cannot be generalized or narrowed down because there can exist a distinct cause in every attack scenario. The most common cause that was considered in all the above-mentioned papers was the classification algorithm and feature extraction and awareness of phishing by the victim. And also the considered paper mainly deals with attack prevention only. The scenario after an attack involves passing the information at the right time which saves the victim credentials.