IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CHROME EXTENSION FOR DETECTION AND PREVENTION OF PHISHING WEBSITES AND RELATED ATTACKS BY USING MACHINE LEARNING

Vinayak Jalan[1], Mrunal Hemant Pawshe[2], Manali Rajesh Oswal[3], K. S. Mulani[4]

[1,2,3]Student, [4]Asstistant Professor
Department of Computer Engineering
Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract: Phishing is a type of cyber-attack where a fraudulent message is sent by an attacker in order to deceive an individual into revealing sensitive information. The fraudulent message is often designed to mimic a legitimate website or organization, and the attacker can observe the victim's activity on the site. According to the FBI's Internet Crime Complaint Centre, phishing incidents have been recorded at more than twice the rate of any other type of computer crime. In 2022, phishing attacks were the most common type of attack carried out by cybercriminals. Phishing attacks peaked at an all-time high in 2021, with 300,000 attacks being registered in just one month (December), more than tripling from the previous two years. Our aim is to create a chrome extension to detect the Phishing websites and alert the user using machine learning and deep learning techniques whenever a user visits the website. The project aims to gather URLs from multiple sources, including UCI machine learning repository, Kaggle, Phish Tank, and Alexa URL. Whenever a user opens a website on his/her browser, the extension will work in the background. If the website is detected as phishing website, the user will be alerted with a pop-up box with an 'OK' button. If the website is not detected as phishing website, then no action will be taken. We have used various machine learning algorithms (Random Forest, etc.) along with Single Layer Perceptron to train the model. The train/test split rule for dataset were 80/20 respectively. The browser extension was written in JavaScript. The JavaScript file extracts features of URL such as browser popup, use of frames, shortening services, etc. and then applied the algorithm to detect whether the website is legitimate or not. The model was evaluated and on the basis of evaluation function such as accuracy, precision, recall, F1 score.

Keywords **- Phishing, Extension, URL, Random Forest, Feature extraction, Single Layer Perceptron.**

I. INTRODUCTION

With the increasing use of the internet and digital platforms, the risk of online attacks such as phishing has also increased significantly. Phishing is a form of online attack where cybercriminals create fake websites or emails that mimic legitimate ones to deceive users into providing sensitive information as shown in Fig. 1. This confidential data has the potential to be exploited for illicit activities such as financial fraud or identity theft. The need to protect one from such attacks has never been more urgent, and this is where the development of our model for detection and prevention of phishing websites using machine learning comes in picture. Machine learning is a branch of artificial intelligence that allows systems to learn and enhance their performance automatically based on experience. It involves creating algorithms capable of detecting data patterns and utilizing them to make predictions. In the context of our model for detection and prevention of phishing websites, machine learning algorithms are used to identify patterns in the data associated with websites, such as their URLs, HTML tags, and text content. By utilizing these patterns, the model can discern whether a website is genuine or deceptive. Developing a model for detecting and preventing phishing websites using machine learning is crucial in today's digital landscape. Phishing attacks are becoming increasingly sophisticated, and traditional methods of detecting and preventing such attacks are no longer sufficient.

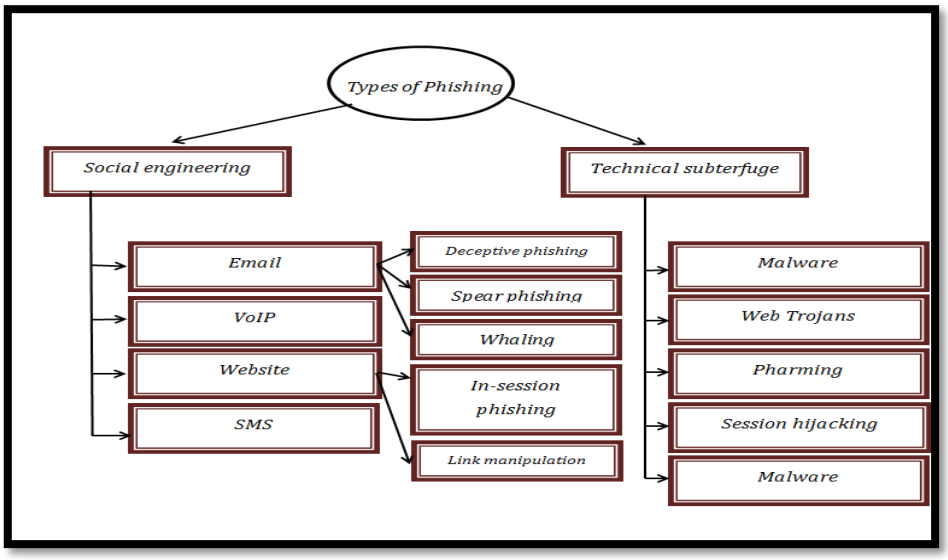

Figure 1: Types of Phishing

With the help of machine learning algorithms, the model can provide real-time protection against phishing attacks, allowing users to browse the internet with confidence.

II. LITERATURE SURVEY

Mohith Gowda et al. [1], A dataset consisting of 11,055 tuples is used to train the model. These processes are carried out on the client-side with the help of a redesigned browser architecture. For ease of access to the users they have improvised and introduced detection methods into the browser architecture named as 'Embedded Phishing Detection Browser' (EPDB), which is a novel method to preserve the existing user experience while improving its security. The system architecture for the model contains the following components User Interface, Browser Engine, Rendering Engine, Networking, UI Backend, Data Storage and the most important Intelligent Engine for detection of phishing attacks. The results shows that if the Intelligent Engine detects a Phishing Website it alerts the user with a pop-up box with two options as 'Back to Safety' and 'Continue'. Another set of result were if we compared various other classification models i.e., Logistic Regression and Support Machine Vector with the random forest classification model. The Random Forest Classification model showed an accuracy of 99.36%, with a F1 Score of 99.43%.

Patil and Dhage [2] The five approaches to anti-phishing are Rules based, Blacklisting, Content based, Machine Learning based and Hybrid. Anti-phishing tools such as Google Safe Browsing (GSB) and Netcraft, Mcfee Site Advisor, Avast and Quick Heal are used to protect against phishing websites. An effective framework for designing an anti-phishing model is presented, which involves URL gathering, feature collection, feature selection and classification. Heuristics and Hybrid approach perform best with 99.60 and 99.14% accuracy respectively.

Yang et al. [3] The paper proposes a multidimensional feature-based approach for detecting phishing, which employs a rapid deep learning detection method. The initial stage involves extracting character sequence features from the provided URL, which are then utilized for rapid categorization via deep learning. The second stage integrates various features such as statistical information about the URL, characteristics of the webpage's code, textual content of the webpage, and the outcome of the initial deep learning classification to form multi-dimensional features. The accuracy of the model reached 98.99% while the false positive rate was only 0.59%.

Xu et al. [4] This paper presents a method named "Gemini" that aims to protect users from inadvertently disclosing sensitive login information on phishing websites. It does not use appearance, but instead uses username. Prototypes of Gemini as a browser extension were implemented in Firefox, Chrome, and IE respectively. It works for pop-up login pages and searches the source of the page for elements like type= "password". Gemini data can be imported and exported, and is compatible with other anti-phishing tools. In the evaluation, two sets are sent for testing: legitimate sites and the other phishing ones.

Mughaid et al. [5] This paper reviews several methodologies for detecting phishing attacks, such as PILFER, Bhat et al.'s "Beaks", and Chiew et al.'s anti-phishing tool. PILFER employs a feature set of 10 characteristics such as URL grounded and script grounded features to identify phishing attacks, while Bhat et al.'s "Beaks" employs a spam filter to classify emails as spam or non-spam. Chiew et al.'s anti-phishing tool relies on a combination of structure-based and behavior-based features, such as the sender's name, blacklisted words in the subject and content, IP address in the URL, fleck and symbol in the URL, unique sender and sphere name, hyperlink consistency, and return path. To evaluate the effectiveness of phishing email detection, seven supervised classification algorithms were selected and utilized for training and testing purposes. The selected rate is 0.70 of the training set and 0.30 of the test, and feature selection ways need further enhancement to manage with the continuous development of new ways by the phishers.

Marchal et al. [6] Phishing is a lucrative cyber-crime that causes losses of several billion dollars every year. This paper creates an automated phishing detection system called Phish Storm which can analyze any URL in real-time to identify potential phishing sites with a correct classification rate of 94.91%. It uses the Phishing dataset and legitimate dataset to create a balanced dataset from which 12 features are selected to be used in supervised classification using random forest algorithm.

Zhu et al. [7] Phishing attack is now a big threat to people's daily life. During training dataset many useless and small influence features can cause problem of overfitting which causes inefficiency while detecting phishing websites. Based on FVV (Feature Validation Value), an algorithm is designed to select optimal features from fishing website to reduce overfitting problem and train neural network to detect phishing website. It considers various sensitive features in the start, from which, features are selected based on higher FVV. It uses Neural Network classifier with three layers for URL classification. A black and white list is first introduced to reduce time cost. For the URLs which are not in list, the neural network classifier is used to process this URL. This algorithm could properly deal with problems of big number of phishing sensitive features and the continuous change of features.

Shukla and Sharma [8] The paper designs a system using a Bayesian optimized Support Vector Machine classification approach to assign '1' if the address is secure, otherwise '0'. The system is provided with unclassified URLs and binary class output is expected. The URLs are collected, loaded, and divided into three parts: protocol, domain, and route. The results presented by the model require obtaining results with a higher level of accuracy, with a fault tolerance of 0.001%. After executing the URL function, a Bayesian optimized SVM classifier is used with a distribution of data of 40%.

Parthiban et al. [9] The proposed system introduces a new image verification process that creates a unique identity for each user. Images used for verification are encrypted using the RSA algorithm, so they cannot be used by third parties even when someone logs into the web wallet. If a single user is targeted for a phishing attack, hackers can create virtualization of custom image authentication, which requires more security in the future.

Su [10] this paper investigates heuristic detection methods such as CANTINA and CANTINA+ and visual similarity tests. The model uses the stochastic gradient descent (SGD) optimization method with an initial learning rate of 1 in 1000 and a batch size of 128. The dataset used was 2,000 legitimate websites collected by Yahoo Director and 2,000 phishing websites collected by Phish Tank. 70% of the dataset was allocated for training and the remaining 30% for testing purposes. The LSTM network employed in this study has 10 input layer nodes and one output layer node, with the aforementioned 10 features serving as the input.

III. METHODOLOGY

The development of a model for discovery and prevention of phishing websites using machine literacy requires a well-defined methodology. The methodology outlines the way involved in creating the model, from data collection to model deployment. This section discusses the methodology used in the development of our model, as shown in Fig. 2

Dataset

1. **Abnormal URL**: Checks whether URL is without hostname.
2. **'@' Symbol**: Checks whether URL contains '@' symbol.
3. **Sub domain**: Calculates the number of sub domain on the basis of dots present in URL
4. **URL requests**: Calculates percentage of number of times URL is requested
5. **Shortening services**: Checks whether the URL is too short.
6. **'HTTPS' token**: Checks whether the domain has HTTPS token or not.
7. **Server from handler (SFH)**: Checks whether SFH contain "about: blank" or "Is empty"
8. **URL with anchor**: Calculates the percentage of anchor URL
9. **Tag containing links**: Calculates the percentage of links in 'Script', 'Meta' and 'link'.
10. **Iframe**: Checks whether webpage makes use of iframe.
11. **IP Address**: Checks whether URL contains IP Address.
12. **Length of URL**: Calculates and checks whether the length of URL is too big.
13. **Double slash forwarding**: Checks whether the '//' in URL is within 7th character.
14. **Non-standard ports**: Checks whether the port number has preferred status
15. **Prefix and suffixes**: Checks whether domain contains '_'.
16. **Favicon**: Checks whether favicon is retrieved by external or internal source
17. **SSL final certificate**: Checks if URL is using https by trusted providers and certificate age.
18. **Age of domain**: Calculates the age of Domain.
19. **DNS record**: Checks whether the domain is with or without DNS record.
20. **Links pointing to page**: Calculates how many links are pointing to the Webpage.
21. **Domain registration length**: Checks the expiry date of Domain

Data Collection

The initial step is to gather data. Data collection involves the collection of a large dataset of both legit and fraudulent websites. The dataset should be large enough to capture the variability of the different types of phishing attacks. There are various styles for collecting data, analogous as web scraping or using being datasets. In this design, we used a dataset from Kaggle.

The link for the dataset can be found here.

Data Pre-processing

Once the data has been collected, the subsequent step involves pre-processing it. Data pre-processing encompasses cleaning and transforming the data to make it ready for analysis . This step is essential because it ensures that the data is of high quality and suitable for machine literacy algorithms. The pre-processing step entails removing duplicates, managing missing values, and transforming the data into a format that is appropriate for machine learning algorithms.

The above dataset was checked for missing values, null values, duplicates and other noise using box plot and other method. From the above dataset, the features that were not very useful for detection of the phishing were dropped.

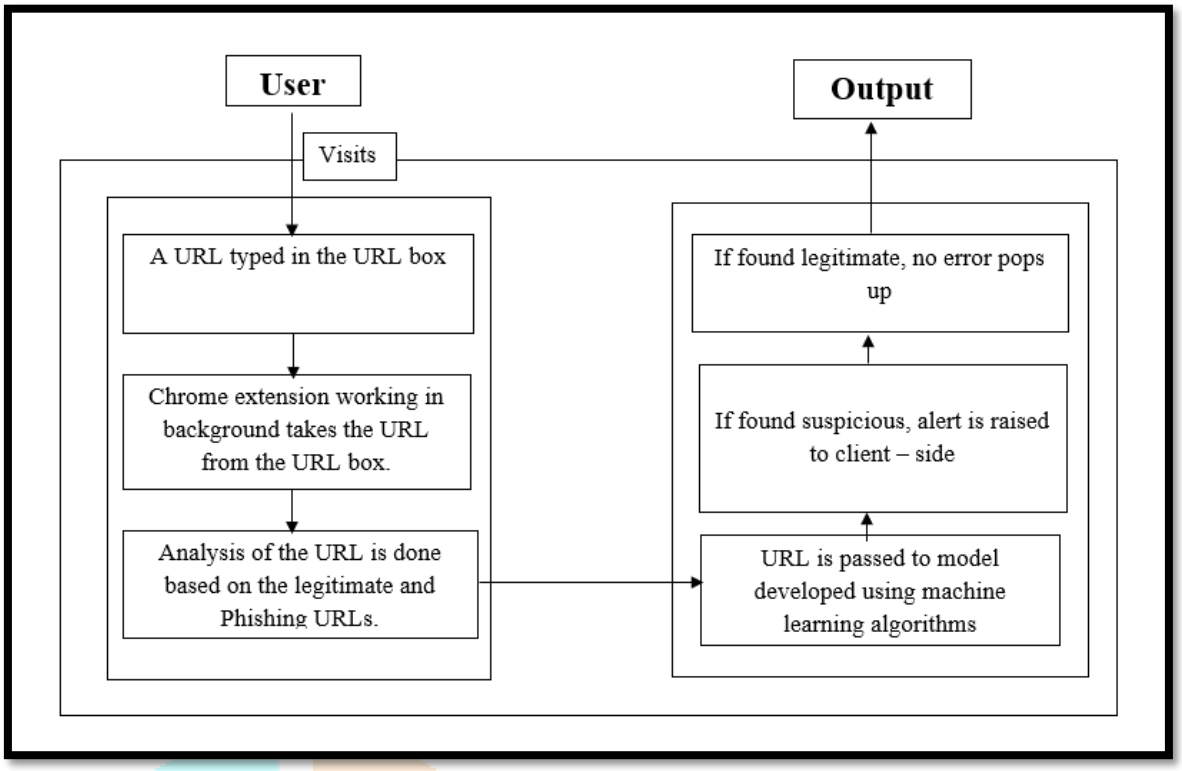

Figure 2: Design Methodology

Model Selection

The coming step is to handpick a machine literacy model. Model selection involves choosing the swish algorithm that can directly classify legit and fraudulent websites. There exists a variety of machine learning algorithms, such as Random Forest, Decision Tree, Support Vector Machines, Gradient Boosting Classifier, K-Nearest Neighbors, AdaBoost Classifier, Logistic Regression and others. In this design, we used a random forest algorithm.

For this project, we trained the model using various algorithms. For each the accuracy, F1-score, precision, recall was calculated. The algorithm which provided the best values was random forest. Hence, random forest was used for training and testing the model.

We have trained and evaluated our model using 22 parameters dataset and various algorithms. From all the algorithms used Random Forest provided the best accuracy. For the implementation of extension, 16 parameters were used and single layer perceptron was used to detect phishing websites.

Random Forest

Random Forest is a machine learning algorithm technique that is utilized for both classification and regression tasks. It is an ensemble method that chains multiple decision trees to make predictions. Random Forest is a powerful and versatile algorithm that is widely used in various applications, such as finance, healthcare, and marketing. Random Forest is a machine learning algorithm that creates multiple decision trees by randomly selecting subsets of the original dataset and features. This ensemble method aims to achieve better performance by combining the predictions of individual trees. This helps to reduce over fitting and increase the model's generalization ability The ultimate prediction of the Random Forest algorithm is determined by taking into account the majority vote of all the individual trees.

Single Layer Perceptron

A single-layer perceptron is a type of artificial neural network with one layer of nodes, which takes input values and produces a set of output values. The perceptron is a supervised learning algorithm used for classification tasks
where the output is a binary classification (i.e., two classes).

The single-layer perceptron consists of one or more input nodes, a set of weights, an activation function, and an output node. Each input node is connected to the output node by a set of weights, which are adjusted during training to minimize the error in the output. The activation function used in a perceptron is a threshold function, which determines whether the output of the perceptron is 0 or 1 based on the input and the weights.

Model Training

After concluding the machine learning algorithm, the coming step is to train the model. Model training involves feeding the model with the pulled features and their corresponding labels. The model is trained by learning from the data and adjusting its parameters to minimize errors. According to this, data is divided into a training set and a validation set. The training set is utilized to train the model, whereas the validation set is used to assess the performance of the model. In this particular study, 80% of the data from the aforementioned dataset was employed to train the model.

Model Evaluation

After training the model, the coming step is to estimate its performance. To evaluate the effectiveness of the model, it is tested on a separate test set that has not been used in training. The performance of the model is then measured using various metrics such as sensitivity, accuracy, and recall. These metrics help in determining the model's capability to detect and prevent phishing attacks.

20% of data is used for testing the model.

The development of a model for discovery and prevention of phishing websites using machine literacy requires a well-defined methodology. The methodology involves collecting data, preprocessing the data, lodging applicable features, concluding a machine knowledge model, training the model, assessing its performance, and planting the model. By following this methodology, we can develop a model that provides real-time protection against phishing attacks.

IV. RESULTS AND DISCUSSION

The extension shows an alert to the user when a phishing website is visited to save the user from any harm. For this to work the extension needs to be added in the browser by the user. Extension is implemented using single layer perceptron in deep learning after evaluating the accuracy of deep learning and various machine learning models.

The extension is to be first uploaded by going to the chrome::///extensions sections and the on Load unpacked as shown in the Fig. 3.

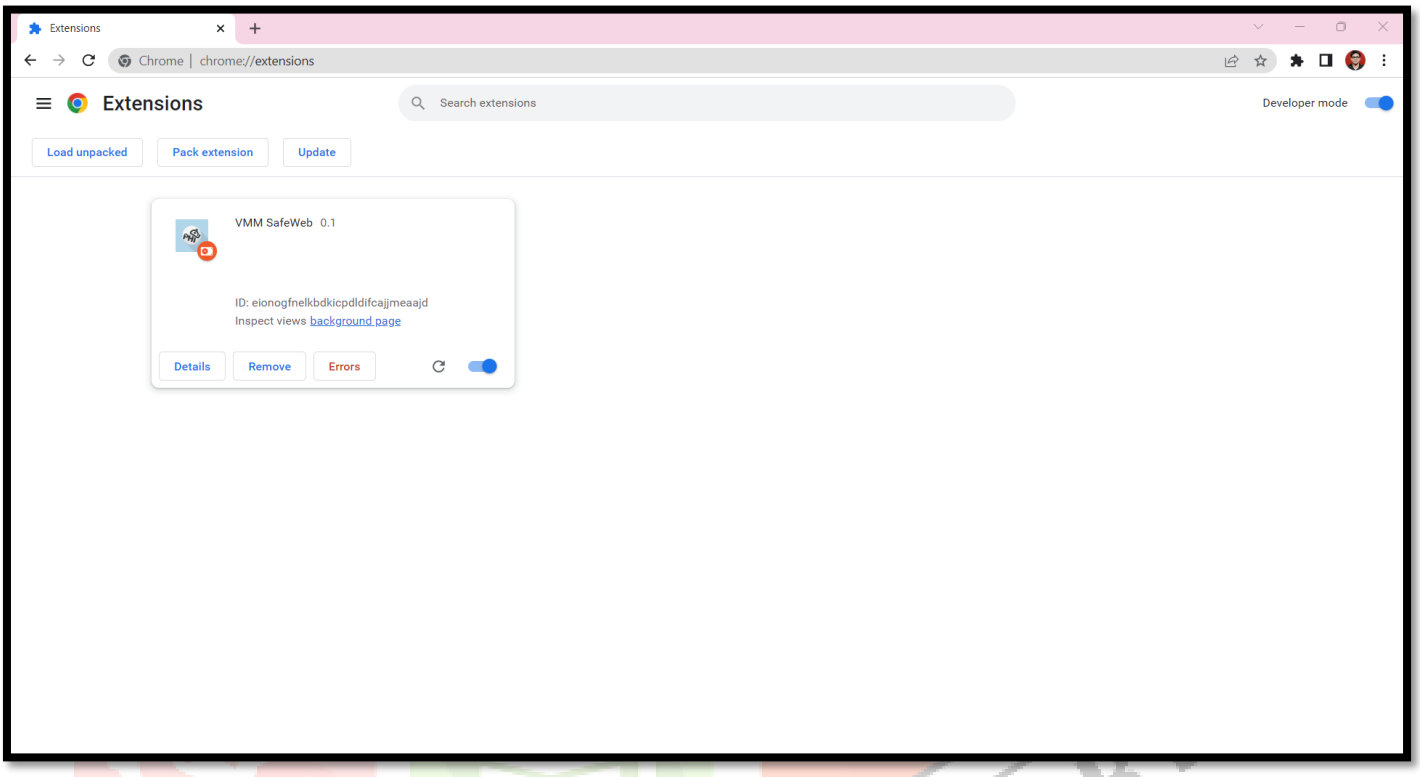

Figure 3: Loading Extension

The websites are detected as phishing based on various URL features. When any website is visited the URL of the website is extracted by extension, the extension then processes the URL to detect it as safe or phishing, this processing is done by JavaScript file(content.js).

If the URL is detected as phishing, then an alert is given in form of a popup to user else there is no popup. This alert is given with the use of background.js file as shown in Fig. 4.

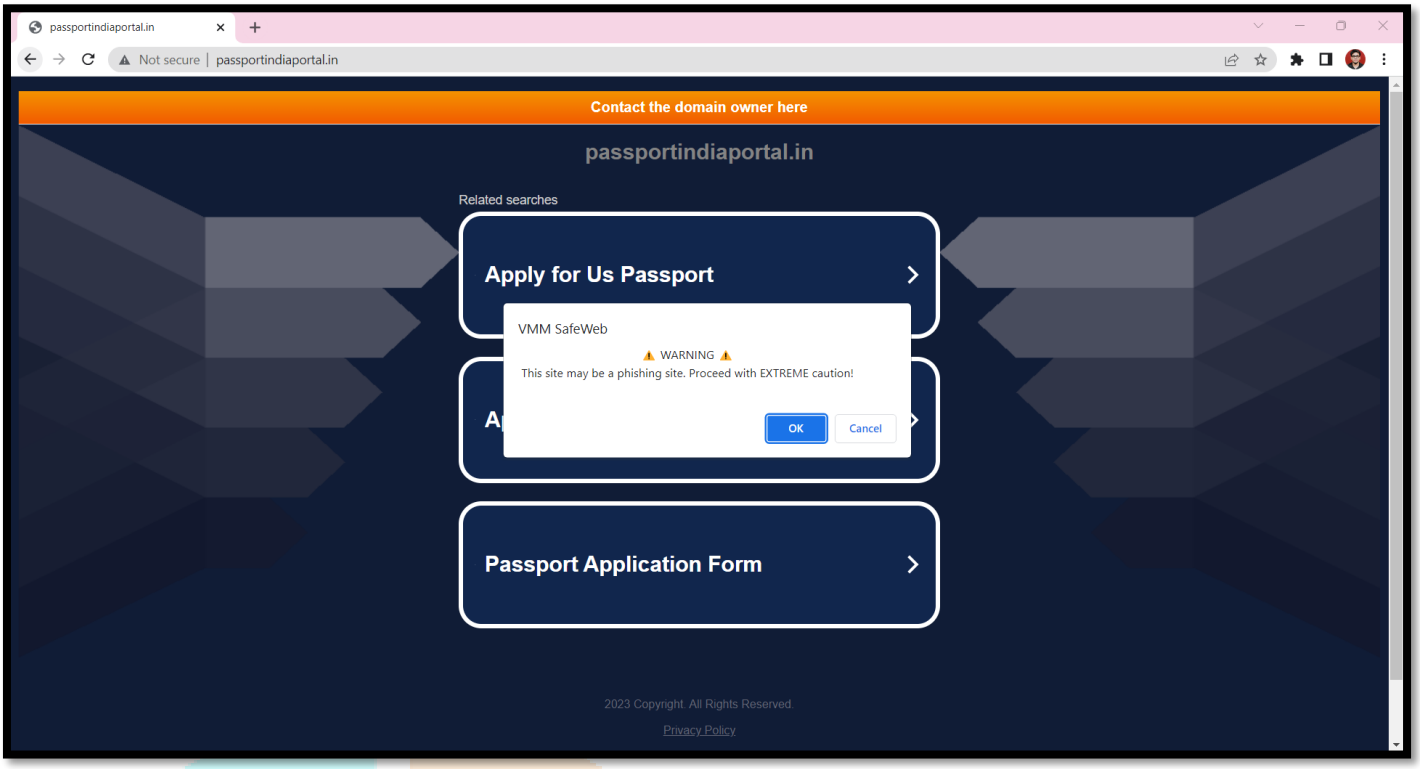

Figure 4: Phishing alert on sample website

After the website is detected as phishing the user is provided a form Fig. 5 to enter the URL, source of URL and location of the user. The location of the user is asked to protect them and others from such phishing URLs in their residing location and to get more information about the phishing attacks and avoid future attacks.

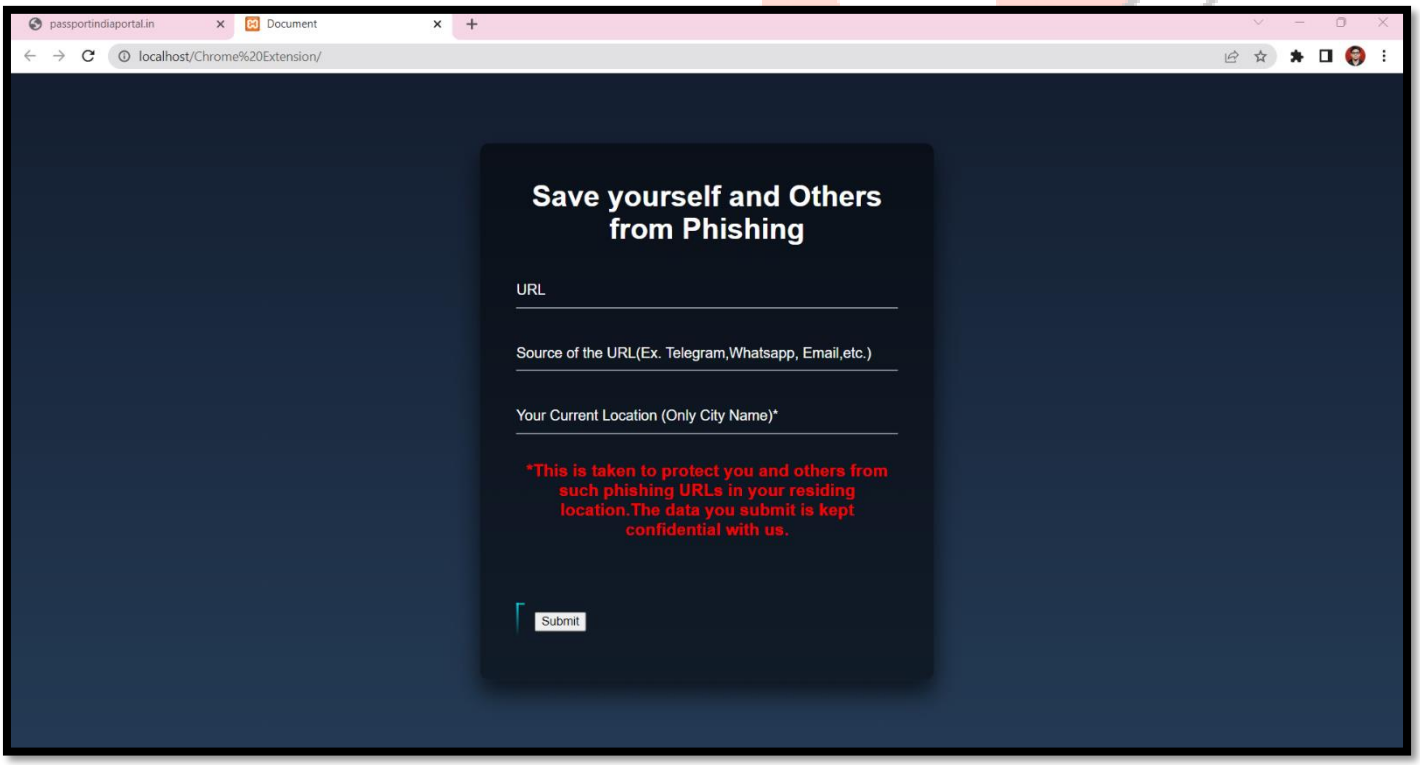

Figure 5: Form for credentials

The accuracies obtained by various machine learning algorithms (like Random Forest, Decision Tree, Support Vector Machines, Gradient Boosting Classifier, K-Nearest Neighbors, AdaBoost Classifier and Logistic Regression) are shown in table 1.

Table 1: Metrics of various Machine Learning Algorithms

Sr. No.	Classifier	Accuracy (in %)	Precision	Recall	F1-Score
1	Random Forest	96.11	0.96	0.96	0.96
2	Decision Tree	95.70	0.94	0.94	0.94
3	Support Vector Machines	94.57	0.56	1.00	0.72
4	Gradient Boosting Classifier	94.48	0.93	0.96	0.94
5	K-Nearest Neighbors	94.26	0.65	0.69	0.67
6	AdaBoost Classifier	93.48	0.92	0.96	0.94
7	Logistic Regression	93.39	0.92	0.95	0.94

V. CONCLUSION

In this work, we have proposed a system for detection and prevention of phishing websites. For that we have focused on URL classification of the websites. The dataset taken for this purpose contains 11055 tuples with 22 different features which has helped us to identify the website as phishing. The data present in the dataset is in the format of 1, 0, –1 which represents Legitimate, Suspicious and Phishing respectively. The Random Forest Algorithm was utilized for both training and testing of the model. The URL passed as the input to the model is first processed such that the 21 distinct features (apart from the Result i.e., is 22nd feature) are calculated in the format of 1, 0 and –1. The dataset is split into 80/20 ratio which gives us optimal data for good training and testing in order to prevent both under-fitting and overfitting of the model. The model classifies the input URL as Legitimate or Phishing with an accuracy of 96.11% having the n_estimators (i.e., number of trees in random forest) as 112.

VI. FUTURE SCOPE

As a part of the future scope, deep learning models like Recurrent Neural Network (RNN) or Generative Adversarial Network (GAN) can be used. Adding to that, we would like to notify the original users related to their phishing websites; for example, if a phishing website similar to www.microsoft.com is created, say www.microsooft.com, so, we would like to inform the original creator of the website regarding the phishing website that has been created under their name. Along with that, the type of websites which showcase a fake product and take away the money without receiving any products in exchange can be detected using web scraping and sentimental analysis.

VII. REFERENCES

[1] Mohith Gowda Hr1*, Adithya Mv2, Gunesh Prasad S3 And Vinay S4. Development of anti-phishing browser based on random forest and rule of extraction framework. Spinger.

[2] Srushti Patil, Sudhir Dhage. A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework, 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). 2019 IEEE. 10.1109/ICACCS.2019.8728356

[3] Peng Yang, Guangzhen Zhao, Peng Zeng. Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning. IEEE Access 2019. Digital Object Identifier 10.1109/ACCESS.2019.2892066

[4] Zhang Xu, Haining Wang, Sushil Jajodia. Gemini: An Emergency Line of Defence against Phishing Attacks. 2014 IEEE. 10.1109/SRDS.2014.26

[5] Ala Mughaid, Shadi AlZu'bi, Adnan Hnaif, Salah Taamneh, Asma Alnajjar, Esraa Abu Elsoud. An intelligent cyber security phishing detection system using deep learning techniques. 2022. 10.1007/s10586-022-03604-4

[6] Samuel Marchal,Jerome Francois, Radu State, Thomas Engel. PhishStorm: Detecting Phishing with Streaming Analytics. 2014 IEEE. DOI: 10.1109/TNSM.2014.2377295

[7] Erzhou Zhu, Yuyang Chen, Chengcheng Ye, Xuejun Li, Feng Liu. OFS-NN: An Effective Phishing Websites Detection Model Based on Optimal Feature Selection and Neural Network Volume 7. 2019. DOI: 10.1109/ACCESS.2019.2920655

[8] Shrishti Shukla,.Pratyush Sharma. Detection of Phishing URL using Bayesian Optimized SVM Classifier. 2020. DOI: 10.1109/ICECA49313.2020.9297412

[9] R. Parthiban, V. Abarna, M. Banupriya, S. Keethana, D. Saravanan. Web folder phishing discovery and prevention with Customer image verification IEEE. 2020. DOI: 10.1109/ICSCAN49426.2020.9262395

[10] SU Yang. Research on Website Phishing Detection Based on LSTM RNN. 2020. DOI: 10.1109/ITNEC48623.2020.9084799N

[11] Ishita Saha, Mohammad Nazmul Alam, Dhiman Sarma, Asma Sultana, Rana Joyti Chakma, Sohrab Hossain. Phishing Attacks Detection using Deep Learning Approach. 2020. DOI: 10.1109/ICSSIT48917.2020.9214132

[12] Fortinet: https://www.fortinet.com

[13] Coursera: https://www.coursera.org/articles/machine-learning-models

[14] Detection of URL based Phishing Attacks using Machine Learning – IJERT
[15] Geeks for Geeks: https://www.geeksforgeeks.org/data-preprocessing-in-data-mining/
[16] Ionut Cernica, Nirvana Popescu. Computer vision based framework for detecting phishing webpages. 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)
[17] Junaid Rashid, Toqeer Mahmood, Muhammad Wasif Nisar, Tahira Nazir. Phishing Detection Using Machine Learning Technique. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)
[18] Abdul Basit, Maham Zafar, Abdul Rehman Javed, Zunera Jalil. A Novel ensemble machine learning method to detect phishing attack. 2020 IEEE 23rd International Multitopic Conference (INMIC)
[19] Yohanes Priyo Atmojo, Made Darma Susila, Muhammad Riza Hilmi, Erma Sulistyo Rini, Lilis Yuningsih, Dandy Pramana Hostiadi. A New Approach for Spear phishing Detection. 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT)
[20] B. Janet, Yazhmozhi. V.M, Srinivasulu Reddy. Anti-phishing System using LSTM and CNN. 2020 IEEE International Conference for Innovation in Technology (INOCON)