# Phishing Detection in Browsers using Machine Learning

Tanmay Naik
*Khoury College of Computer Sciences*
*Northeastern University*
Boston, US
naik.t@northeastern.edu

Nithin Gangadharan
*Khoury College of Computer Sciences*
*Northeastern University*
Boston, US
gangadharan.n@northeastern.edu

***Abstract*—Phishing is a cybercrime in which a target visits a website that is posing as a legitimate application, to lure individuals into providing sensitive data such as - banking and credit card details, and passwords. An unsuspecting user can click a link in an email or social media platform, and be led to a phishing website, leading to frauds and identity thefts. Phishing is a widespread attack that still does not have a concrete solution.**

**This report proposes a solution for the protection of end users through a browser extension while comparing various Machine Learning approaches to identify phishing websites. // TODO add "the most important results and findings"**

## I. Introduction

With the recent advancement in various cybersecurity technology, the weakest link in the cybersecurity happen to be the end users. Attackers utilize phishing which exploits naivety of users to trick them into handing out sensitive information. This poses a great risk not only to the users themselves but the organizations and institutions of which they are a part of. According to recent research from Proofpoint, 75% of organizations around the world experienced a phishing attack in 2020, and 74% of attacks targeting US businesses were successful.[1]

Apart from increasing security awareness among users, the tools which complement that awareness to help users make safe decisions must be developed. This report proposes and demonstrates a Chromium-based browser extension to help mitigate the risk of phishing while browsing the web. The central idea of the browser extension is to notify the user whenever they open any *potential* phishing website.

The solution also includes a Python web server which utilizes various Machine Learning classification techniques to determine the legitimacy of the webpage in question. The web server takes in a URL and returns a boolean value indicating if the given URL is part of a potential phishing attempt.

The browser extension monitors each URL that the user visits, and tries to determine if the URL is malicious with the help of the web server. The web server exposes a REST API which is consumed by the extension for communication. The same API can also be reused as-is to implement a similar phishing detection in a different context like a network-level application or in a mobile application like Android.

//TODO "summary of experimental results which is more fine-grained than abstract."

## II. Related Work

*a) PhishDetector[2]:* This too is a Chromium extension which has set out to solve exactly the same problem as this project. Based to its description on the website and the analysis of its behavior, it can be concluded that this extension uses a rule-based system to determine if a webpage is a phishing attempt. It also seems to be particularly accurate when it comes to identifying illegitimate banking pages. Even though rule-based systems are great for detecting simple phishing attempts, they are not ideal for more sophisticated phishing attempts. Rule-based systems are also inherently complex to maintain - adding and modifying rules over time makes the system more complex and unmanageable with time. They also demand more human intervention to define the rules and for their maintenance. Using Machine Learning in lieu of rule-based system gets rid of many of these limitations. As Machine Learning is data centric, it doesn't require managing complex rules and makes it straightforward to tweak the algorithms.

*b) Cloudphish[3]:* Cloudphish is a phishing detector for web-based email software. It monitors all emails received by a user and checks each email for a phishing attack. Having a paid subscription model, it offers a *decent* service. But the major limitation it has is that it works only with the email inbox. Even though many of the phishing attacks are carried over through email, phishing is as prominent on social media and messaging apps in this age. And that calls for a solution which monitors all the web activity to identify phishing attacks regardless of their method of delivery.

There are various other browser extensions which virtually have the same limitations as the aforementioned solutions[4][5][6] As their limitations are encompassed in the discussion of other solutions above, their detailed discussion has been omitted for brevity.

To summarize, there are various browser plugins consisting of rule-based systems, simple whitelists-blacklists and some even making use of Machine Learning and Artificial Intelligence. But there needs to be a solution which utilizes all available phishing detection methods to protect the average internet user from criminals.

## III. Approach

The architecture of this project consists of two primary components: The browser extension and the web server.

*a) Browser Extension:* The extension is developed for Chromium-based browsers using JavaScript with HTML and CSS. Therefore it is compatible with any Chromium implementation including Google Chrome, Microsoft Edge, Brave, etc. The extension monitors each web page that is visited by the user and fetches the URL of that webpage. It then communicates with the web server which tells if the given URL is part of a phishing attempt or not. The user is notified with the results of the analysis based on the response from server. The extension will stay silent in the background while the user is only visiting safe sites. It only *bothers* them when there is a potential of phishing on the site they are currently visiting with an option to view detailed information to help them make a safer decision.

*b) Python Web Server:* The web server has an REST endpoint which takes in a URL and uses various Machine Learning techniques to classify it into categories. It extracts relevant "features" from the URL and feeds them to *Classification Models* to determine the legitimacy of the URL. This process is expanded upon further down in this section.

Classification is a process of categorizing a given set of data into classes. In this case, there would be two classification labels: "spam" and "not spam". And the input data would be values of various features of the URL which are deemed effective for high quality classification of any URL into one of the classes.

The process of creating a classification model consists of two primary stages. The first is the training stage where a classifier is fed a large amount of input with along with their respective class labels. That creates a classification model which is given a set of inputs without their respective labels to let it classify each input to a class. That constitutes the second stage where the correctness of the newly created classification model is compared against the actual labels. The input set given to the model for the second stage is often referred to as *testing dataset* and the data used for the first stage is called *training dataset*. As a common practice, the dataset on hand is split into training and testing datasets for creation and testing of the classification models, respectively.

The classifiers used in this project are described below:

1) Decision Trees: Decision Trees belong to the family of supervised machine learning algorithms. Decision trees classify the input by running them down the tree from the root node to some leaf node, whereas the leaf node provides the classification of the input.
2) K-Nearest Neighbors (KNN): The KNN algorithm assumes that similar things are *near* to each other. Based on this assumption, it classifies all nearby data points into one. Then, it classifies the given input by locating N-nearest neighbors and finding mode of their labels which is predicted to be the label of the input set.
3) Random Forests: Random Forests consist of a large number of Decision Trees that operate as an ensemble. Each tree in a forest classifies the given input set to a label and the label with the highest number of votes is considered as the prediction of the Random Forest.
   The individual trees in a random forest are relatively *uncorrelated*, and they perform better as an ensemble than they would on their own. To put it in layman's terms, the trees safeguard each other from their individual errors.

The following section describes the datasets used for training and testing the models with the aforementioned classifiers.

1) Phishing Websites Dataset:[7] This dataset has 11,055 datapoints with 6,157 legitimate URLs and 4,898 phishing URLs. And it contains 30 features subdivided into three categories:
   a) Features based on the domain and subdomains
   b) Features derived from the other parts of the URL
   c) Features derived from the webpage HTML and JavaScript
2) Datasets for phishing websites detection:[8] This dataset consists of 111 features, of which 97 are based on the URL. For the phishing websites, the list was extracted from the PhishTank registry which are verified by multiple users. And for sets of legitimate websites, the publicly available and community labeled lists are utilized.[9]

Before the URL to be tested is sent to any of the Machine Learning models, they are checked against a whitelist. The whitelist is extracted from The Majestic Million dataset[10] which maintains a list of top 1 million domains on the internet. The whitelist helps in reduce processing and network overhead of checking the most popular sites which would be visited by an average user on a day to day basis.

The machine learning models trained with both datasets are precomputed and stored on the server. If the given domain is not part of the whitelist, the URL is then passed on to these models. Whenever the server receives a URL to be tested, it extracts all the features from the given URL. Many of the features are extracted through string parsing and the rest of them require use of external APIs and libraries. For example, PageRank of a given domain is fetched using Open PageRank API.[11]

After extracting the relevant features for each dataset, they are passed on to the classification models and their ensembles. And the result it sent back based on the outputs of the various models.

## IV. Experiments and Results

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Commodo quis imperdiet massa tincidunt nunc pulvinar sapien et ligula. Elit pellentesque habitant morbi tristique senectus et netus et. Tempus quam pellentesque nec nam aliquam sem et. Risus sed vulputate odio ut enim blandit volutpat maecenas. Amet commodo nulla facilisi nullam vehicula ipsum a arcu. Adipiscing tristique risus nec feugiat in fermentum posuere urna. Sit amet consectetur adipiscing elit pellentesque habitant morbi. Auctor eu augue ut lectus arcu bibendum at varius vel. Blandit volutpat maecenas volutpat blandit. Ac tortor vitae purus faucibus ornare suspendisse sed nisi lacus.

Vitae aliquet nec ullamcorper sit. Quis auctor elit sed vulputate. Fermentum dui faucibus in ornare quam. Vehicula ipsum a arcu cursus. Egestas congue quisque egestas diam in arcu cursus euismod. Elementum integer enim neque volutpat ac tincidunt vitae. Dui vivamus arcu felis bibendum. Id neque aliquam vestibulum morbi blandit cursus risus at ultrices. Mauris vitae ultricies leo integer malesuada nunc. Ultrices sagittis orci a scelerisque purus semper eget duis.

Sed lectus vestibulum mattis ullamcorper velit. Porttitor massa id neque aliquam. Amet nisl suscipit adipiscing bibendum. Quam quisque id diam vel quam elementum. Amet dictum sit amet justo donec enim diam vulputate. Purus sit amet luctus venenatis lectus magna fringilla. Eget aliquet nibh praesent tristique magna. Viverra nam libero justo laoreet sit amet cursus sit. Neque sodales ut etiam sit amet. Nullam ac tortor vitae purus faucibus ornare.

Lorem ipsum dolor sit amet consectetur adipiscing. Tortor condimentum lacinia quis vel eros donec ac odio. Nibh praesent tristique magna sit amet purus gravida quis blandit. Sed augue lacus viverra vitae congue eu consequat. Rhoncus est pellentesque elit ullamcorper dignissim cras tincidunt lobortis feugiat. Sit amet volutpat consequat mauris nunc congue. Convallis posuere morbi leo urna molestie. A diam maecenas sed enim ut sem viverra aliquet. Etiam tempor orci eu lobortis elementum nibh tellus molestie. Placerat duis ultricies lacus sed turpis tincidunt id aliquet risus. Convallis aenean et tortor at risus viverra adipiscing at in. Ut etiam sit amet nisl purus. Interdum velit laoreet id donec ultrices tincidunt arcu. Magna eget est lorem ipsum. Ultricies mi eget mauris pharetra et ultrices neque ornare aenean. Massa massa ultricies mi quis hendrerit. Non arcu risus quis varius quam quisque id. Est placerat in egestas erat imperdiet sed euismod.

Arcu non odio euismod lacinia at quis. In nisl nisi scelerisque eu ultrices vitae auctor. At erat pellentesque adipiscing commodo elit at imperdiet. Morbi tristique senectus et netus et malesuada fames ac turpis. Aliquam malesuada bibendum arcu vitae elementum curabitur vitae nunc. Sem viverra aliquet eget sit amet tellus. Nec ultrices dui sapien eget mi proin sed libero enim. Lacus vestibulum sed arcu non odio euismod. Et pharetra pharetra massa massa ultricies mi quis hendrerit dolor. Diam quis enim lobortis scelerisque. Tempus imperdiet nulla malesuada pellentesque elit. Purus viverra accumsan in nisl. Nam libero justo laoreet sit amet cursus sit amet. Orci dapibus ultrices in iaculis nunc sed augue. Feugiat scelerisque varius morbi enim nunc. Senectus et netus et malesuada fames ac turpis.

Placerat orci nulla pellentesque dignissim enim sit. Quam pellentesque nec nam aliquam. Sit amet porttitor eget dolor morbi non arcu risus quis. Nec feugiat in fermentum posuere urna. Metus dictum at tempor commodo ullamcorper a lacus vestibulum sed. Nibh cras pulvinar mattis nunc sed blandit libero. Amet mattis vulputate enim nulla aliquet porttitor lacus luctus. Aenean pharetra magna ac placerat vestibulum lectus. Eleifend mi in nulla posuere. Purus faucibus ornare suspendisse sed nisi.

Habitant morbi tristique senectus et netus. Ac tortor vitae purus faucibus ornare suspendisse sed nisi lacus. Mattis nunc sed blandit libero volutpat sed cras ornare arcu. Leo integer malesuada nunc vel. Sed lectus vestibulum mattis ullamcorper velit sed ullamcorper morbi tincidunt. Risus sed vulputate odio ut enim blandit. Amet massa vitae tortor condimentum lacinia. Quam elementum pulvinar etiam non quam lacus suspendisse faucibus. Sed lectus vestibulum mattis ullamcorper velit sed. Dignissim enim sit amet venenatis urna cursus eget nunc scelerisque. Sed tempus urna et pharetra pharetra massa. Turpis egestas maecenas pharetra convallis posuere.

Sed vulputate odio ut enim blandit. Sed elementum tempus egestas sed. Tempor orci dapibus ultrices in iaculis nunc. Arcu cursus euismod quis viverra nibh cras pulvinar mattis nunc. Nunc eget lorem dolor sed viverra ipsum nunc. A diam sollicitudin tempor id eu nisl nunc. Sed lectus vestibulum mattis ullamcorper. Lacus suspendisse faucibus interdum posuere lorem ipsum dolor. Dictum sit amet justo donec enim diam vulputate ut pharetra. Lorem donec massa sapien faucibus. Habitasse platea dictumst vestibulum rhoncus est pellentesque. Vitae proin sagittis nisl rhoncus mattis rhoncus urna neque. Elit duis tristique sollicitudin nibh. Amet luctus venenatis lectus magna fringilla urna porttitor rhoncus. Vulputate odio ut enim blandit volutpat maecenas volutpat. Fames ac turpis egestas maecenas pharetra convallis posuere morbi leo. Mattis pellentesque id nibh tortor id. Neque gravida in fermentum et sollicitudin. Iaculis eu non diam phasellus vestibulum lorem.

Aliquam sem et tortor consequat id porta. Fringilla urna porttitor rhoncus dolor purus non. Pellentesque eu tincidunt tortor aliquam nulla facilisi cras. Tincidunt lobortis feugiat vivamus at. Cursus turpis massa tincidunt dui ut. Leo duis ut diam quam. Et malesuada fames ac turpis egestas. Purus faucibus ornare suspendisse sed nisi. Aliquet porttitor lacus luctus accumsan. Amet dictum sit amet justo. Aliquam nulla facilisi cras fermentum odio eu feugiat pretium. Mi in nulla posuere sollicitudin aliquam ultrices sagittis. Dolor morbi non arcu risus quis. Eu tincidunt tortor aliquam nulla facilisi cras fermentum odio eu. Leo integer malesuada nunc vel risus commodo viverra. Platea dictumst quisque sagittis purus sit amet. Ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim. Sagittis eu volutpat odio facilisis. Nisi quis eleifend quam adipiscing vitae proin sagittis nisl.

Tempus imperdiet nulla malesuada pellentesque elit eget gravida cum sociis. Gravida neque convallis a cras semper auctor. Elementum nibh tellus molestie nunc non blandit massa. Ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim. Nulla pharetra diam sit amet nisl suscipit adipiscing. Molestie at elementum eu facilisis sed odio morbi quis. Egestas congue quisque egestas diam. Purus gravida quis blandit turpis cursus in. Egestas sed tempus urna et pharetra pharetra massa massa. Ultrices tincidunt arcu non sodales neque sodales ut etiam sit. Molestie nunc non blandit massa enim nec dui nunc mattis. Sollicitudin ac orci phasellus egestas tellus rutrum. Orci phasellus egestas tellus rutrum tellus pellentesque eu. Placerat duis ultricies lacus sed. Morbi tincidunt augue interdum velit euismod in. Faucibus vitae aliquet nec ullamcorper sit amet risus nullam. In hac habitasse platea dictumst quisque sagittis purus sit. Dictum at tempor commodo ullamcorper.

Tellus at urna condimentum mattis pellentesque id. Sed libero enim sed faucibus turpis. Adipiscing bibendum est ultricies integer quis auctor elit. Mattis enim ut tellus elementum sagittis vitae et leo. Risus feugiat in ante metus dictum at tempor commodo ullamcorper. Nec tincidunt praesent semper feugiat nibh sed. Adipiscing elit duis tristique sollicitudin nibh. Scelerisque purus semper eget duis at tellus at. Risus in hendrerit gravida rutrum quisque non tellus orci ac. Lectus sit amet est placerat in egestas erat. Non arcu risus quis varius quam quisque. Ullamcorper malesuada proin libero nunc consequat. At augue eget arcu dictum. Adipiscing bibendum est ultricies integer quis. Habitasse platea dictumst vestibulum rhoncus est pellentesque. Lorem ipsum dolor sit amet consectetur adipiscing. Massa enim nec dui nunc mattis. Habitasse platea dictumst quisque sagittis purus.

At elementum eu facilisis sed odio. A scelerisque purus semper eget duis at tellus at urna. Aliquam etiam erat velit scelerisque in dictum non consectetur a. Cursus vitae congue mauris rhoncus. Tincidunt eget nullam non nisi est sit. Amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar. Enim tortor at auctor urna nunc id cursus. Sed velit dignissim sodales ut eu sem. Quam id leo in vitae turpis massa sed. Purus gravida quis blandit turpis cursus in hac habitasse platea. Nunc faucibus a pellentesque sit amet porttitor eget. Amet commodo nulla facilisi nullam. Urna molestie at elementum eu.

Vel risus commodo viverra maecenas accumsan lacus. Sit amet mattis vulputate enim. Ut tortor pretium viverra suspendisse potenti nullam ac tortor. Morbi non arcu risus quis varius quam quisque id. Risus ultricies tristique nulla aliquet enim tortor at. Eu scelerisque felis imperdiet proin fermentum leo vel. Nulla pharetra diam sit amet nisl suscipit adipiscing bibendum. Enim eu turpis egestas pretium aenean pharetra. Non consectetur a erat nam. Phasellus faucibus scelerisque eleifend donec pretium vulputate sapien nec sagittis. Elit ut aliquam purus sit amet luctus venenatis lectus magna. Feugiat vivamus at augue eget arcu dictum varius. Turpis egestas maecenas pharetra convallis posuere morbi leo urna molestie. Vitae purus faucibus ornare suspendisse sed nisi lacus sed. Ultrices tincidunt arcu non sodales neque sodales. Elit duis tristique sollicitudin nibh sit. Elit at imperdiet dui accumsan sit amet nulla facilisi morbi. Quisque egestas diam in arcu cursus euismod quis viverra. Non quam lacus suspendisse faucibus interdum posuere lorem. Ultricies lacus sed turpis tincidunt id aliquet risus.

## V. Conclusion and Future Work

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Sagittis purus sit amet volutpat consequat mauris. Nec feugiat nisl pretium fusce id. Sapien faucibus et molestie ac feugiat sed lectus vestibulum mattis. Faucibus interdum posuere lorem ipsum dolor. Viverra nibh cras pulvinar mattis nunc sed blandit libero volutpat. Mauris nunc congue nisi vitae suscipit tellus mauris a diam. Vel turpis nunc eget lorem dolor. Interdum velit euismod in pellentesque massa. Adipiscing bibendum est ultricies integer quis auctor elit. Elit pellentesque habitant morbi tristique senectus et netus et. Odio pellentesque diam volutpat commodo sed egestas egestas fringilla phasellus. Senectus et netus et malesuada fames ac turpis. In aliquam sem fringilla ut morbi tincidunt augue interdum velit. Aliquam sem fringilla ut morbi tincidunt augue interdum velit euismod.

## VI. Appendices

Optional

## VII. Contributions

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Felis eget velit aliquet sagittis id. Interdum velit euismod in pellentesque massa. Felis eget nunc lobortis mattis aliquam faucibus purus in. Mauris ultrices eros in cursus turpis. Commodo nulla facilisi nullam vehicula ipsum. Mi sit amet mauris commodo quis imperdiet massa. Tincidunt nunc pulvinar sapien et. Dolor sit amet consectetur adipiscing elit pellentesque. Non curabitur gravida arcu ac tortor dignissim convallis aenean et. Felis imperdiet proin fermentum leo vel orci porta non pulvinar. Malesuada nunc vel risus commodo viverra maecenas accumsan lacus vel.

Feugiat sed lectus vestibulum mattis ullamcorper velit sed. Ornare quam viverra orci sagittis eu volutpat. Turpis massa sed elementum tempus. Felis eget velit aliquet sagittis id consectetur purus. Cursus metus aliquam eleifend mi in nulla posuere sollicitudin aliquam. Nulla facilisi morbi tempus iaculis urna id volutpat lacus. Arcu felis bibendum ut tristique et egestas. A erat nam at lectus urna. Id donec ultrices tincidunt arcu non. Adipiscing tristique risus nec feugiat in fermentum posuere urna. Etiam tempor orci eu lobortis elementum nibh tellus molestie. Bibendum ut tristique et egestas quis ipsum. Sollicitudin tempor id eu nisl nunc mi ipsum faucibus.

## References


[1] Proofpoint, "Threat report: 2021 state of the phish report." [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[2] M. Moghimi, "Phishdetector - true phishing detection." [Online]. Available: https://chrome.google.com/webstore/detail/phishdetector-true-phishi/kgecldbalfgmgelepbblodfoogmjdgmj

[3] Cloudphish, "Cloudphish anti-phishing extension." [Online]. Available: https://chrome.google.com/webstore/detail/cloudphish-anti-phishing/fcahokjdmffdhglnlhgbceafccfdfjkd?hl=en

[4] B. Arca, "Blue arca anti-phishing extension." [Online]. Available: https://chrome.google.com/webstore/detail/blue-arca-anti-phishing-e/nbladngkelnbhcinepiogponadjggkcd?hl=en

[5] Retruster, "Retruster phishing protection." [Online]. Available: https://chrome.google.com/webstore/detail/retruster-phishing-protec/akcpbmbdplmbhlpeglpbghnkcbhiapil?hl=en
[6] A. Zuelsdorf, "Phishing boat." [Online]. Available: https://chrome.google.com/webstore/detail/phishing-boat/ljaiihgfejfaggbjfildfnjdckomlfop?hl=en
[7] M. et al, "Phishing websites data set by uci." [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Phishing+Websites
[8] G. Vrbančič, "Datasets for phishing websites detection." [Online]. Available: https://archive.ics.uci.edu/ml/datasets/Phishing+Websites
[9] T. C. Lab, "Test lists." [Online]. Available: https://github.com/citizenlab/test-lists
[10] Majestic, "Majestic top 1 million websites." [Online]. Available: https://majestic.com/reports/majestic-million
[11] O. P. initiative, "Open pagerank api." [Online]. Available: https://www.domcop.com/openpagerank/