JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

FRAUD FENCE
A PHISHING SHIELD FOR WEBSITES

Prof. Reena Deshmukh, Aishwarya Nehete, Sampada Payal, Riddhi Radia [1]Assistant Professor Professor , Student[2,3,4],
Department of Computer Engineering, University of Mumbai, Shivajirao S. Jondhale College of Engineering Maharashtra

Abstract: In today's fast-evolving technological landscape with a burgeoning number of internet users and data, the need for a web browser extension dedicated to detecting phishing websites has become more critical than ever. Users struggle to differentiatebetween legitimate and fraudulent websites, making their personal and financial information increasingly vulnerable. Cybercriminals have refined their methods, further complicating the identification of fraudulent webpages, elevating the risk to personal and financial information to unprecedented levels. The existing system for phishing website detection faces several drawbacks, including a limited dataset and reduced accuracy. In response to these challenges, the demand for phishing detection extensions has surged. We have implemented an extension that utilizes machine learning techniques, including the Random Forest algorithm, multilayer perceptron, support vector machine to autonomously detect various features. FraudFence serves safeguarding users from the ever- present risk of online fraud, ensuring a secure digital experience. FraudFence-A Phishing Shield for Websites is a crucial line of defense, diligently scanning websites and issuing timely alerts when potential phishing attempts are identified. It plays a pivotal role in safeguarding users from the ever-present threat of online fraud.

Keywords **- FraudFence, Phishing, Web Extension.**

I. INTRODUCTION

In today's era of rapid technological advancement and the exponential growth of internet users and data, the need fora phishing detection extension for web browsers becomes increasingly critical. With the sheer volume of websites visited during online activities, it has become incredibly challenging for users to distinguish between legitimate and potentially fraudulent websites. Attackers have honed their skills, making it even harder to identify these deceptive sites. As a result, the risk to personal and financial information is higher than ever before [8].

These phishing detection extensions are the much-needed defense mechanism in this digital landscape. They act as avital safeguard, diligently scanning websites and raising alerts when potential phishing attempts are detected. By doingso, they play a pivotal role in protecting users from the ever-present threat of online fraud.

Given the prevalence of online threats, the role of these extensions in maintaining a secure online environment cannotbe overstated. They provide users with the peace of mind and confidence they need to navigate the internet safely, safeguarding their personal data and financial assets. In summary, the expansion of the internet and the sophisticationof cyber attackers make phishing detection extensions indispensable for ensuring secure browsing experiences in themodern digital age.

II. LITERATURE SURVEY

The literature survey encompassed an examination of 7 research papers focusing on the detection of phishing attackson websites. Various techniques were employed in these papers, such as content-based extraction, the application ofthe Random Forest algorithm [1][2][3], and logistic regression [3]. Some systems adopted a traditional listing approach[5][6]. The 'SAFE- PC' system utilized a corpus phishing message-based approach and incorporated NLP techniques like Named Entity Recognition [4]. Notably, PhishCatcher[1], AntiPhishing system [5], and Phishing website detection [3] either trained models using small datasets or relied on data collected from a single data source. Severalof these systems necessitated manual data input from users [4][5][6]. It's important to note that all the surveyed systems issued phishing alerts but do not redirect to a safe web page if the visited website is phished.[1][2][3][4][5][6][7].

III. METHODOLOGY

The FraudFence Chrome extension is designed to enhance user security by identifying and alerting them to potential phishing websites. It operates in real-time, actively monitoring the websites visited by the user. Utilizinga combination of advanced algorithms and heuristics, it scrutinizes various aspects of web pages, including content, URL composition, and server behavior.

When the extension identifies a website that exhibits characteristics indicative of phishing, it takes immediate action to protect the user. This action may include displaying a warning message, advising the user to exercise caution, or even redirecting the user to safer web page. By leveraging this comprehensive approach to web safety, FraudFence empowers users to make informed decisions while browsing, minimizing the risks associatedwith phishing attempts. Ultimately, the extension's primary aim is to create a safer online environment by proactively identifying and mitigating potential threats in real-time.

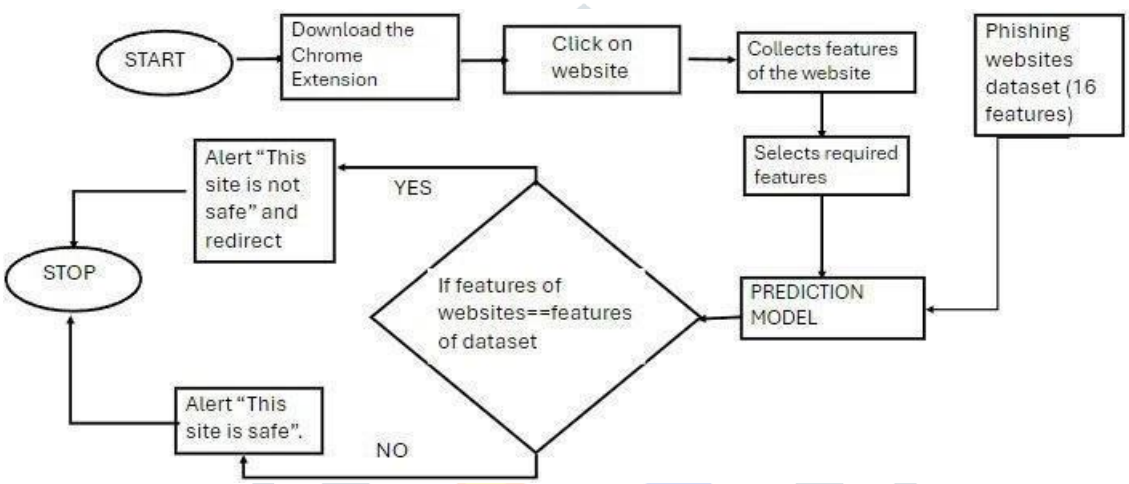


Fig. 1. Working of Proposed System

IV. SYSTEM SETUP

SOFTWARE SETUP:

- **Browser:** Browsers act as the operating environment, allowing extensions to modify, interact with, and add featuresto web pages.

- **Stable Internet Connection:** A stable internet connection is vital for effective phishing detection because itallows for real-time updates on evolving threats. It enables timely queries to external services for website verification, reducing false positives/negatives**.**

- **Operating System:** It manages hardware resources, provides a user interface, organizes files, enables device communication, ensures security, handles processes, facilitates networking, manages software, and handles errors.

- **JAVASCRIPT**: Adds interactivity to web pages, runs on browsers, enables dynamic content and animations,and is supported by all modern browsers. It's complemented by popular frameworks like React and Angular for building robust web applications.

➢ **Manifest.json :-**The manifest.json file in Chrome extensions provides essential metadata like name,version, permissions, and scripts, informing Chrome about the extension's behavior and requirements. It defines the extension's structure and capabilities, facilitating seamless integration into the browser ecosystem.

- **PYTHON 3.0:** Python is an interpreted, object-oriented, high-level programming language with dynamic semantics.Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive forRapid Application Development, as well as for use as a scripting or glue language to connect existing componentstogether.

➢ **scikit-learn (sklearn):** Sklearn is a Python library for machine learning, offering tools for classification, regression, clustering, and model evaluation. It provides efficient algorithms and user-friendly interfaces,making it a go-to choose for building and deploying machine learning models.

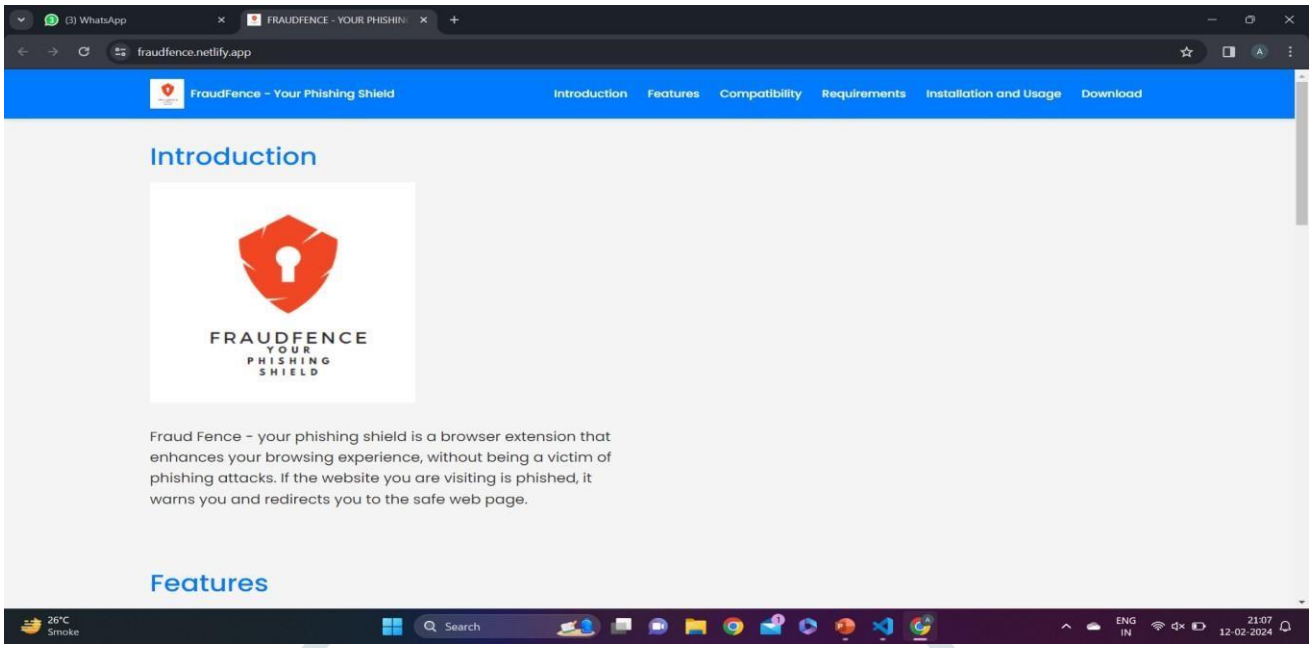
➢ **NumPy:** NumPy is a core library for numerical computing in Python, facilitating operations on large, multi-dimensional arrays and matrices. It's essential for efficient numerical computations and is widely used in scientific computing and data analysis.

➢ **Pandas:** Pandas is a versatile Python library for data manipulation and analysis, built on top of NumPy. It simplifies tasks such as data cleaning, transformation, and exploration with its powerful data structures andfunctions, making it indispensable for data science projects.

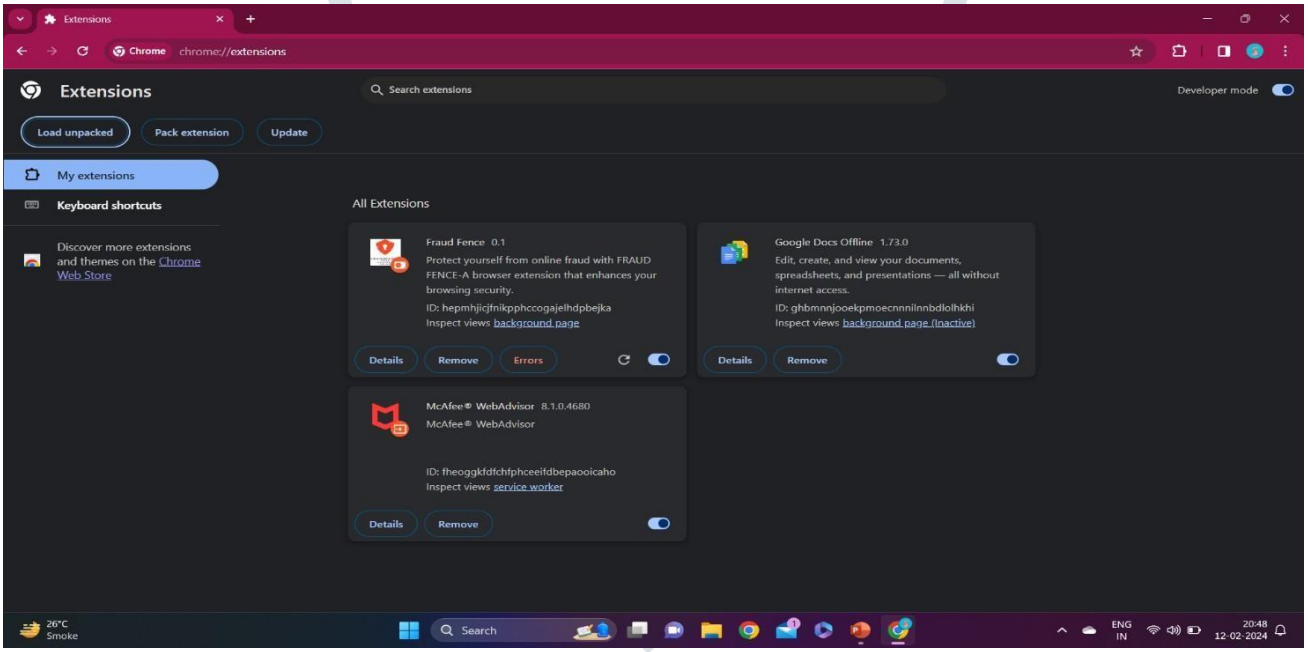
HARDWARE SETUP:

- **Processor** – Intel core i5-1335U
- **RAM** - 16 GB
- **SSD** – 512 GB
- **System** - Dell Inspiron 5430 13th gen laptop.

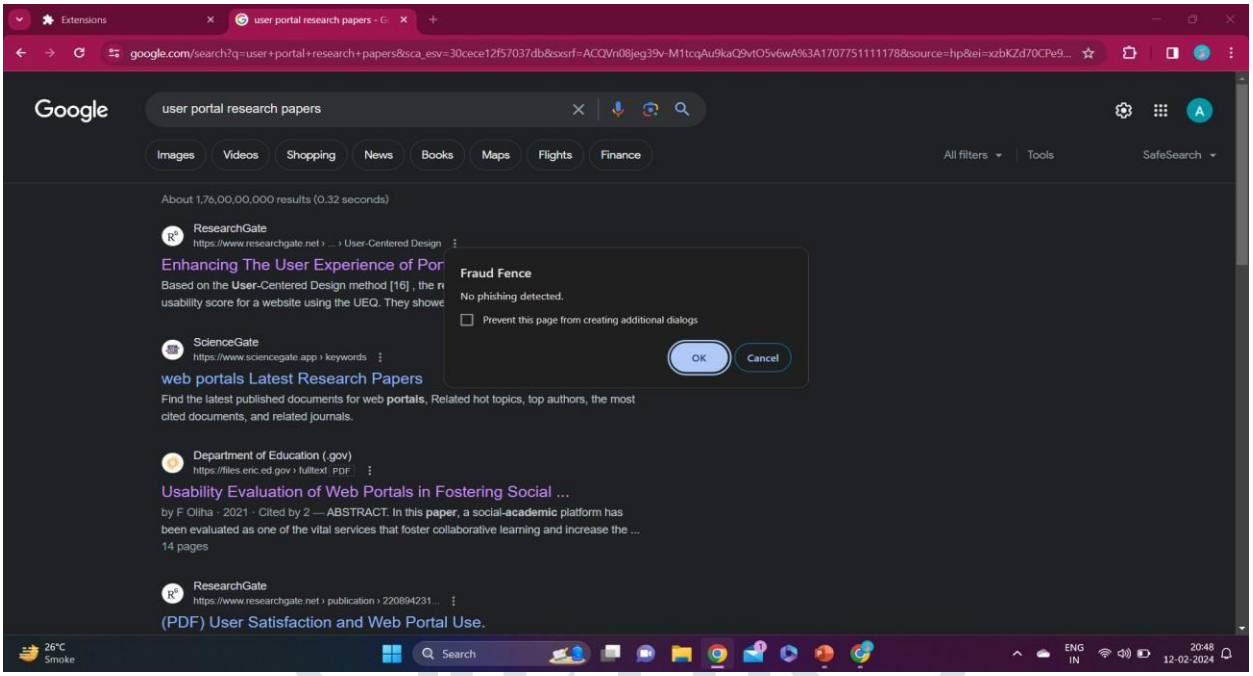
V. RESULTS



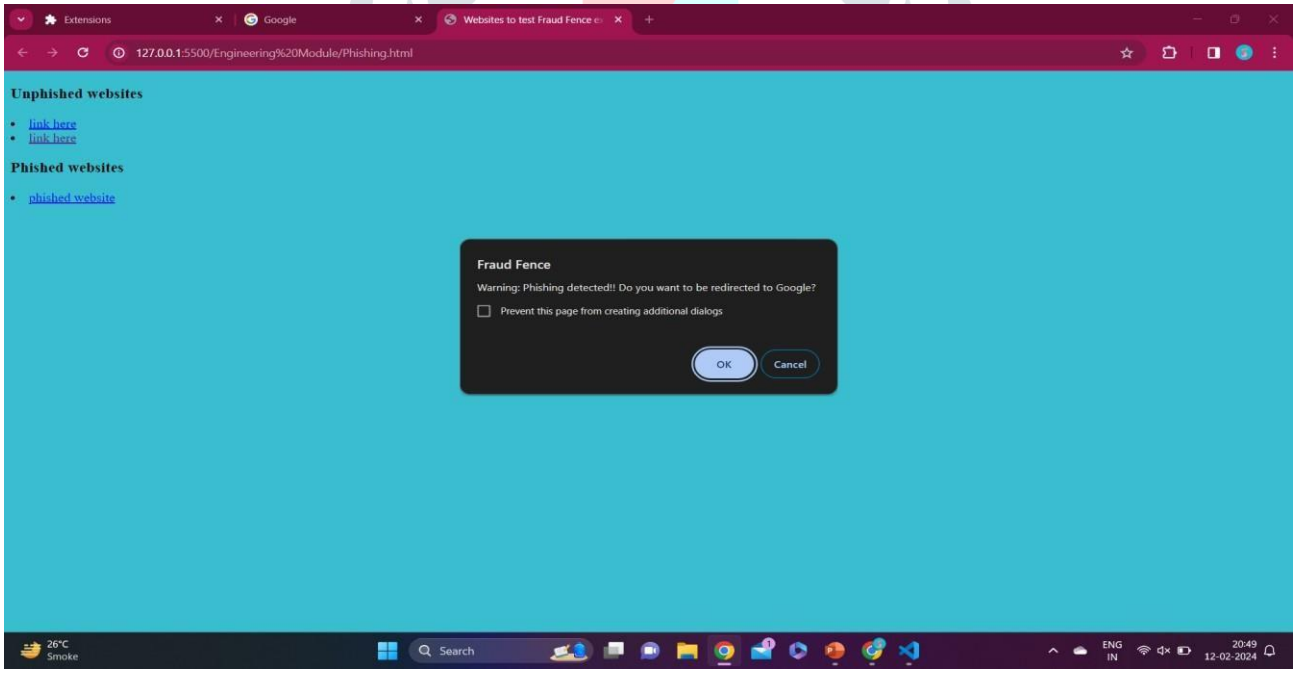
6.1 Download the zip folder from the website



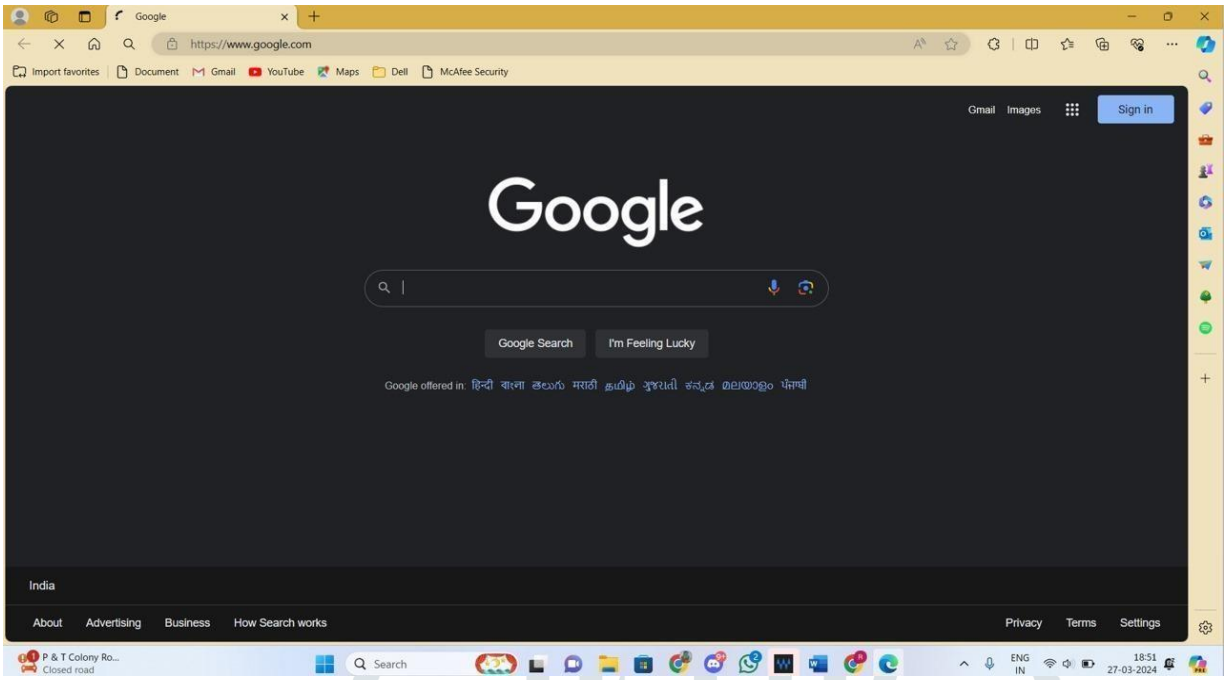
6.2 Load unpack the Extension on chrome



6.3 Phishing Not Detected



6.4 Phishing detected in website



6.5 Redirecting to safe web page.

VI. CONCLUSION

Phishing detection in Chrome extensions is a critical feature that helps protect users from fraudulent websites and cyber threats. By analyzing website URLs, content, and user interactions, these extensions aim to identify and block potential phishing attempts. However, the effectiveness of such detection depends on the extension's accuracy, timely updates, and theuser's vigilance. While Chrome's security measures and reputable extensions play a vital role in mitigating phishing risks, users should remain cautious and informed about online security best practices to maintain a robust defense against phishingattacks.

VII. ACKNOWLEDEGEMENT

We thank our project guide Prof. Reena Deshmukh along with our Head of Department Dr. Uttara Gogate and our Principal Dr. Pramod R. Rodge for providing us an opportunity of the project work in SSJCOE Dombivli and providingus all support and guidance which made us pursue the project duly. We are extremely thankful to them for providing Such nice support and guidance. We are thankful to and fortunate enough to get constant encouragement, support and guidance from all teaching staff of Computer Engineering which helped us in pursuing our project work.

REFERENCES

[1] MUZAMMIL A[illegible] B. ALTAMIMI, WILAYAT KHAN, MOHAMMAD ALSAFFAR, AAKASH AHMAD, ZAWAR HUSSAIN KHAN AND ABDULRAHMAN ALRESHIDI, "PhishCatcher: Client-Side Defense Against Web Spoofing Attacks Using MachineLearning" 19 June 2023, date of current version 22 June 2023.

[2] PAVAN. M, VENKATA SAI, MOUNIKA.B, MAHITHA. G, AMEENA BEGUM SK"Chrome Extension for Detecting Phishing Websites" Volume 12 Issue 03, Mar 2023 ISSN 2456 – 5083

[3] DINESH P.M, MUKESH M, NAVANEETHAN B, SABEENIAN R.S, PARAMASIVAMM.E, AND MANJUNATHAN "An Identification of Phishing Attacks using Machine Learning Algorithm" E3S Web of Conferences 399, 04010 (2023) https://doi.org/10.1051/e3sconf/202339904010ICONNECT-2023

[4] CHRISTOPHER N. GUTIERREZ, TAYU KIM, RAFFAELE DELLA CORTE, JEFFREY AVERY, DAN GOLDWASSER, MARCELLO CINQUE, SAURABH BAGCHI, "Learning from theOnes that Got Away: Detecting New Forms of Phishing Attacks" 1545-5971 © IEEE Journal.

[5] YAZHMOZHI. V.M, B. JANET, SRINIVASULU REDDY "Anti-phishing System 2020 IEEE International Conference for Innovation in Technology (INOCON)" Bengaluru, India. Nov 6-8, 2020

[6] FATIMA SALAHDINE, ZAKARIA EL MRABET, NAIMA KAABOUCH "Phishing Attacks Detection A Machine Learning-Based Approach" 2020

[7] AJAY P NAIR, VISHNU PRASAD A, DEVPRASAD V, "PhishDetector5" Nov 2019

[8] ARATHI KRISHNA V, ANUSREE A, BLESSY JOSE, KARTHIKA ANILKUMAR, OJUS THOMAS LEE "Phishing Detection using Machine Learning based URL Analysis" International Journalof Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org NCREIS

- 2021 Conference Proceedings

[9] https://archive.ics.uci.edu/dataset/327/phishing+websites

[10] https://scikit-learn.org/stable/modules/neural_networks_supervised.html

[11] https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html

[12] https://scikit-learn.org/stable/modules/svm.html.