PROJECT REPORT

UNIVERSITY COLLEGE OF ENGINEERING KANCHIPURAM

Team ID	**PNT2022TMID40431**
Project Name	**Web Phishing Detection**

1. INTRODUCTION

1.1 PROJECT OVERVIEW

There are number of users who purchase products online and make payment through various websites. There are multiple websites who ask user to provide sensitive data such as username, password or credit card details etc. often for malicious reasons. This type of websites is known as phishing website. In order to detect and predict phishing website, we proposed an intelligent, flexible and effective system that is based on using classification Data mining algorithm. The phishing website can be detected based on some important characteristics like URL and Domain Identity, and security and encryption criteria in the final phishing detection rate. Once user makes transaction through online when he makes payment through the website our system will use data mining algorithm to detect whether the website is phishing website or not. This application can be used by many E-commerce enterprises in order to make the whole transaction process secure. Data mining algorithm used in this system provides better performance as compared to other traditional classifications algorithms. With the help of this system user can also purchase products online without any hesitation. Admin can add phishing website URL or fake website URL into system where system could access and scan the phishing website and by using algorithm, it will add new suspicious keywords to database. System uses machine learning technique to add new keywords into database.

We have developed our project using a website as a platform for all the users. This is an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different web designing languages which include HTML, CSS, Java Script.

The basic structure of the website is made with the help of HTML. CSS is used to add effects to the website and make it more attractive and user-friendly. It must be noted that the website is created for all users, hence it must be easy to operate with and no user should face any difficulty while making its use. Every person must be able to use this website and avail maximum benefits from it.

The website shows information regarding the services provided by us. It also contains information regarding ill- practices occurring in today technological world. The website is created with an opinion such that people are not only able to distinguish between legitimate and fraudulent website, but also become aware of the mal-practices occurring in current world. They can stay away from the people trying to exploit one’s personal information, like email address, password, debit card numbers, credit card details, CVV, bank account numbers, and the list goes on.

1.2 PURPOSE

The main purpose of the project is to detect the fake or phishing websites who are trying to get access to the sensitive data or by creating the fake websites and trying to get access of the user personal credentials. We are using machine learning algorithms to safeguard the sensitive data and to detect the phishing websites who are trying to gain access on sensitive data

2. LITERATURE SURVEY

The purpose or goal behind phishing is data, money or personal information stealing through the fake website. The best strategy for avoiding the contact with the phishing web site is to detect real time malicious URL. Phishing websites can be determined on the basis of their domains. They usually are related to URL which needs to be registered (low-level domain and upper-level domain, path, query). These properties are further led to the machine-learning based classification for the identification of phishing URLs from a real dataset. For detecting a phishing website certain typical blacklisted URLs are used, but this technique is unproductive as the duration of phishing websites is very short. It can also be defined as intentionally using harsh weapons such as Spasm to automatically target the victims and targeting their private information.

2.1 EXISTING PROBLEM

2.1.1 TITLE: DETECTING PHISHING USING MACHINE LEARNING IEEE CONFERENCE PUBLICATION ,2020

AUTHOR NAME: MOHAMMED HAZIM ALKAWAZ

In the year (2020) anamoly detection solutions are readily available, are deployed quickly and immediately and automatically protect all account holders against all types of fraud attack with minimal Disruption to legitimate online banking activity. Limitation of this project is there was no facility of displaying pop-up and email notification once user had access blacklisted website

2.1.2 TITLE: DETECTION OF PHISHING WEBSITES USING AN EFFICIENT FEATURE-BASED MACHINE LEARNING FRAMEWORK

AUTHOR: NARESH KUMAR, NISHANTH KUMAR V, NEMALA SAI RAMA HEMNAH

In the year of 2018. In this, they have classified features into three categories such as URL Obfuscation features, Third-Party-based features, Hyperlink-based features. Moreover, the proposed technique gives 99.55% accuracy. Drawback of this is that as this model uses third party features, classification of websites depends on the speed of third-party services.

2.1.3 TITLE: MACHINE LEARNING BASED PHISHING DETECTION FROM URLS

AUTHOR: ONDER DEMIR, BANU DIRI, 2018

In this paper, a real-time anti-phishing system, which uses seven different classification algorithms and natural language processing (NLP) based features, is proposed. The system has the following distinguishing properties from other studies in the literature: language independence, use of a huge size of phishing and legitimate data, real-time execution, detection of new websites, independence from third-party services and use of feature-rich classifiers. For measuring the performance of the system, a new dataset is constructed, and the experimental results are tested on it. According to the experimental and comparative results from the implemented classification algorithms, Random Forest algorithm with only NLP based features gives the best performance with the 97.98% accuracy rate for detection of phishing URLs.

2.1.4 TITLE: DETECTING OF E-BANKING PHISHING WEBSITE -USING MACHINE LEARNING APPROACH

AUTHOR: PROF DURGA WANJARI, NIKAHAT SALAM QURESHI2 , DIVYA MAHESH , BHAVANA YASHVANT WAGMARE5 , SUJATA YASHWANT, 2022

There had been several strategies given within the literature to locate phishing assaults. In this segment, we gift an overview of detection approaches towards phishing attacks. In well-known, phishing detection techniques can be classified as either user education or software-based anti-phishing techniques. Software program-based totally strategies may be further categorized as listing-based totally, heuristic-based totally, and visual similarity-primarily based strategies. List-primarily based anti-phishing strategies maintain a black-list, white-list, or mixture of both. In black-list-based anti-phishing approach, a black-list is maintained which contains suspicious domains and ip addresses. Black-lists are regularly up to date; but, the maximum of the black-list-primarily based strategies are not effective in coping with zero- hour phishing assaults conclude that forty-seven % to eighty three % of phishing domain names replace inside the black-list after 12 h. A number of the processes utilizing black-lists are google safe surfing api, dns-primarily based black-lists, and predictive black-list. However, maintaining a black-list calls for a first-rate deal of sources for reporting and affirmation of the suspicious websites. As heaps of phishing webpages are created every day, updating each phishing website within the black-list is a hard venture.

2.2 REFERENCES

1. J. Shad and S. Sharma, A Novel Machine Learning Approach to Detect Phishing Websites Jaypee Institute of Information Technology, pp. 425430, 2018.

2. Y. Sainmez, T. Tuncer, H. Gatkal, and E. Avci, Phishing web sites features classification based on extreme learning machine, 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 – Proceeding, vol. 2018 Janua, pp. 15, 2018.

3. T. Peng, I. Harris, and Y. Sawa, Detecting Phishing Attacks Using Natural Language Processing and Machine Learning, Proc. – 12th IEEE Int. Conf. Semant. Comput. ICSC 2018, vol. 2018Janua, pp. 300301, 2018.

4. M. Karabatak and T. Mustafa, Performance comparison of classifiers on reduced phishing website dataset, 6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 – Proceeding, vol. 2018Janua, pp. 15, 2018.

5. S. Parekh, D. Parikh, S. Kotak, and P. S. Sankhe, A New Method for Detection of Phishing Websites: URL Detection, in 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, vol. 0, no. Icicct, pp. 949952.

6. K. Shima et al., Classification of URL bitstreams using bag of bytes, in 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2018, vol. 91, pp. 15.

7. W. Fadheel, M. Abusharkh, and I. Abdel-Qader, On Feature Selection for the Prediction of Phishing Websites, 2017 IEEE 15th Intl Conf Dependable,

Auton. Secur. Comput. 15th Intl Conf Pervasive Intell. Comput. 3rd Intl Conf Big Data Intell. Comput. Cyber Sci. Technol. Congr., pp. 871876, 2017.

8. X. Zhang, Y. Zeng, X. Jin, Z. Yan, and G. Geng, Boosting the Phishing Detection Performance by Semantic Analysis, 2017.

9. L. MacHado and J. Gadge, Phishing Sites Detection Based on C4.5 Decision Tree Algorithm, in 2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017, 2018, pp. 15.

10. A. Desai, J. Jatakia, R. Naik, and N. Raul, Malicious web content detection using machine leaning, RTEICT 2017 – 2nd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol. Proc., vol. 2018Janua, pp. 14321436, 2018.

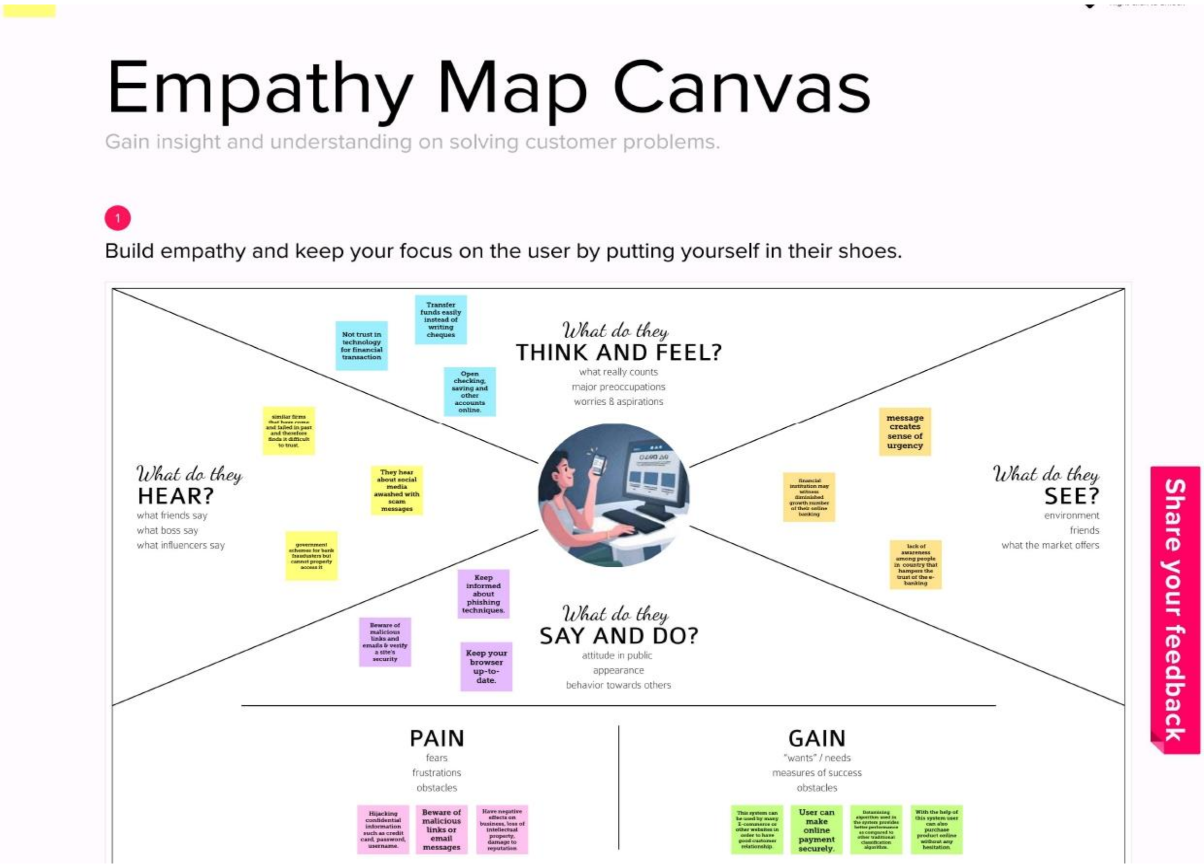
2.3 : PROBLEM STATEMENT DEFINITION

Phishing is one of the techniques which are used by the intruders to get access to the user credentials or to gain access to the sensitive data. This type of accessing the is done by creating the replica of the websites which looks same as the original websites which we use on our daily basis but when a user click on the link he will see the website and think its original and try to provide his credentials .

To overcome this problem we are using some of the machine learning algorithms in which it will help us to identify the phishing websites based on the features present in the algorithm. By using these algorithms we can be able to keep the user personal credentials or the sensitive data safe from the intruders

3.IDEATION & PROPOSED SOLUTION

3.1 EMPATHY MAP CANVAS



Empathy Map Canvas

Gain insight and understanding on solving customer problems.

1

Build empathy and keep your focus on the user by putting yourself in their shoes.

What do they THINK AND FEEL?

what really counts

major preoccupations

worries & aspirations

Not trust in technology for financial transaction

Transfer funds easily instead of writing cheques

Open checking, saving and other accounts online.

What do they HEAR?

what friends say

what boss say

what influencers say

similar firms that have come and failed in past and therefore finds it difficult to trust.

They hear about social media awashed with scam messages

government schemes for bank fraudsters but cannot properly access it

What do they SEE?

environment

friends

what the market offers

message creates sense of urgency

financial institution may witness diminished growth number of their online banking

lack of awareness among people in country that hampers the trust of the e-banking

What do they SAY AND DO?

attitude in public

appearance

behavior towards others

Keep informed about phishing techniques.

Beware of malicious links and emails & verify a site's security

Keep your browser up-to-date.

PAIN

fears

frustrations

obstacles

Hijacking confidential information such as credit card, password, username.

Beware of malicious links or email messages

Have negative effects on business, loss of intellectual property, damage to reputation

GAIN

"wants" / needs

measures of success

obstacles

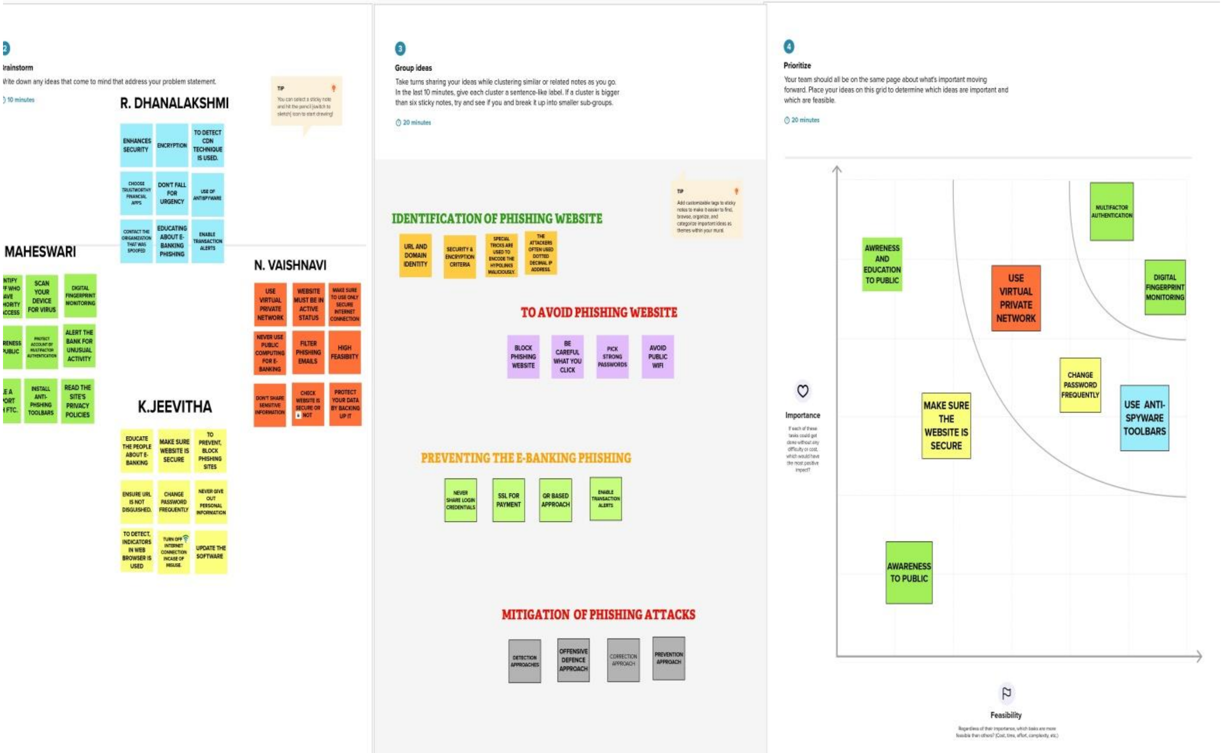
This system can be used by many E-commerce or other websites in order to have good customer relationship.

User can make online payment securely.

Ensembling algorithm used in the system provides better performance as compared to other traditional classification algorithm.

With the help of this system user can also purchase product online without any hesitation.

3.2 IDEATION & BRAINSTORMING:



rainstorm

rite down any ideas that come to mind that address your problem statement.

10 minutes

TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. In the last 10 minutes, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you and break it up into smaller sub-groups.

20 minutes

TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.

Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

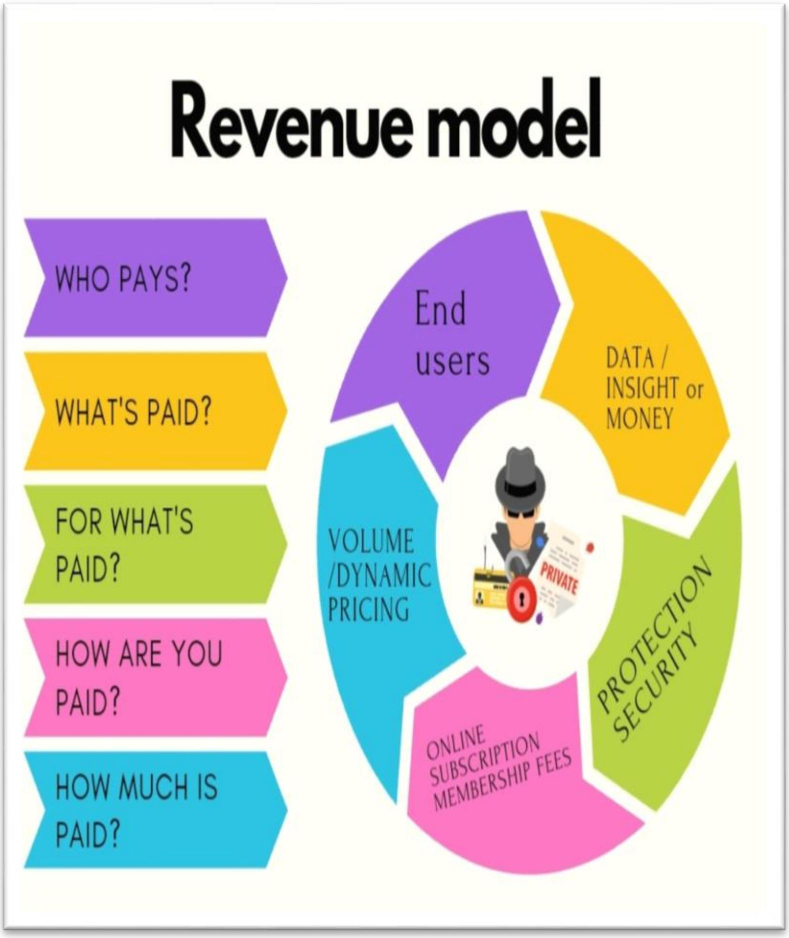
20 minutes

2
3
4
R. DHANALAKSHMI
ENHANCES SECURITY
ENCRYPTION
TO DETECT CDN TECHNIQUE IS USED.
CHOOSE TRUSTWORTHY FINANCIAL APPS
DON'T FALL FOR URGENCY
USE OF ANTISPYWARE
CONTACT THE ORGANIZATION THAT WAS SPOOFED
EDUCATING ABOUT E-BANKING PHISHING
ENABLE TRANSACTION ALERTS
MAHESWARI
NTIFY F WHO AVE HORITY CCESS
SCAN YOUR DEVICE FOR VIRUS
DIGITAL FINGERPRINT MONITORING
RENESS UBLIC
PROTECT ACCOUNT BY MULTIFACTOR AUTHENTICATION
ALERT THE BANK FOR UNUSUAL ACTIVITY
E A ORT FTC.
INSTALL ANTI-PHISHING TOOLBARS
READ THE SITE'S PRIVACY POLICIES
N. VAISHNAVI
USE VIRTUAL PRIVATE NETWORK
WEBSITE MUST BE IN ACTIVE STATUS
MAKE SURE TO USE ONLY SECURE INTERNET CONNECTION
NEVER USE PUBLIC COMPUTING FOR E-BANKING
FILTER PHISHING EMAILS
HIGH FEASIBITY
DON'T SHARE SENSITIVE INFORMATION
CHECK WEBSITE IS SECURE OR NOT
PROTECT YOUR DATA BY BACKING UP IT
K.JEEVITHA
EDUCATE THE PEOPLE ABOUT E-BANKING
MAKE SURE WEBSITE IS SECURE
TO PREVENT, BLOCK PHISHING SITES
ENSURE URL IS NOT DISGUISHED.
CHANGE PASSWORD FREQUENTLY
NEVER GIVE OUT PERSONAL INFORMATION
TO DETECT, INDICATORS IN WEB BROWSER IS USED
TURN OFF INTERNET CONNECTION INCASE OF MISUSE.
UPDATE THE SOFTWARE
IDENTIFICATION OF PHISHING WEBSITE
URL AND DOMAIN IDENTITY
SECURITY & ENCRYPTION CRITERIA
SPECIAL TRICKS ARE USED TO ENCODE THE HYPOLINKS MALICIOUSLY.
THE ATTACKERS OFTEN USED DOTTED DECIMAL IP ADDRESS.
TO AVOID PHISHING WEBSITE
BLOCK PHISHING WEBSITE
BE CAREFUL WHAT YOU CLICK
PICK STRONG PASSWORDS
AVOID PUBLIC WIFI
PREVENTING THE E-BANKING PHISHING
NEVER SHARE LOGIN CREDENTIALS
SSL FOR PAYMENT
QR BASED APPROACH
ENABLE TRANSACTION ALERTS
MITIGATION OF PHISHING ATTACKS
DETECTION APPROACHES
OFFENSIVE DEFENCE APPROACH
CORRECTION APPROACH
PREVENTION APPROACH
MULTIFACTOR AUTHENTICATION
AWRENESS AND EDUCATION TO PUBLIC
USE VIRTUAL PRIVATE NETWORK
DIGITAL FINGERPRINT MONITORING
CHANGE PASSWORD FREQUENTLY
MAKE SURE THE WEBSITE IS SECURE
USE ANTI-SPYWARE TOOLBARS
AWARENESS TO PUBLIC
Importance
If each of these tasks could get done without any difficulty or cost, which would have the most positive impact?
Feasibility
Regardless of their importance, which tasks are more feasible than others? (Cost, time, effort, complexity, etc.)

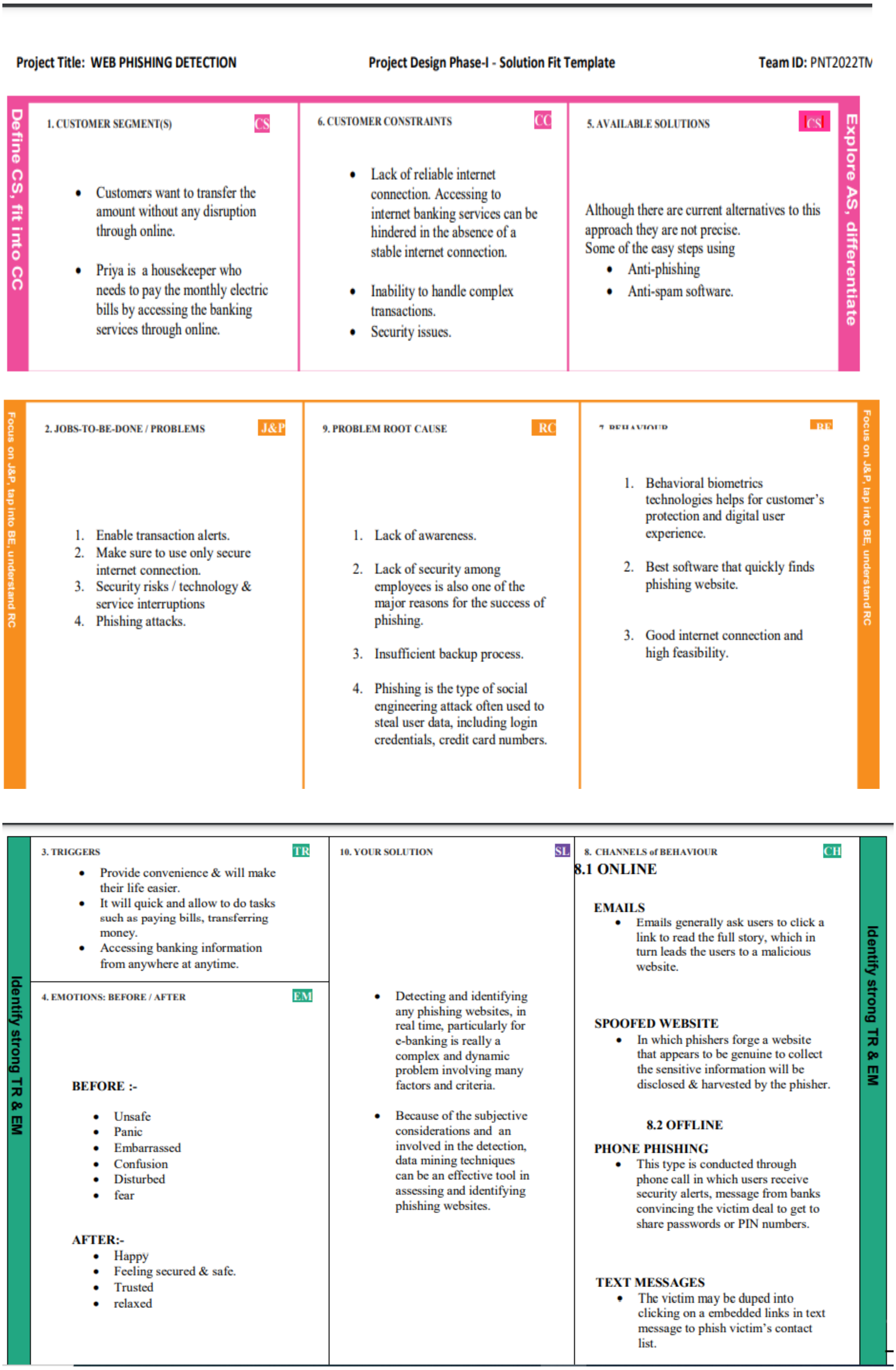
3.3 PROPOSED SOLUTION

S. No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Phishing has become one of the biggest and most effective cyber threats causing hundreds of Million of dollars in losses and millions of data breaches every years .Attackers fool the users by presenting the marked webpage as legitimate or trustworthy to retrieve their essential data such as username, password and credit card details etc., often for malicious reasons.

2.	Idea / Solution description	In order to detect and predict phishing website, we proposed an intelligent, flexible and effective system that is based on using classification, data mining algorithm. We implemented classification algorithm and techniques to extract the phishing data sets criteria to analyse their legitimacy. The solution should be useful in preventing online frauds leading to leakage of important and private user data. The mechanisms deals in order to ensure high security.
3.	Novelty / Uniqueness	We have evaluated the performance of our proposed phishing detection approach on various classification algorithm. Our system will use a datamining technique approach whether e-banking website is a phishing website or not. The system detect the phishing website and alert the user beforehand by giving signals as to prohibit the users from getting their misused credentials.
4.	Social Impact / Customer Satisfaction	Data collection to demonstrate the scalability of phishing attacks system choosing OTT attack channel. From our proposed solution, with the development of the internet, customer get statisfied by the significant security benefits and keeping both users and device safe. And proactively protect against phishing which reduce time-consuming security management.
5.	Business Model (Revenue Model)	To avoid phishing in e-banking, it can be used in the authorised e-banking apps, so it avoid money loss to the common peoples and very helpful to the business man who will be in some confused state to use online banking.

		 Revenue model WHO PAYS? WHAT'S PAID? FOR WHAT'S PAID? HOW ARE YOU PAID? HOW MUCH IS PAID? End users DATA / INSIGHT or MONEY PROTECTION SECURITY ONLINE SUBSCRIPTION MEMBERSHIP FEES VOLUME /DYNAMIC PRICING PRIVATE
6.	Scalability of the Solution	The system analyses all e-banking websites and check against past phishing patterns to detect and classify e-banking sites as genuine or phishing. This technology has maximum accuracy.

3.4 PROBLEM SOLUTION FIT



Project Title: WEB PHISHING DETECTION **Project Design Phase-I - Solution Fit Template** **Team ID:** PNT2022TM

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

- Customers want to transfer the amount without any disruption through online.
- Priya is a housekeeper who needs to pay the monthly electric bills by accessing the banking services through online.

6. CUSTOMER CONSTRAINTS CC

- Lack of reliable internet connection. Accessing to internet banking services can be hindered in the absence of a stable internet connection.
- Inability to handle complex transactions.
- Security issues.

5. AVAILABLE SOLUTIONS CS

Although there are current alternatives to this approach they are not precise.
Some of the easy steps using

- Anti-phishing
- Anti-spam software.

Explore AS, differentiate

Focus on J&P, tap into BE, understand RC

2. JOBS-TO-BE-DONE / PROBLEMS J&P

1. Enable transaction alerts.
2. Make sure to use only secure internet connection.
3. Security risks / technology & service interruptions
4. Phishing attacks.

9. PROBLEM ROOT CAUSE RC

1. Lack of awareness.
2. Lack of security among employees is also one of the major reasons for the success of phishing.
3. Insufficient backup process.
4. Phishing is the type of social engineering attack often used to steal user data, including login credentials, credit card numbers.

7. BEHAVIOUR BE

1. Behavioral biometrics technologies helps for customer's protection and digital user experience.
2. Best software that quickly finds phishing website.
3. Good internet connection and high feasibility.

Focus on J&P, tap into BE, understand RC

Identify strong TR & EM

3. TRIGGERS TR

- Provide convenience & will make their life easier.
- It will quick and allow to do tasks such as paying bills, transferring money.
- Accessing banking information from anywhere at anytime.

4. EMOTIONS: BEFORE / AFTER EM

BEFORE :-

- Unsafe
- Panic
- Embarrassed
- Confusion
- Disturbed
- fear

AFTER:-

- Happy
- Feeling secured & safe.
- Trusted
- relaxed

10. YOUR SOLUTION SL

- Detecting and identifying any phishing websites, in real time, particularly for e-banking is really a complex and dynamic problem involving many factors and criteria.
- Because of the subjective considerations and an involved in the detection, data mining techniques can be an effective tool in assessing and identifying phishing websites.

8. CHANNELS of BEHAVIOUR CH

8.1 ONLINE

EMAILS

- Emails generally ask users to click a link to read the full story, which in turn leads the users to a malicious website.

SPOOFED WEBSITE

- In which phishers forge a website that appears to be genuine to collect the sensitive information will be disclosed & harvested by the phisher.

8.2 OFFLINE

PHONE PHISHING

- This type is conducted through phone call in which users receive security alerts, message from banks convincing the victim deal to get to share passwords or PIN numbers.

TEXT MESSAGES

- The victim may be duped into clicking on a embedded links in text message to phish victim's contact list.

Identify strong TR & EM

4.REQUIREMENT ANALYSIS

4.1 FUNCTIONAL REQUIREMENT

Following are the functional requirements of the proposed solution.

FR. NO	FUNCTIONAL REQUIREMENT (EPIC)	SUB REQUIREMENT (STORY/SUB TASK)
FR-1	USER REGISTRATION	➢ Registration through online form. ➢ Registration through Gmail.\ ➢ Registration through linked in.
FR-2	USER CONFIRMATION	➢ Confirmation via email. ➢ Confirmation via OTP
FR-3	INPUT VERIFICATION	➢ Verifying URL(uniform resource locator) and pay close attention to the web address and display if the website is malicious Or not.
FR-4	WEBSITE EVALUATION	➢ Extracting efficient features from the URL and html of the given webpages without relying on Third party services.
FR-5	ALERT MESSAGE	➢ Providing the warning message to the customer by alerting from being Victim.

4.2 NON-FUNCTIONAL REQUIREMENTS:

Following are the non-functional requirements of the proposed solution.

FR NO.	NON-FUNCTIONAL REQUIREMENT	DESCRIPTION
NRF-1	USABILITY	➢ Detect active or emerging phishing. ➢ Available as a cloud service; no software to install. ➢ Third party independent. ➢ URL filtering
NRF-2	SECURITY	➢ Provide multi-vector phishing protection. ➢ Data loss prevention. ➢ User can make online payment securely and Trustworthy.
NRF-3	REALIABILITY	➢ This machine learning technology is completely signature-less and automatically adapts to ever-changing fake and phishing sites. ➢ It does not rely on signatures and blocklists like anti-

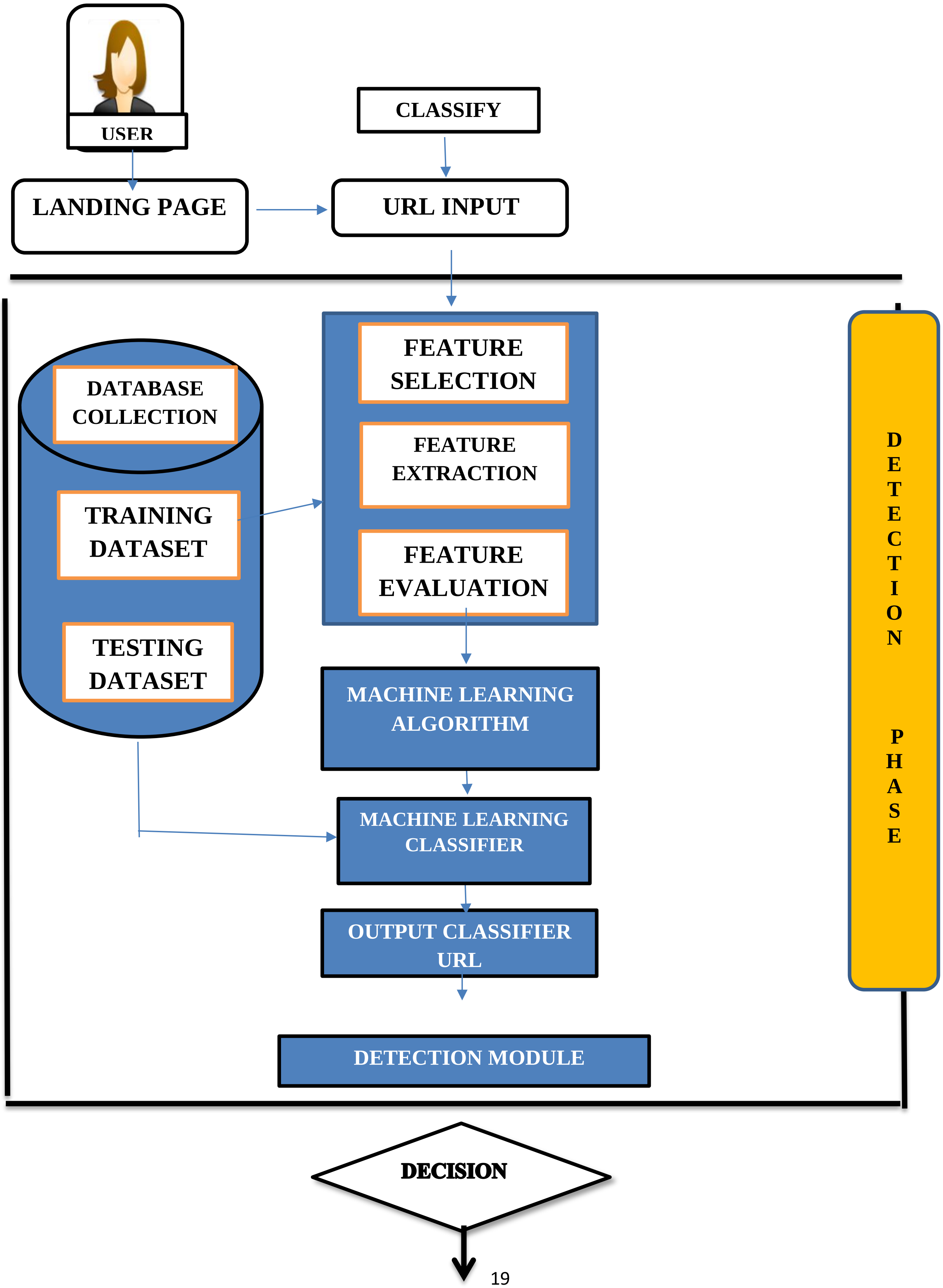
		phishing tools. ➢ Real world phishing campaign Simulations.
NRF-4	PERFORMANCE	➢ High performance. ➢ Advanced threat analysis. Data mining algorithm used in this system provides better
NRF-5	AVAILABILITY	➢ User-friendly and transparent. ➢ this system can be used by many e-commerce or other websites in order to have good customer Relationship.
NFR-6	SCALABILITY	➢ Increase user alertness to phishing risks. ➢ Eliminate the cyber threat risk level. ➢ Measures the degree of corporate and employee vulnerability.

5. PROJECT DESIGN

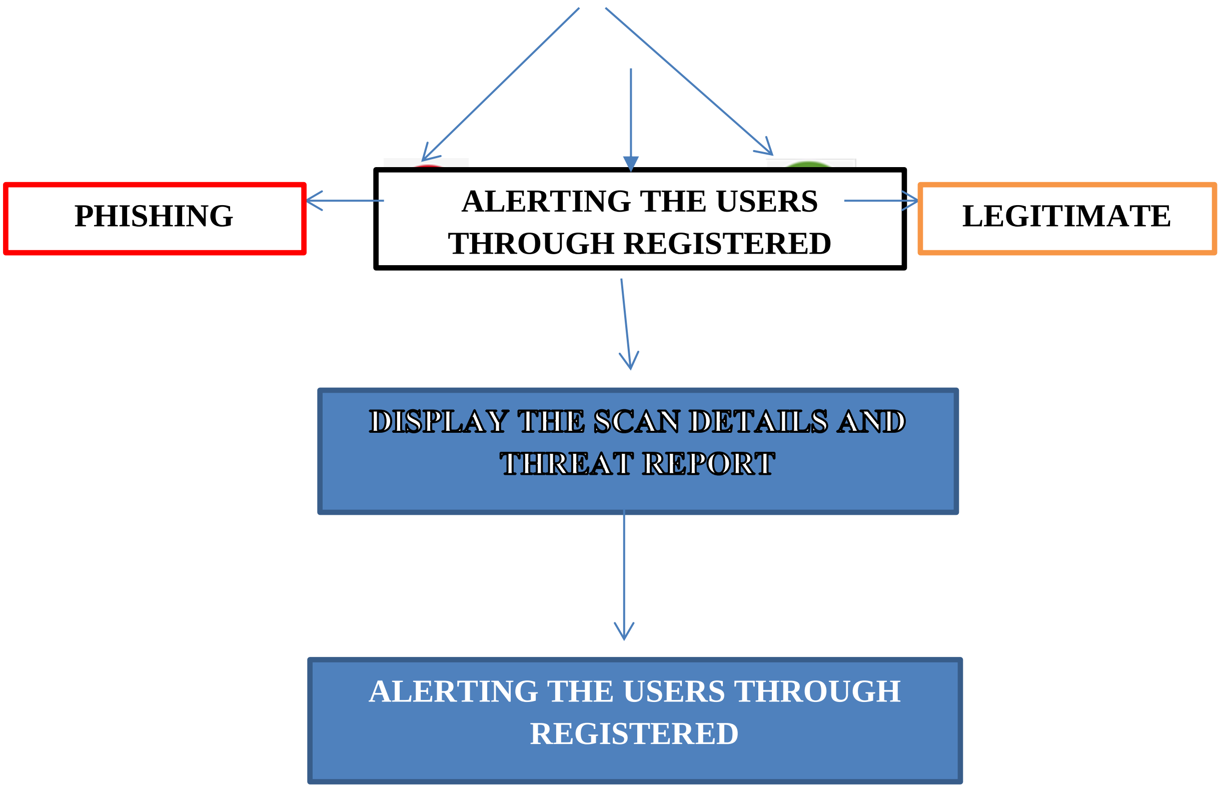
5.1 DATA FLOW DIAGRAMS

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.

A Two-dimensional diagrams shows how the data is processed and transferred in a system. The graphical representation identifies each source of data and how it interacts with the other data sources to reach a common output determine how the input and output is processed.

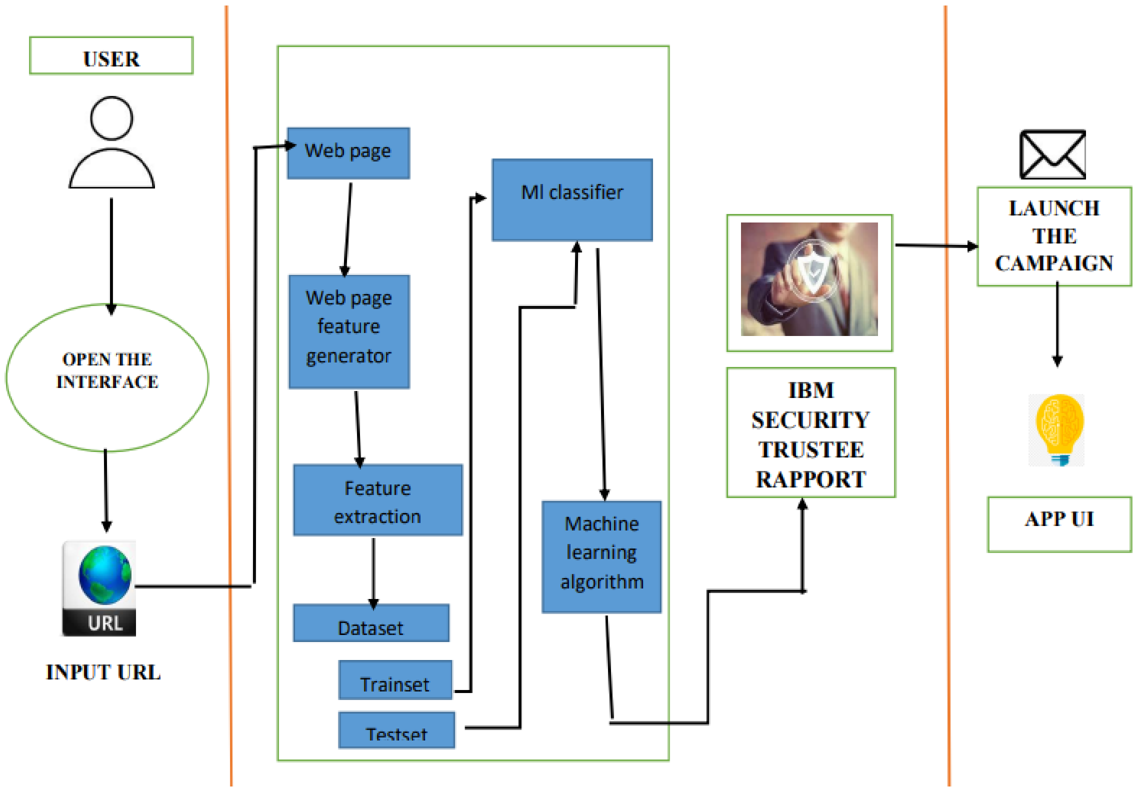


USER
CLASSIFY
LANDING PAGE
URL INPUT
DATABASE COLLECTION
TRAINING DATASET
TESTING DATASET
FEATURE SELECTION
FEATURE EXTRACTION
FEATURE EVALUATION
MACHINE LEARNING ALGORITHM
MACHINE LEARNING CLASSIFIER
OUTPUT CLASSIFIER URL
DETECTION MODULE
DETECTION PHASE
DECISION


PHISHING
ALERTING THE USERS THROUGH REGISTERED
LEGITIMATE
DISPLAY THE SCAN DETAILS AND THREAT REPORT
ALERTING THE USERS THROUGH REGISTERED

5.2 SOLUTION & TECHNICAL ARCHITECTURE

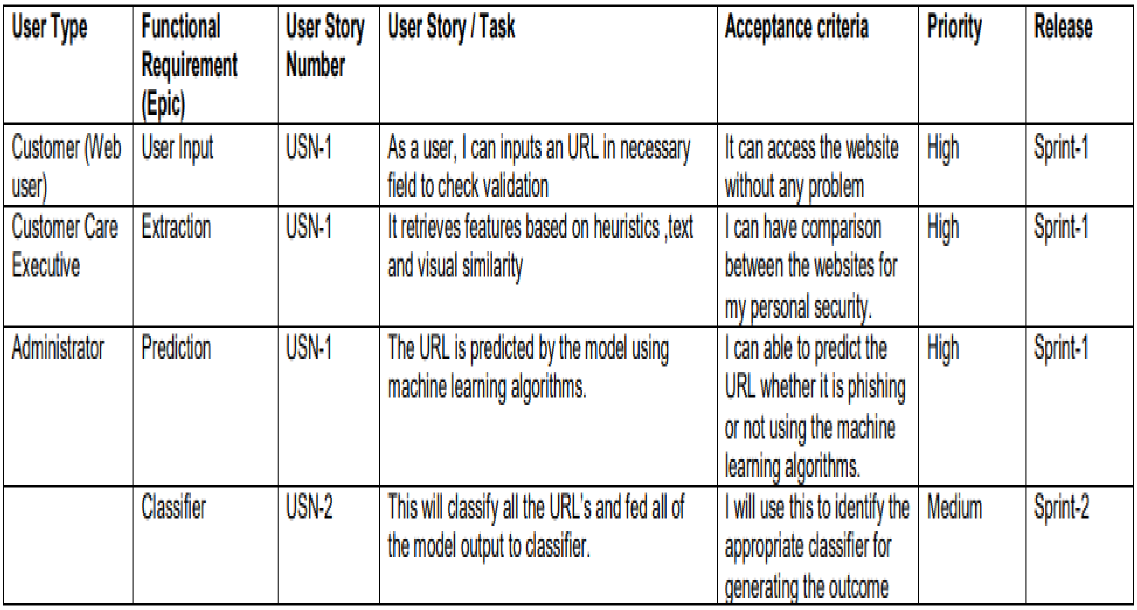
A system architecture is the conceptual model that defines the structure, behaviour and more views of a system. An architecture description is a formal description and representation of a system, organised in a way supports reasoning about the structures and behaviours of the system. System architecture can comprise system components, the externally visible properties of the component and relationship between them.



5.3 USER STORIES

Use the below template to list all the user stories for the product.

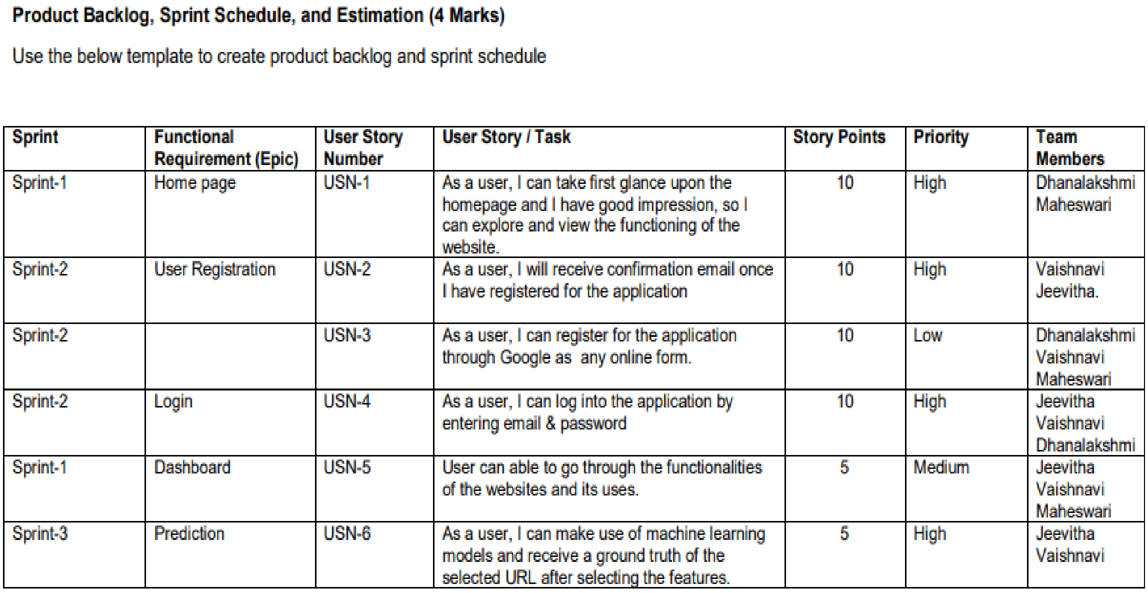
User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Mobile user)	User Registration	USN-1	Registration through online form. Registration through Gmail and password. Registration through linked in.	I can access my account / dashboard	High	Sprint-1
		USN-2	As a user, I will receive confirmation or verification code through OTP or email once I have registered for the application	I can receive confirmation email or OTP & click confirm	High	Sprint-1
		USN-3	As a user, Sometimes I can register for the application through SMS, Facebook	I can register & access the dashboard with Facebook Login	Low	Sprint-2
	Login	USN-5	As a user, I can log into the application by entering email & password	I can enter the details and login to the application	High	Sprint-1



User Type	Functional Requirement (Epic)	User Story Number	User Story / Task	Acceptance criteria	Priority	Release
Customer (Web user)	User Input	USN-1	As a user, I can inputs an URL in necessary field to check validation	It can access the website without any problem	High	Sprint-1
Customer Care Executive	Extraction	USN-1	It retrieves features based on heuristics ,text and visual similarity	I can have comparison between the websites for my personal security.	High	Sprint-1
Administrator	Prediction	USN-1	The URL is predicted by the model using machine learning algorithms.	I can able to predict the URL whether it is phishing or not using the machine learning algorithms.	High	Sprint-1
	Classifier	USN-2	This will classify all the URL's and fed all of the model output to classifier.	I will use this to identify the appropriate classifier for generating the outcome	Medium	Sprint-2

6.PROJECT PLANNING & SCHEDULING

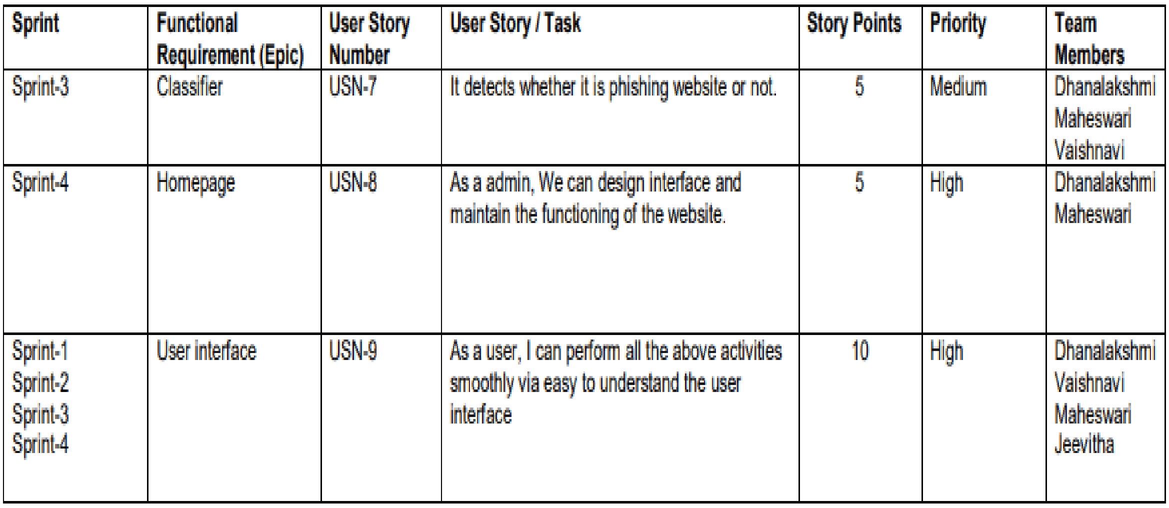
6.1 SPRINT PLANNING & ESTIMATION



Product Backlog, Sprint Schedule, and Estimation (4 Marks)

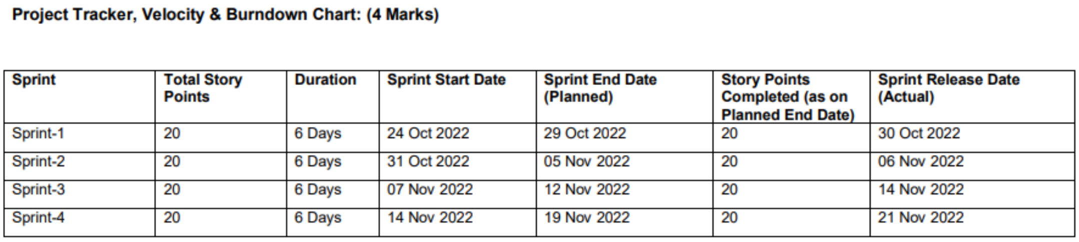
Use the below template to create product backlog and sprint schedule

Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-1	Home page	USN-1	As a user, I can take first glance upon the homepage and I have good impression, so I can explore and view the functioning of the website.	10	High	Dhanalakshmi Maheswari
Sprint-2	User Registration	USN-2	As a user, I will receive confirmation email once I have registered for the application	10	High	Vaishnavi Jeevitha.
Sprint-2		USN-3	As a user, I can register for the application through Google as any online form.	10	Low	Dhanalakshmi Vaishnavi Maheswari
Sprint-2	Login	USN-4	As a user, I can log into the application by entering email & password	10	High	Jeevitha Vaishnavi Dhanalakshmi
Sprint-1	Dashboard	USN-5	User can able to go through the functionalities of the websites and its uses.	5	Medium	Jeevitha Vaishnavi Maheswari
Sprint-3	Prediction	USN-6	As a user, I can make use of machine learning models and receive a ground truth of the selected URL after selecting the features.	5	High	Jeevitha Vaishnavi



Sprint	Functional Requirement (Epic)	User Story Number	User Story / Task	Story Points	Priority	Team Members
Sprint-3	Classifier	USN-7	It detects whether it is phishing website or not.	5	Medium	Dhanalakshmi Maheswari Vaishnavi
Sprint-4	Homepage	USN-8	As a admin, We can design interface and maintain the functioning of the website.	5	High	Dhanalakshmi Maheswari
Sprint-1 Sprint-2 Sprint-3 Sprint-4	User interface	USN-9	As a user, I can perform all the above activities smoothly via easy to understand the user interface	10	High	Dhanalakshmi Vaishnavi Maheswari Jeevitha

6.2SPRINT DELIVERY SCHEDULE

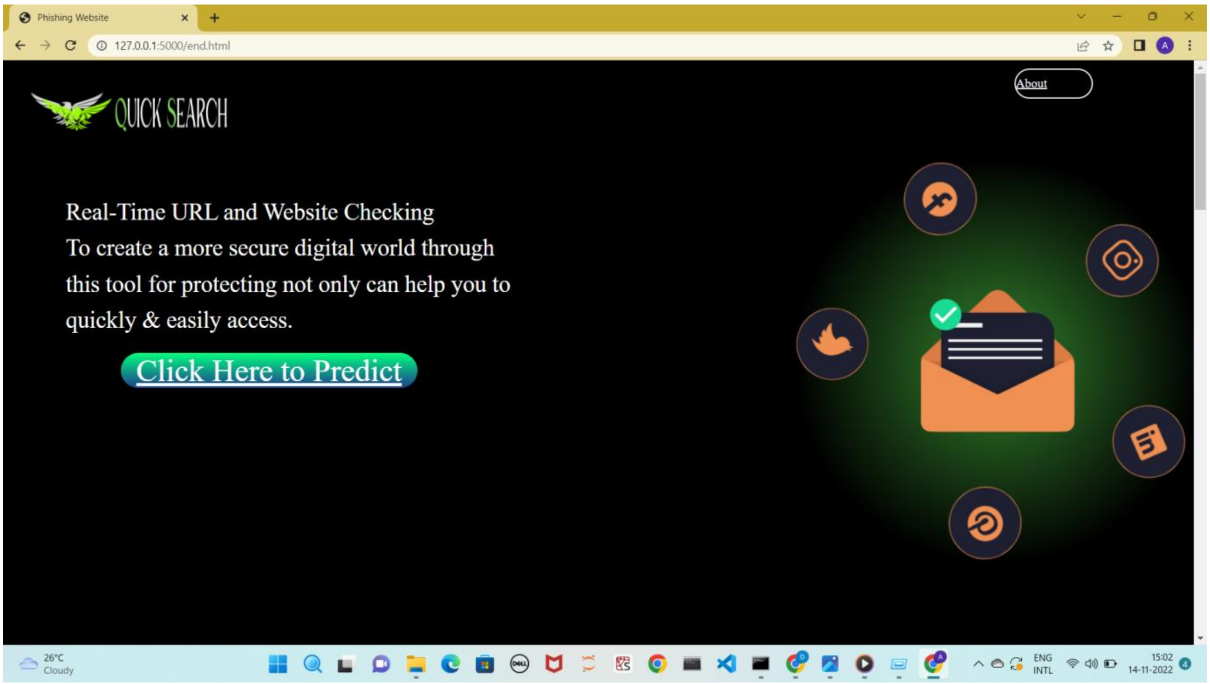


Project Tracker, Velocity & Burndown Chart: (4 Marks)

Sprint	Total Story Points	Duration	Sprint Start Date	Sprint End Date (Planned)	Story Points Completed (as on Planned End Date)	Sprint Release Date (Actual)
Sprint-1	20	6 Days	24 Oct 2022	29 Oct 2022	20	30 Oct 2022
Sprint-2	20	6 Days	31 Oct 2022	05 Nov 2022	20	06 Nov 2022
Sprint-3	20	6 Days	07 Nov 2022	12 Nov 2022	20	14 Nov 2022
Sprint-4	20	6 Days	14 Nov 2022	19 Nov 2022	20	21 Nov 2022

7. CODING & SOLUTIONING

7.1 FEATURE 1



Real-Time URL and Website Checking
To create a more secure digital world through this tool for protecting not only can help you to quickly & easily access.

Code

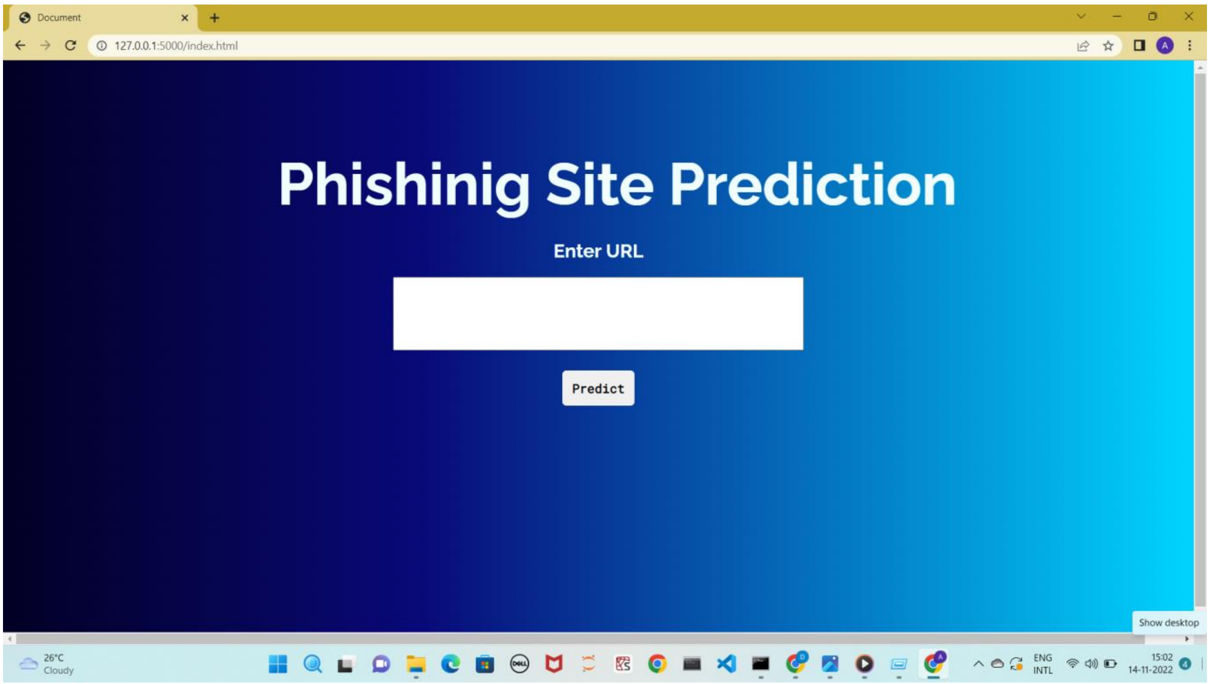
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet"  type="text/css" href="../static/end.css">
            <title>Phishing Website</title>
</head>
<body>
```

```
    <div class="wrapper">
        <header>
            <div class="container">
                <img src="../static/images/menu.png" class="menu">
                <img src="../static/images/qc.png" class="quick">
                <a href="#section1" class="about-btn">About</a>
            </div>
            </header>

    <div class="content">
        <div class="text">
            <p>Real-Time URL and Website Checking<br>
                To create a more secure digital world through this tool for protecting not only can help you to quickly & easily access.</p>
                <div class="input-group-append">
                <a href="/index.html" class="input-group-text btn">Click Here to Predict</a>
                </div>
            </div>
        </div>
        <div class="img">
            <div class="social-icons">
                <img src="../static/images/social-icon1.png" alt="">
                <img src="../static/images/social-icon2.png" alt="">
                <img src="../static/images/social-icon3.png" alt="">
                <img src="../static/images/social-icon4.png" alt="">
                <img src="../static/images/social-icon5.png" alt="">
            </div>
            <img class="email-icon" src="../static/images/email-icon.png" alt="">
        </div>
    </div>

<div class="wave">
    <img src="../static/images/wave.svg" alt="">
</div>
</div>
<section class="features">
    <div class="container" id="section1">
        <h1>INFO</h1>
        <div class="row">
            <div class="col-md-4">
                <div class="feature-box">
                    <div class="feature-img">
                        <img src="../static/images/a.gif">
                        <img src="../static/images/7zon.gif">
            <div class="detail">
              <p>Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate.</p>
            </div>
            </div>
          </div>
        </div>
      </div>
      <div class="row">
            <div class="col-md-4">
                  <div class="info">
                    <p>A measurement for phishing detection is the number of suspicious e-mails reported to the security team. This measurement is designed to evaluate the number of employees who followed the proper procedure for reporting suspicious messages.</p>
                  </div>
                </div>
              </div>
            </div>
      </div>
    </div>
  </div>
```

```
    </section>

    <hr>

    <section class="FAQ">

        <div class="create">

        <h2>FAQ & Answers</h2>


        <div class="v1">

            <h4>Do you know what is phishing?</h4>

            <p>This is the type of virtual threat has become increasingly
common.Its aims to obtain this information through bait.</p>

            </div>

            <br>

        <div class="v2">

        <h4>What is QuickCheck?</h4>

        <p>QuickCheck uses advanced machine learning techniques to quickly
detect scam websites and determine whether a website is legit or not.</p>

        </div>

        <br>

        <div class="v3">

        <h4>What are the benefits of using QuickCheck?</h4>

        <p>Often, you want to visit a website for various reasons, but you are
unsure whether to trust the website.<br>
```

```
            You are asking yourself questions such as “is this website legit?” or “is
it a scam website?” or “is this a safe website?” or “is this site real?” and so
many similar questions.<br>

            QuickCheck is an intelligent scam detector which analyses website link
characteristics and allows finding out proactively and swiftly whether by
clicking on the link you will land on an unsafe website or a website that is
safe. It helps with website credibility check and verifying whether a company
is legit.</p>

        </div>

        <br>

        <div class="v4">

        <h4>How to use QuickCheck??</h4>

        <p>Using QuickCheck for fraudulent websites check or to check whether
a website is safe is very easy.<br>

            Just enter the link in the search box and click the Search icon.<br>

             QuickCheck will check the website link a0nd quickly displays its
results as whether this is a scam website or a safe website.</p>

        </div>

        <br>

        <div class="v5">

        <h4>How QuickCheck works?</h4>

        <p>URL Checker is a safe link checker which uses advanced machine
learning algorithms and natural language processing techniques to analyze
website link characteristics and check the credibility of the users owning
it.</p>

        </div>
        <br>
        <div class="v6">
        <h4>Features</h4>
        <p>1. Advanced threat protection.<br>
          2. Thread intelligence.<br>
          3. Advanced threat analysis.<br>
          4. Threat mitigation.<br>
          5. Data loss protection.<br>
        </p>


        </div>
        </section>



</body>
</html>
```

7.2 FEATURE 2



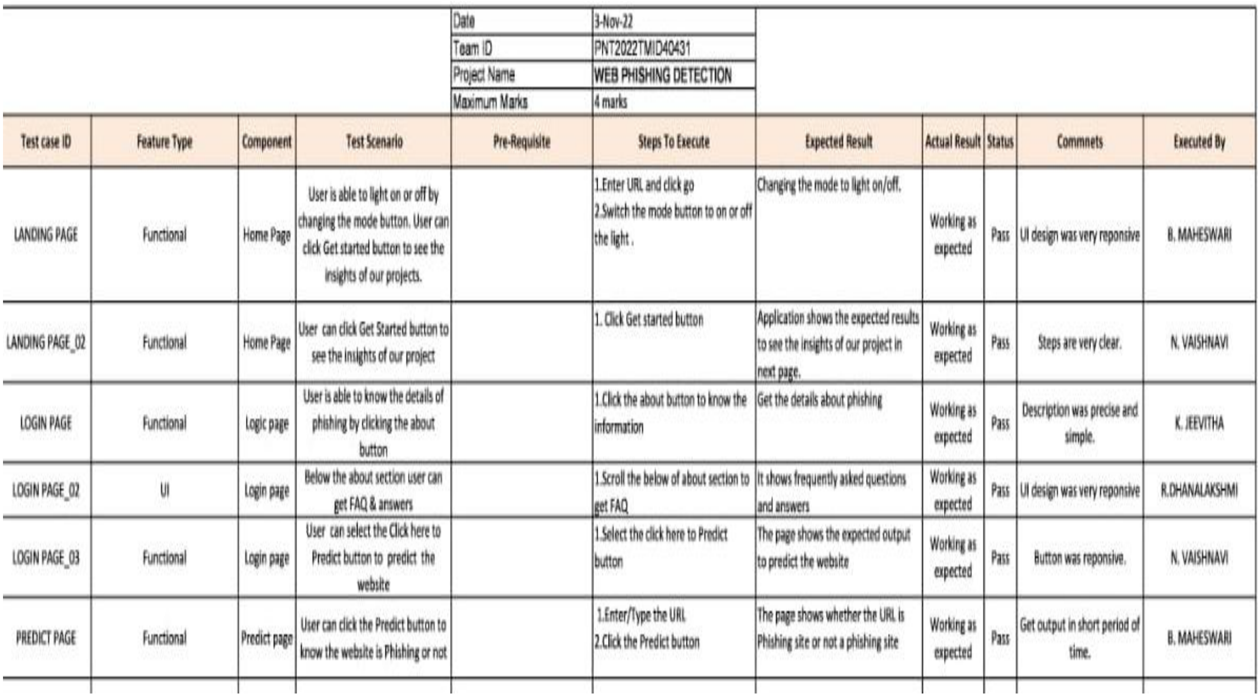
```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
  <link rel="stylesheet"  href="../static/style.css">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link
href="https://fonts.googleapis.com/css2?family=Raleway:wght@100&family=
Roboto+Mono&display=swap"
    rel="stylesheet">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link
href="https://fonts.googleapis.com/css2?family=Raleway:wght@100;700&fa
mily=Roboto+Mono&display=swap"
    rel="stylesheet">
  <link rel="preconnect" href="https://fonts.gstatic.com">


</head>


<body>
<br><br><br><br>
  <div class="welcome ">
    <h2 style="color: azure;">Phishinig Site Prediction</h2>
  </div>
  <div class="userinput">
    <h2>Enter URL </h2>
<br>
    <form action='/predict' method="post">
      <div class="input">
```

```
        <input id="url" name="z1" type="text" width="48" height="48"
size="50" required><br>

        <button class="button" type="Summarize">Predict</button>

      </div>

    </form>

    <br>

    <br>

    <div id='result'>

      {{ prediction_text }}

    </div>

  </div>

</body>

</html>
```

8. TESTING

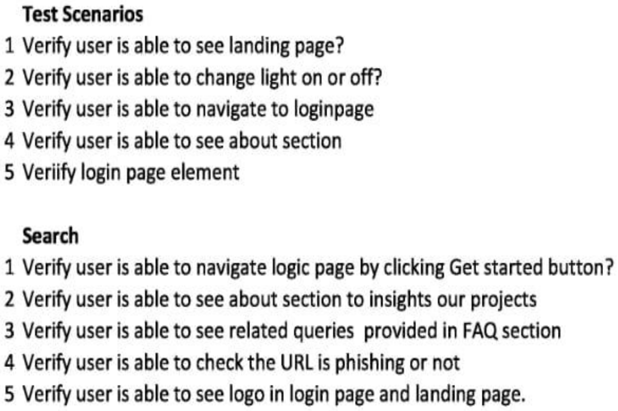
8.1 TEST CASES

A test case has components that describe input, actionand an expected response, in order to determine if a feature of an application is working correctly. A set case is a set of instructions on “HOW” to validate a particular test objective/target, which when followed will tell us if the expected behaviour of the system is satisfied or not.



Date	3-Nov-22
Team ID	PNT2022TMID40431
Project Name	WEB PHISHING DETECTION
Maximum Marks	4 marks

Test case ID	Feature Type	Component	Test Scenario	Pre-Requisite	Steps To Execute	Expected Result	Actual Result	Status	Commnets	Executed By
LANDING PAGE	Functional	Home Page	User is able to light on or off by changing the mode button. User can click Get started button to see the insights of our projects.		1.Enter URL and click go 2.Switch the mode button to on or off the light .	Changing the mode to light on/off.	Working as expected	Pass	UI design was very reponsive	B. MAHESWARI
LANDING PAGE_02	Functional	Home Page	User can click Get Started button to see the insights of our project		1. Click Get started button	Application shows the expected results to see the insights of our project in next page.	Working as expected	Pass	Steps are very clear.	N. VAISHNAVI
LOGIN PAGE	Functional	Logic page	User is able to know the details of phishing by clicking the about button		1.Click the about button to know the information	Get the details about phishing	Working as expected	Pass	Description was precise and simple.	K. JEEVITHA
LOGIN PAGE_02	UI	Login page	Below the about section user can get FAQ & answers		1.Scroll the below of about section to get FAQ	It shows frequently asked questions and answers	Working as expected	Pass	UI design was very reponsive	R.DHANALAKSHMI
LOGIN PAGE_03	Functional	Login page	User can select the Click here to Predict button to predict the website		1.Select the click here to Predict button	The page shows the expected output to predict the website	Working as expected	Pass	Button was reponsive.	N. VAISHNAVI
PREDICT PAGE	Functional	Predict page	User can click the Predict button to know the website is Phishing or not		1.Enter/Type the URL 2.Click the Predict button	The page shows whether the URL is Phishing site or not a phishing site	Working as expected	Pass	Get output in short period of time.	B. MAHESWARI



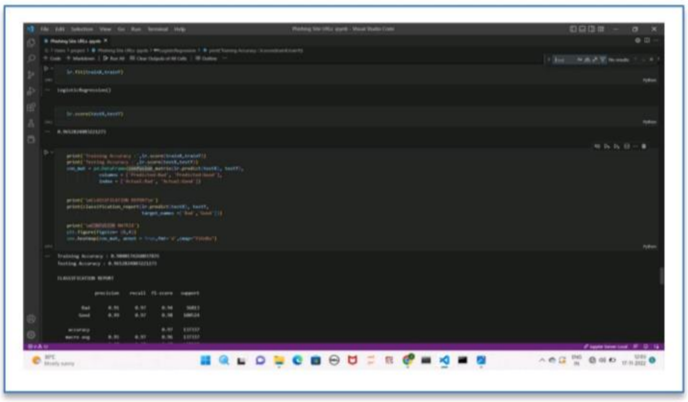
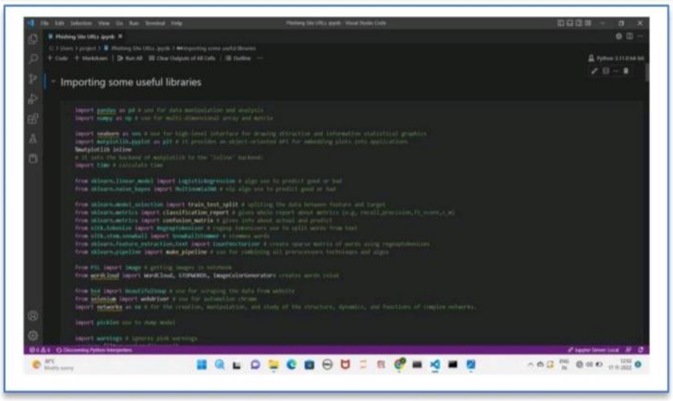
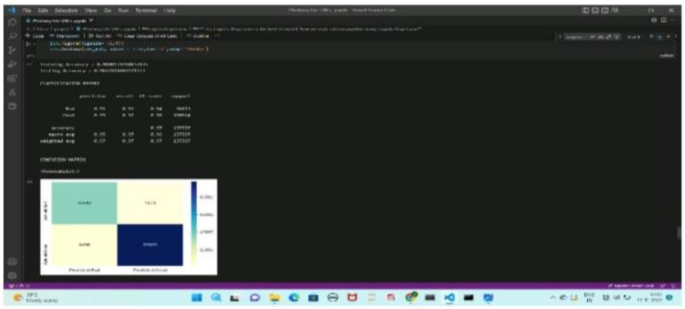
Test Scenarios

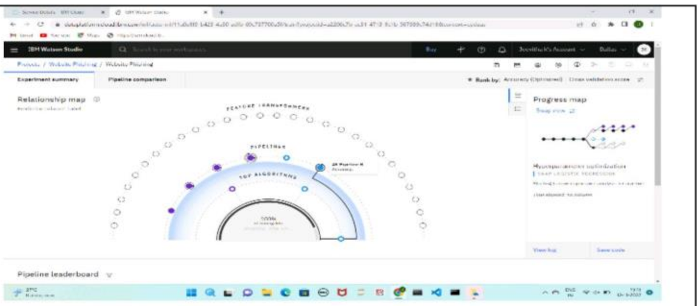
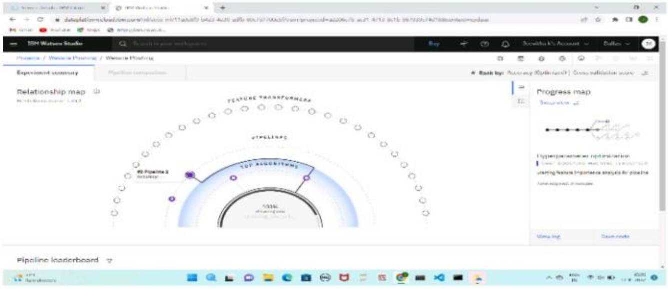
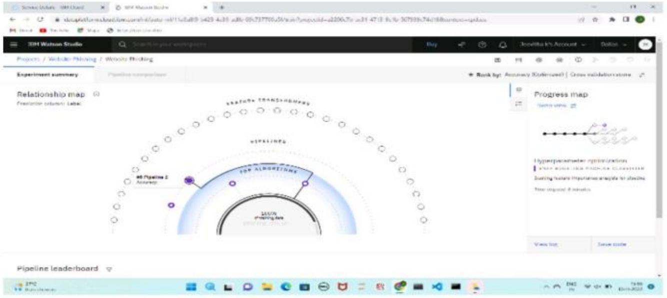
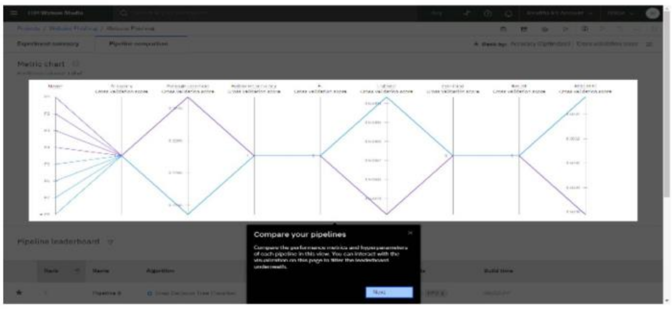
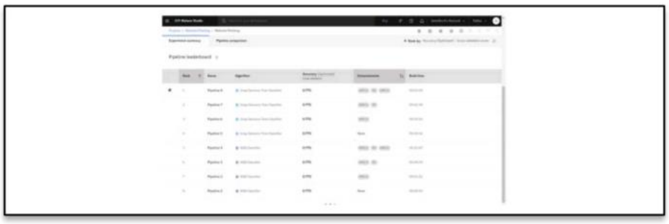
1 Verify user is able to see landing page?
2 Verify user is able to change light on or off?
3 Verify user is able to navigate to loginpage
4 Verify user is able to see about section
5 Veriify login page element

Search

1 Verify user is able to navigate logic page by clicking Get started button?
2 Verify user is able to see about section to insights our projects
3 Verify user is able to see related queries provided in FAQ section
4 Verify user is able to check the URL is phishing or not
5 Verify user is able to see logo in login page and landing page.

8.2 USER ACCEPTANCE TESTING

S. No.	Parameter	Values	Screenshot
1.	Metrics	**Regression Model:** MAE - , MSE - , RMSE - , R2 score - **Classification Model:** Confusion Matrix – Accuray Score- & Classification Report -	  Importing some useful libraries 

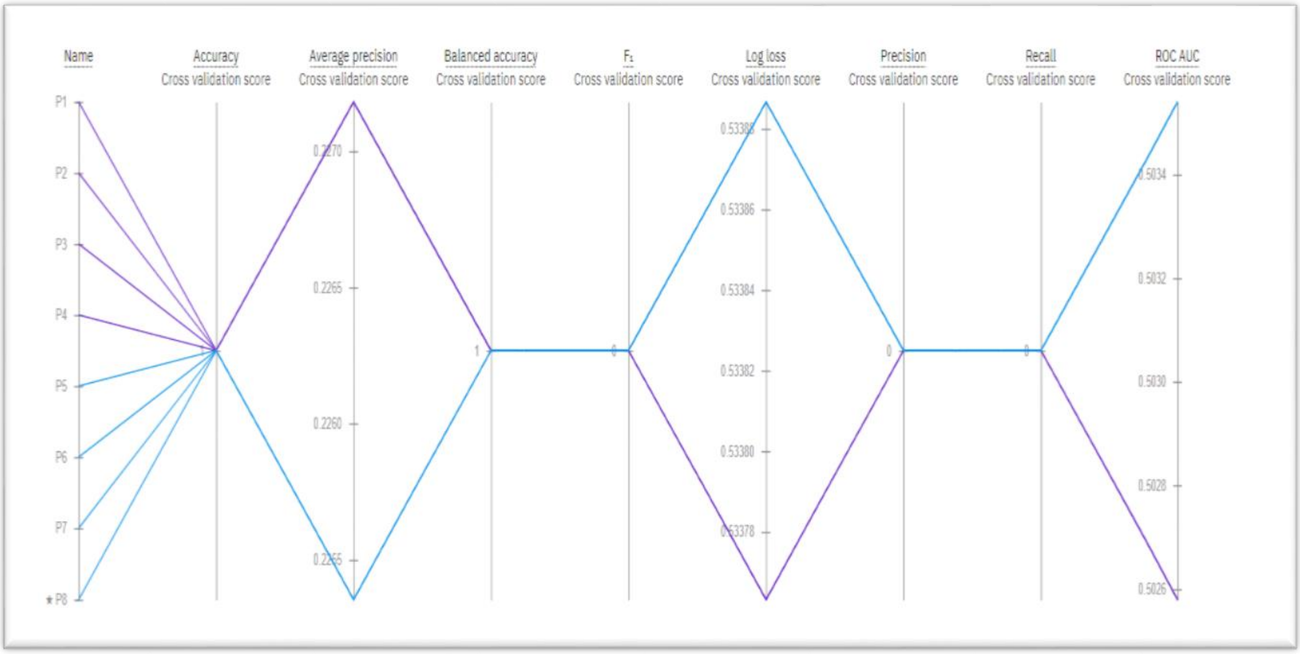
2.	**<u>Tune the Model</u>**	**HYPER PARAMETER TUNING –** **Validation Method -**	    

Compare your pipelines

Compare the performance metrics and hyperparameters of each pipeline in this view. You can interact with the visualization on this page to filter the leaderboard underneath.

9. RESULTS

9.1 PERFORMANCE METRICS



11. ADVANTAGES & DISADVANTAGES

ADVANTAGES

- This system can be used by many E-commerce or other websites in order to have good customer relationship.
- User can make online payment securely.
- Data mining algorithm used in this system provides better performance as compared to other traditional classifications algorithms.
- With the help of this system user can also purchase products online without any hesitation.

DISADVANTAGES

- If Internet connection fails, this system won’t work.

12. CONCLUSION

It is found that phishing attacks is very crucial and it is important for us to get a mechanism to detect it. As very important and personal information of the user can be leaked through phishing websites, it becomes more critical to take care of this issue. This problem can be easily solved by using any of the machine learning algorithm with the classifier.

We already have classifiers which gives good prediction rate of the phishing beside, further improve the accuracy prediction rate of phishing websites. We have seen that existing system gives less accuracy so we proposed a new phishing method that employs URL based features and also we generated classifiers through several machine learning. We have got the desired results of testing the site is phishing or not by using four different classifiers.

12. FUTURE SCOPE

In future if we get structured dataset of phishing we can perform phishing detection much more faster than any other technique. In future we can use a combination of any other two or more classifier to get maximum accuracy. We also plan to explore various phishing techniques that uses Lexical features, Network based features, Content based features, In particular, we extract features from URLs and pass it through the various classifiers. And we can try to find the website through offline mann

13. APPENDIX

SOURCE CODE

Start.html

```
<!DOCTYPE html>
<html>
    <head>
        <title> PHISHING DETECTION WEBSITE-QUICKCHECK</title>
        <link rel="stylesheet" href="../static/start.css">
    </head>
    <body>
        <div class="hero"
            <nav>
                <img src="../static/images/menu.png" class="menu-png" id="bird">
                <img src="../static/images/Black, White and Triangle Data Chase
Games Logo.png" class="logo-png" >


                <ul>
<li><a href="">HOME</a></li>
<li><a href="">MODE</a></li>
</ul>
<buttontype="button"onclick="toggleBtn()" id="btn"><span></span></button>
            </nav>
            <div class="lamp-container">
                <img src="../staticimages/lamp.png" class="lamp">
                <img src="../static/images/light.png" class="light" id="light">
            </div>
            <div class="hacker">
                <img src="../static/images/hack.jpg" class="hack" id="hack">
            </div>
              </nav>

        <div class="text-container">
            <h1> Real time URL & Website Sandbox</h1><br><br>
            <p> Free URL scanner and Website checker to detect phishing, scam sites & fradulent sites.<br>
                <br>QUICKCHECK is a free tool to detect malicious URLs including malware, scams and phishing links.<br>
                <br>Safe links checker scans URLs for malware, viruses,scam and phishing links
            </p>
            <a href="/end.html" class="get-started-btn scrollto">Get Started</a>

            <div class="control">
                <p>04</p>
                <div class="line"><span></span></div>
                <p>05</p>
            </div>
        </div>

        <script>
            var btn=document.getElementById("btn");
            var light=document.getElementById("light");
```

```
            function toggleBtn(){
             btn.classList.toggle("active");
             light.classList.toggle("on");

            }
        </script>
        <script src=".../static/main.js"></script>

    </body>
    </html>
    </body>

</html>
```

Start.css

```
*{
    margin: 0;
    padding: 0;
    font-family:'poppins',sans-serif;
    box-sizing: border-box;
}
.hero{
background:black;
min-height: 100vh;
width: 100%;
```

```
color: #fff;
position: relative;
}
nav{
    display: flex;
    align-items: center;
    padding: 20px 8%;
}
nav .menu-png{
    width: 200px;
    margin-right: 55px;
    position: absolute;
    height: 100px;
    left: 20px;



}
nav .logo-png{
    width: 200px;
    margin-left: 93px;



}
nav ul{
    flex: 1;
    text-align: right;
```

```
}
nav ul li{
    display: inline-block;
    list-style: none;
    margin: 0 20px;
}
nav ul li a{
    text-decoration: none;
    color: #fff;
    background: none;
}
button{
    cursor: pointer;
    transition: background 0.5s;
    background:red;
    height: 30px;
    width: 60px;
    border-radius: 20px;
    border: 0;
    outline: 0;
}
button span{
    display: block;
    background: #999;
    height: 26px;
    width: 26px;
    border-radius: 50%;
    margin-left: 2px;
    transition: background 0.5s,margin-left 0.5s;

}
.lamp-container{
    position: absolute;
    top: -20px;
    left: 22%;
    width: 200px;
}
.hack{
    width: 300px;
    height: 300px;
    position: absolute;
    left: 272px;
    border-radius: 50%;
    z-index: 0;
    bottom: 50px;



}


.lamp{
    width: 100%;
}
```

```
.light{
    position: absolute;
    top: 97%;
    left: 50%;
    transform: translateX(-50%);
    width: 700px;
    margin-left: -10px;
    opacity: 0;
    transition: opacity 0.5s;
}



.text-container{
    max-width: 600px;
    margin-top: 7%;
    margin-left: 50%;
    color:#fff;
}
.text-container h1{
    font-size: 50px;
    font-weight: 400;
    color:rgba(38, 177, 23, 0.927);
    color:transparent;
    -webkit-text-stroke: 3px rgba(38, 177, 23, 0.927);
    animation: back 10s linear infinite;
    background-position: 0 0;
    background: url(images/back.png);

}
@keyframes back {
    100%{
        background-position: 1000px 0;
    }

}
.text-container p{
    font-style: Palatino;
}
.text-container a{
    text-decoration: none;
    background-color: rgba(42, 214, 59, 0.856);
    padding: 14px 40px;
    display: inline-block;
    color: #fff;
    font-size: 18px;
    margin-top: 30px;
    border-radius: 30px;
}.control{
    display: flex;
    align-items:center;
    justify-content: flex-end;
    margin-top: 150px;
```

```
}
.control .line{
    width: 250px;
    height: 4px;
    background: #fff;
    margin: 0 20px;
    border-radius: 2px;

}
.control .line span{
    width: 50%;
    height: 8px;
    margin-top: -2px;
    border-radius: 4px;
    background: rgba(38, 177, 23, 0.927);
    display: block;
}
.active {
    background: rgba(38, 177, 23, 0.927);
}
.active span{
    background: #fff;
    margin-left: 31px;
}
.on{
    opacity: 3;
```

}

end.html

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <link rel="stylesheet"  type="text/css" href="../static/end.css">
         <title>Phishing Website</title>
</head>
<body>
   <div class="wrapper">
      <header>
         <div class="container">
            <img src="../static/images/menu.png" class="menu">
            <img src="../static/images/qc.png" class="quick">
            <a href="#section1" class="about-btn">About</a>
         </div>
         </header>

   <div class="content">
      <div class="text">
         <p>Real-Time URL and Website Checking<br>
            To create a more secure digital world through this tool for protecting
not only can help you to quickly & easily access.</p>
            <div class="input-group-append">
```

```
        <a href="/index.html" class="input-group-text btn">Click Here to Predict</a>
        </div>
      </div>
    </div>
    <div class="img">
      <div class="social-icons">
        <img src="../static/images/social-icon1.png" alt="">
        <img src="../static/images/social-icon2.png" alt="">
        <img src="../static/images/social-icon3.png" alt="">
        <img src="../static/images/social-icon4.png" alt="">
        <img src="../static/images/social-icon5.png" alt="">
      </div>
      <img class="email-icon" src="../static/images/email-icon.png" alt="">
    </div>
  </div>

<div class="wave">
  <img src="../static/images/wave.svg" alt="">
</div>
</div>
<section class="features">
  <div class="container" id="section1">
    <h1>INFO</h1>
    <div class="row">
      <div class="col-md-4">
        <div class="feature-box">
```

```
          <div class="feature-img">
            <img src="../static/images/a.gif">
            <img src="../static/images/7zon.gif">
            <div class="detail">
              <p>Phishing is an attack that attempts to steal your money, or
your identity, by getting you to reveal personal information -- such as credit
card numbers, bank information, or passwords -- on websites that pretend to be
legitimate.</p>
            </div>
            </div>
          </div>
        </div>
      </div>
      <div class="row">
            <div class="col-md-4">
                  <div class="info">
                    <p>A measurement for phishing detection is the
number of suspicious e-mails reported to the security team. This measurement is
designed to evaluate the number of employees who followed the proper
procedure for reporting suspicious messages.</p>
                  </div>

                </div>
              </div>
            </div>
      </div>
    </div>
  </div>
  </section>
```

```
<hr>
<section class="FAQ">
    <div class="create">
    <h2>FAQ & Answers</h2>


    <div class="v1">
        <h4>Do you know what is phishing?</h4>
        <p>This is the type of virtual threat has become increasingly
common.Its aims to obtain this information through bait.</p>
        </div>
        <br>



    <div class="v2">
    <h4>What is QuickCheck?</h4>
    <p>QuickCheck uses advanced machine learning techniques to quickly
detect scam websites and determine whether a website is legit or not.</p>
    </div>
    <br>
    <div class="v3">
    <h4>What are the benefits of using QuickCheck?</h4>
    <p>Often, you want to visit a website for various reasons, but you are
unsure whether to trust the website.<br>
        You are asking yourself questions such as “is this website legit?” or “is
it a scam website?” or “is this a safe website?” or “is this site real?” and so
many similar questions.<br>
        QuickCheck is an intelligent scam detector which analyses website link
characteristics and allows finding out proactively and swiftly whether by
clicking on the link you will land on an unsafe website or a website that is safe.
```

```
It helps with website credibility check and verifying whether a company is legit.</p>

        </div>

        <br>

        <div class="v4">

        <h4>How to use QuickCheck??</h4>

        <p>Using QuickCheck for fraudulent websites check or to check whether a website is safe is very easy.<br>

            Just enter the link in the search box and click the Search icon.<br>

             QuickCheck will check the website link a0nd quickly displays its results as whether this is a scam website or a safe website.</p>

        </div>

        <br>

        <div class="v5">

        <h4>How QuickCheck works?</h4>

        <p>URL Checker is a safe link checker which uses advanced machine learning algorithms and natural language processing techniques to analyze website link characteristics and check the credibility of the users owning it.</p>

        </div>

        <br>

        <div class="v6">

        <h4>Features</h4>

        <p>1. Advanced threat protection.<br>

          2. Thread intelligence.<br>

          3. Advanced threat analysis.<br>

          4. Threat mitigation.<br>

          5. Data loss protection.<br>

        </p>
        </div>
        </section>



</body>
</html>
```

End.css

```
*{
    margin: 0;
    outline: none;
    box-sizing: border-box;
}
body{
    font-family: Space Grotesk;
    background-color: black;
    overflow-x: hidden;
}

.wrapper{
    position: relative;
    height: 100vh;
    overflow: hidden;
}
header{
    padding: 50px 100px;
    display: flex;
    align-items: center;
    justify-content: space-between;
}
.menu{
width: 150px;
height: 70px;
float: left;
left: 130px;
margin-top: -20px;
margin-left: -90px;
}
.quick{
width: 150px;
height: 70px;
margin-left: 1px;
float: left;
margin-top: -20px;
margin-left: -20px;
}

.about-btn{
width: 100px;
padding: 8px 0;
outline: none !important;
border: 2px solid #fff;
border-radius: 50px;
background: transparent;
```

```
color: #fff;
float: left;
margin-left: 1000px;
margin-top: -40px;
}

.content{
    display: flex;
    flex-wrap: wrap;
    justify-content: space-between;
    padding: 20px 100px 0;
    font-size: 60px;
    font-weight: 100;
    font-style: serif;
    margin-bottom: 200px;
}
.text{
    width: 50%;
    padding-right: 100px;
}
.text p{
  font-family:didot;
    font-size: 30px;
    font-weight: 400;
    line-height: 46px;
    color: #fff;
    margin-left: -20px;
```

```
}
.text p span{
    color: #01b3fa;
}
.input-group-text{
width: 100px;
height: 70px;
font-size: 40px;
background-image: linear-gradient(#00ff7e,#1f3d90);
border: 0 !important;
border-radius: 50px 50px 50px 50px !important;
color: #fff !important;
padding: 0 20px !important;
box-sizing: none !important;
margin-left: 50px;
margin-top: 10px;
}

.img{
    position: relative;
    width: 500px;
    height: 500px;
    background: radial-gradient(520px, #60f0538c, transparent 50%);
    margin-top: -490px;
    float: right;
}
.email-icon{
    position: absolute;
    top: 50%;
    left: 50%;
    transform: translate(-50%, -50%);
}
.social-icons{
    height: 100%;
    animation: rotation 60s linear infinite;
}
@keyframes rotation {
    100%{
        transform: rotate(360deg);
    }
}
.social-icons img{
    position: absolute;
}
.social-icons img:nth-child(1){
    top: 0;
    left: 42%;
}
.social-icons img:nth-child(2){
    top: 25%;
    right: 0;
}
.social-icons img:nth-child(3){
    top: 70%;
    left: 70%;
}
.social-icons img:nth-child(4){
    top: 25%;
    left: 0;
}
.social-icons img:nth-child(5){
    top: 70%;
    left: 10%;
}


.wave{
    position: absolute;
    bottom: 0;
    left: 0;
    width: 100%;
    line-height: 0;
}
.wave:before{
    content: '';
    position: absolute;
    bottom: 0;
    left: 0;
    width: 100%;
    height: 100%;
    background: url(images/wave.svg) repeat-x;
    background-size: cover;
    background-position: -1000px 0;
    opacity: .2;
    animation: waveOne 60s linear infinite;
}
@keyframes waveOne {
    50%{
        background-position: 0 0;
    }
}
.wave:after{
    content: '';
    position: absolute;
    bottom: 0;
    left: 0;
    width: 100%;
    height: 100%;
    background: url(images/wave.svg) repeat-x;
    background-size: cover;
    background-position: 2732px 0;
    opacity: .3;
    animation: waveOne 120s linear infinite;
}


/*SUBMENU*/
ul ul{
    max-width: 250px;
    position: absolute;
    padding: 10px 0;
    opacity: 0;
    z-index: -9999;
    transition: all ease 0.5s;
}
ul li:hover ul{
    opacity: 1;
    z-index: 9;
    padding: 30px 0;
}
ul ul li{
    margin: 0;
    width: 100%;
}
ul ul li a{
    width: 100%;
    display: inline-block;
    padding: 20px;
    background-color: #383a58;
    color: #fff;
}
ul ul li:first-child a{
    border-top-left-radius: 10px;
    border-top-right-radius: 10px;
}
```

```
ul ul li:last-child a{
    border-bottom-left-radius: 10px;
    border-bottom-right-radius: 10px;
}
ul ul li a:hover{
    background-color: #7ff053;
    color: #fff;
}
/*features*/
.features{
padding: 100px 0;
background-color:black;
height: 700px;
}
h1{
text-align: center;
padding-bottom: 30px;
}
.feature-img img{
width: 40%;
height: 250px;
border: 30%;
margin-left: 40px;
margin-right: 90px;
}
.detail{
font-style: italic;
```

```
font-size: 25px;
width: 500px;
height: 170px;
position: relative;
float: left;
border-radius: 30%;
margin-left: 40px;
margin-top: 20px;
padding-top: 40px;
padding-left: 40px;
padding-right: 10px;
padding-bottom: 20px;
background-color: #00ff7e;
animation-name: slidein;
animation-duration: 3s;
animation-iteration-count: infinite;
box-sizing: content-box;

}
@keyframes slidein {
   0%{background-color: skyblue;}
   25%{background-color: rgb(119, 0, 255);}
   50%{background-color: rgb(233, 37, 70);}
   75%{background-color: lightpink;}
   100%{background-color: orange;}
 }
.info{
```

```
font-style: italic;
font-size: 25px;
width: 500px;
height: 170px;
position: relative;
float: left;
border-radius: 30%;
margin-left: 225px;
margin-top: 20px;
padding-top: 40px;
padding-left: 45px;
padding-right: 10px;
padding-bottom: 30px;
background-color: #00ff7e;
animation-name: ani;
animation-duration: 3s;
animation-iteration-count: infinite;
box-sizing: content-box;
}
@keyframes ani{
0%{background-color: skyblue;}
25%{background-color: rgb(119, 0, 255);}
50%{background-color: rgb(233, 37, 70);}
75%{background-color: lightpink;}
100%{background-color: orange;}
}
```

```
/*FAQ*/
.create{
padding: 0;
margin: 0;
width: 1520px;
height: 1600px;
animation-name: nam;
animation-duration: 3s;
animation-iteration-count: infinite;
}
@keyframes nam{
0%{background-color: #ee0f22c0;}
25%{background-color: #f1db12ef;}
50%{background-color: limegreen;}
75%{background-color: hotpink;}
100%{background-color: aquamarine;}

}
.create h2{
font-weight: 600;
width: 1520px;
height: 70px;
text-align: center;
border-radius: 10px;
box-shadow: none;
background-color: #fff;
}
```

```
.v1 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v1 p{
font-weight: 600;
font-size: 20px;
width: 500px;
height: 150px;
background-color: #fff;
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v1slidein;
}
@keyframes v1slidein {
  from {
    margin-left: 100%;
    width: 300%;
  }

  to {
      margin-left: 0%;
      width: 100%;
    }
  }
.v2 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v2 p{
font-weight: 600;
font-size: 20px;
width: 500px;
height: 200px;
background-color: #fff;
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v2slidein;
}
@keyframes v2slidein {
    from {
      margin-left: 100%;
      width: 300%;
    }

    to {
      margin-left: 0%;
      width: 100%;
    }
  }
.v3 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v3 p{
font-weight: 600;
font-size: 20px;
width: 500px;
height: 310px;
background-color: #fff;
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v3slidein;
```

```
}
@keyframes v3slidein {
    from {
      margin-left: 100%;
      width: 300%;
    }

    to {
      margin-left: 0%;
      width: 100%;
    }
  }
.v4 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v4 p{
font-weight: 600;
font-size: 20px;
width: 500px;
height: 190px;
background-color: #fff;
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
```

```
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v4slidein;
}
@keyframes v4slidein {
    from {
      margin-left: 100%;
      width: 300%;
    }

    to {
      margin-left: 0%;
      width: 100%;
    }
  }
.v5 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v5 p{
font-weight: 600;
font-size: 20px;
width: 500px;
height: 150px;
background-color: #fff;
```

```
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v5slidein;
}
@keyframes v5slidein {
    from {
      margin-left: 100%;
      width: 300%;
    }

    to {
      margin-left: 0%;
      width: 100%;
    }
  }
.v6 h4{
font-weight: 600;
font-size: 25px;
text-align: center;
}
.v6 p{
font-weight: 600;
```

```
font-size: 20px;
width: 500px;
height: 150px;
background-color: #fff;
border-radius: 10px;
margin-top: 20px;
margin-left: 500px;
padding-left: 20px;
padding-right: 20px;
padding-top: 10px;
animation-duration: 5s;
animation-name: v6slidein;
}
@keyframes v6slidein {
   from {
     margin-left: 100%;
     width: 300%;
   }

   to {
     margin-left: 0%;
     width: 100%;
   }
  }
```

Index.html

```
<!DOCTYPE html>
<html lang="en">
```

```
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Document</title>
  <link rel="stylesheet"  href="../static/style.css">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link
href="https://fonts.googleapis.com/css2?family=Raleway:wght@100&family=Roboto+Mono&display=swap"
    rel="stylesheet">
  <link rel="preconnect" href="https://fonts.gstatic.com">
  <link
href="https://fonts.googleapis.com/css2?family=Raleway:wght@100;700&family=Roboto+Mono&display=swap"
    rel="stylesheet">
  <link rel="preconnect" href="https://fonts.gstatic.com">

</head>

<body>
<br><br><br><br>
  <div class="welcome ">
    <h2 style="color: azure;">Phishinig Site Prediction</h2>
  </div>
  <div class="userinput">
    <h2>Enter URL </h2>
<br>
    <form action='/predict' method="post">
      <div class="input">
        <input id="url" name="z1" type="text" width="48" height="48" size="50"
required><br>
        <button class="button" type="Summarize">Predict</button>
      </div>


    </form>
    <br>
    <br>
    <div id='result'>
      {{ prediction_text }}
    </div>


  </div>


</body>


</html>
```

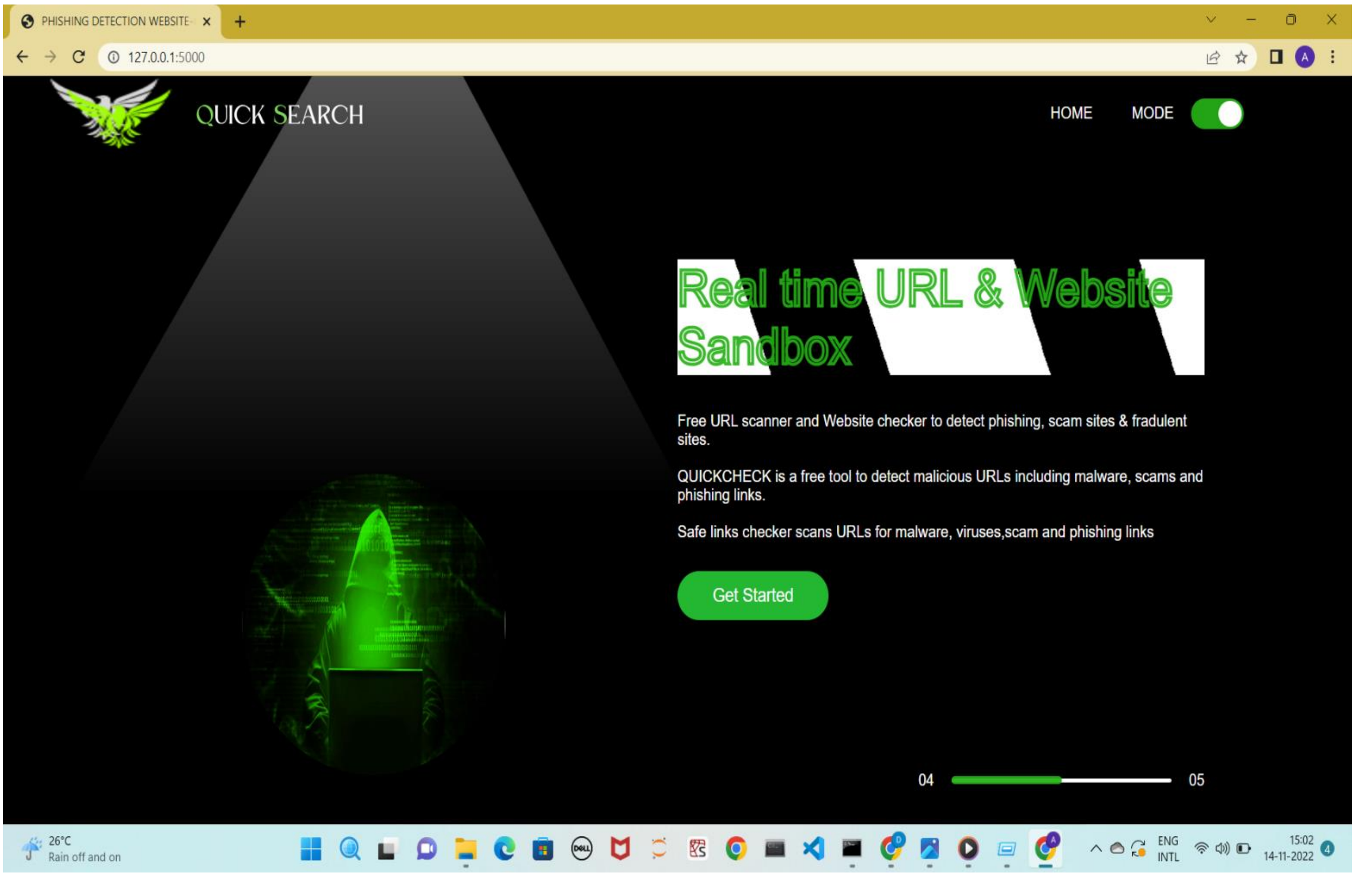
style.css

```
*{
          margin: 0px;
```

```
        padding: 0px;

        /* box-sizing:border-box; */

  }

  body{

        /* background-image: linear-gradient(to right top, #051937, #004d7a, #008793, #00bf72, #a8eb12); */

        background: rgb(2,0,36);

        background: linear-gradient(90deg, rgba(2,0,36,1) 0%, rgba(9,9,121,1) 35%, rgba(0,212,255,1) 100%);

        /* background-image: linear-gradient( 63.1deg,  rgba(5,23,111,1) 16.4%, rgba(24,95,240,1) 64.5% ); */



        height: 100vh;

        font-family: 'Comfortaa', cursive;


  @keyframes typing {

        from {

              width: 0%

        }

        to {

              width: 100%

        }

  }


  @keyframes blink {

        from, to {

              border-color: transparent
        }
        50% {
                border-color: orange;
        }
}
#url
{
        height:90px;
  font-size:14pt;
}
.welcome{
          margin:auto;
          width: 100%;
          font-family: 'Raleway', sans-serif;
          color:azure;
          font-size: 50px;
          font-weight: bold;
          text-align:center;
          padding: 24px;
        }
.userinput{
           padding-top: 3px;
           /* width: 850px; */
           width: 100%;
           /* border: 5px solid gray; */
           margin:auto;
           /* border-collapse: collapse; */
           font-family: Calibri;
           font-style: normal;
           font-weight: bold;
           text-align:center;
           font-family: 'Raleway', sans-serif;
           border-collapse: collapse;
           color:azure;
           /* border-style:green; */
          }
.output{
          padding-top: 3px;
          /* width: 850px; */
          width: 100%;
          /* border: 5px solid gray; */
          margin:auto;
          /* border-collapse: collapse; */
          font-family: Calibri;
          font-style: normal;
          font-weight: bold;
          text-align:center;
          font-family: 'Raleway', sans-serif;
          border-collapse: collapse;
          /* border-style:green; */
         }
         .input-text{
           /* padding-bottom: 5px; */
           font-size: 20px;
```

```
              border: none;
              /* background-color:#A5D9EF; */
            }
            .button{
              margin-top: 25px;
              border-radius: 5px;
              font-family: 'Roboto Mono', monospace;
              padding: 12px;
            }

            button{
              margin-top:50pt;
              margin-bottom:20pt;
              border: none;
              color:black;
              font-weight: bold;
              padding: 15px 32px;
              text-align: center;
              text-decoration: none;
              display: inline-block;
              font-size: 16px;
              margin: 4px 2px;
              cursor: pointer;
            }
#result{
          margin:auto;
           width: 100%;
```

```
            font-family: 'Raleway', sans-serif;

            color:azure;

            font-size: 50px;

            font-weight: bold;

            text-align:center;

            padding: 24px;


}
```

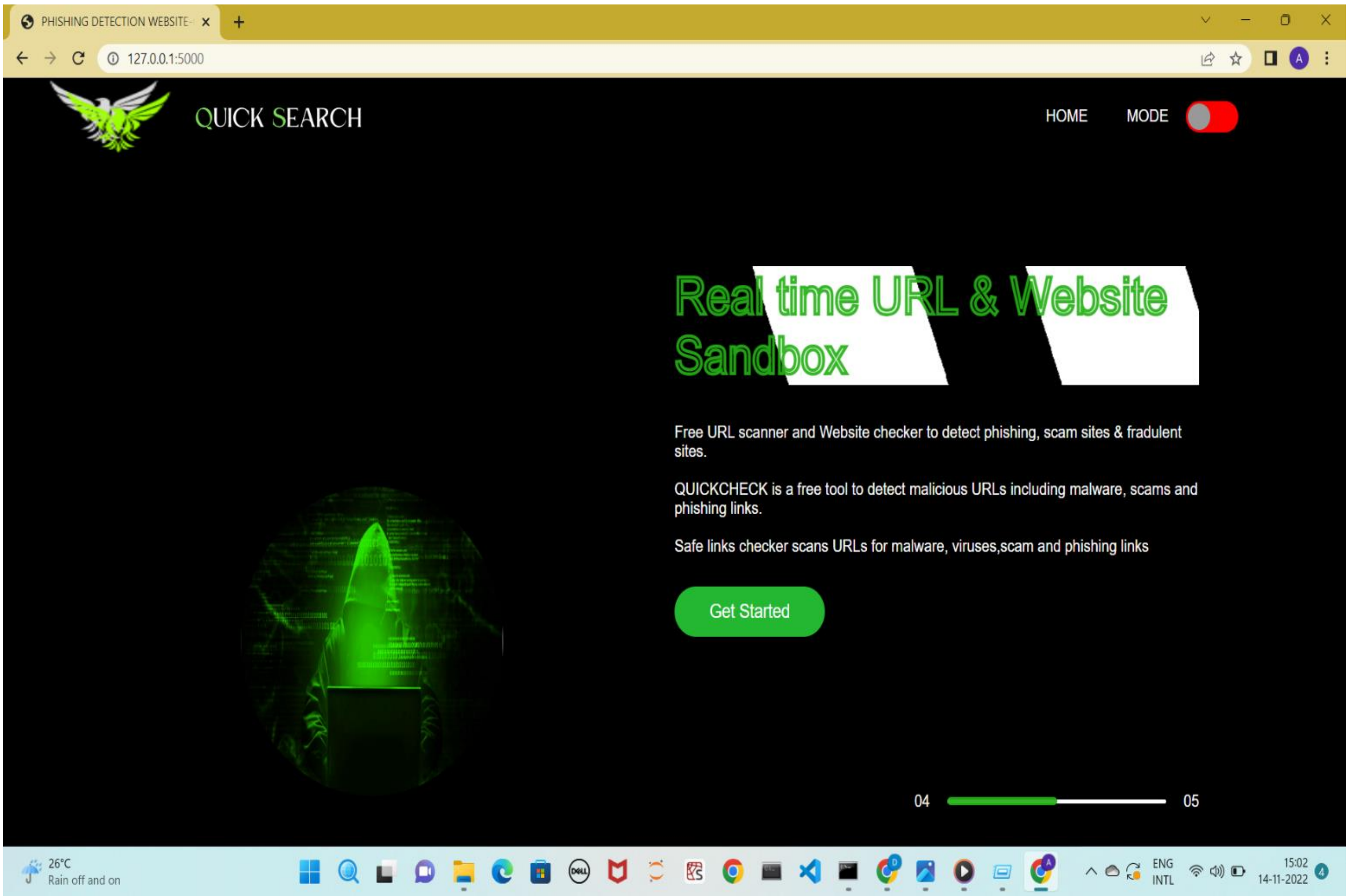


Real time URL & Website Sandbox

Free URL scanner and Website checker to detect phishing, scam sites & fradulent sites.

QUICKCHECK is a free tool to detect malicious URLs including malware, scams and phishing links.

Safe links checker scans URLs for malware, viruses,scam and phishing links

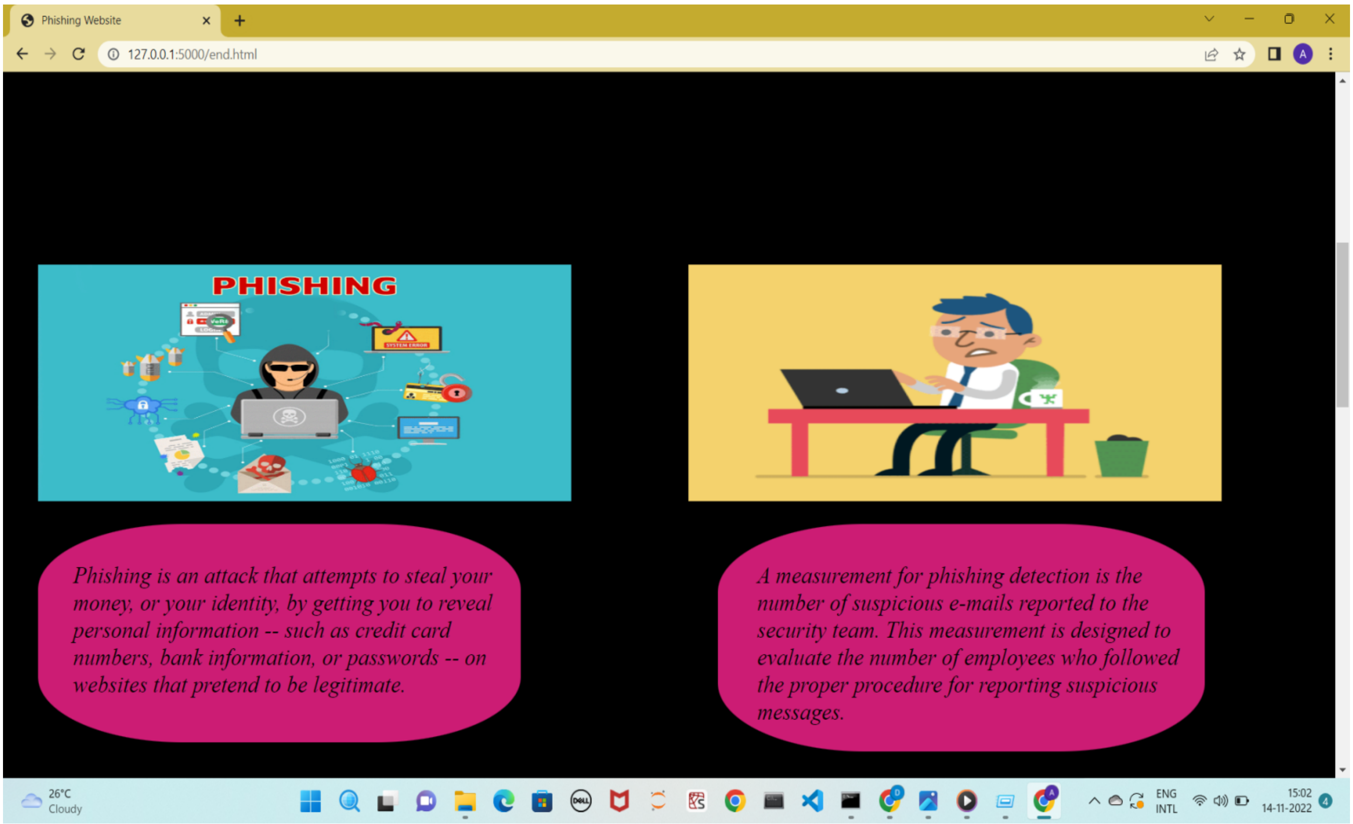


Real time URL & Website Sandbox

Free URL scanner and Website checker to detect phishing, scam sites & fradulent sites.

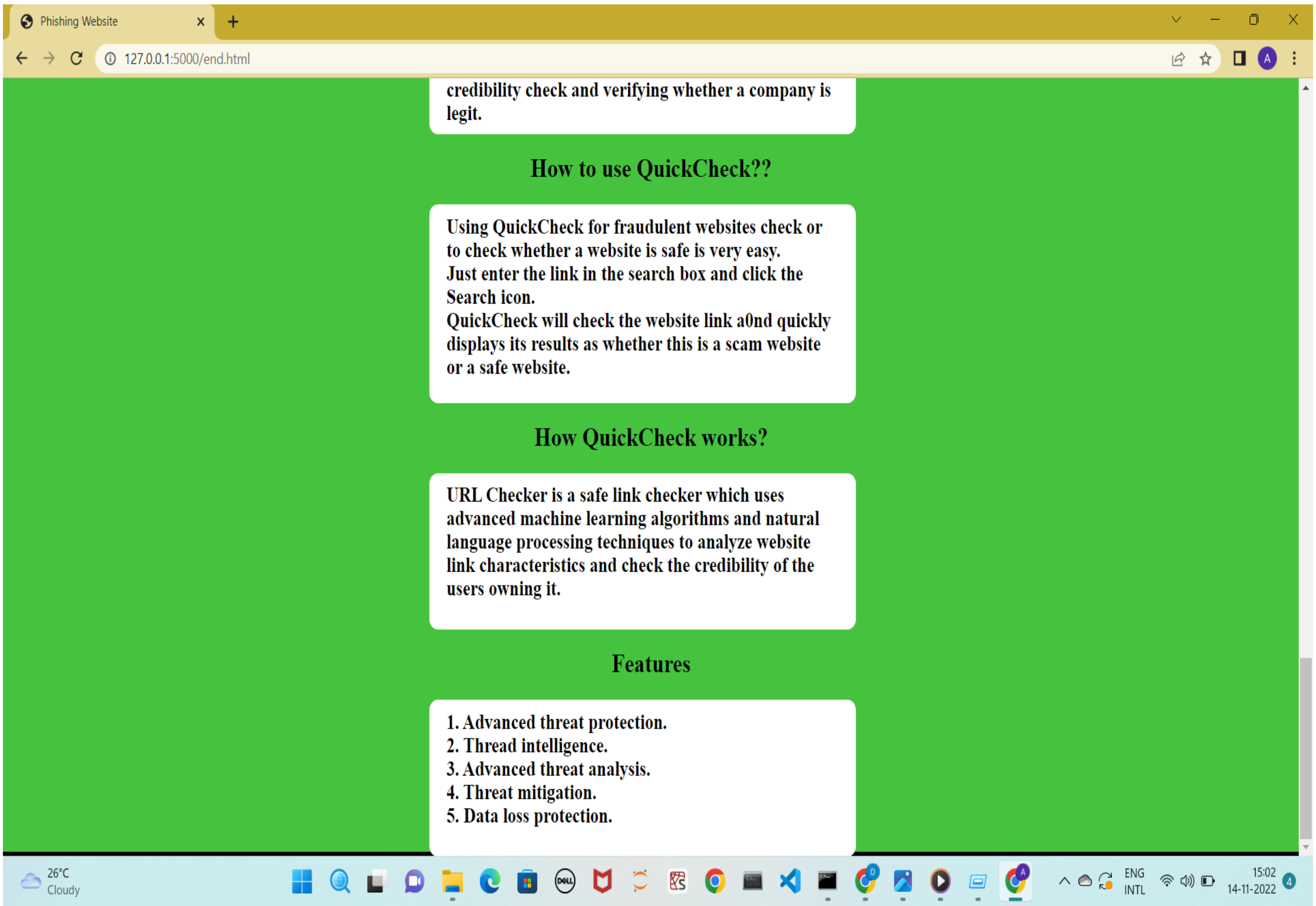
QUICKCHECK is a free tool to detect malicious URLs including malware, scams and phishing links.

Safe links checker scans URLs for malware, viruses,scam and phishing links



Phishing is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate.

A measurement for phishing detection is the number of suspicious e-mails reported to the security team. This measurement is designed to evaluate the number of employees who followed the proper procedure for reporting suspicious messages.



credibility check and verifying whether a company is legit.

How to use QuickCheck??

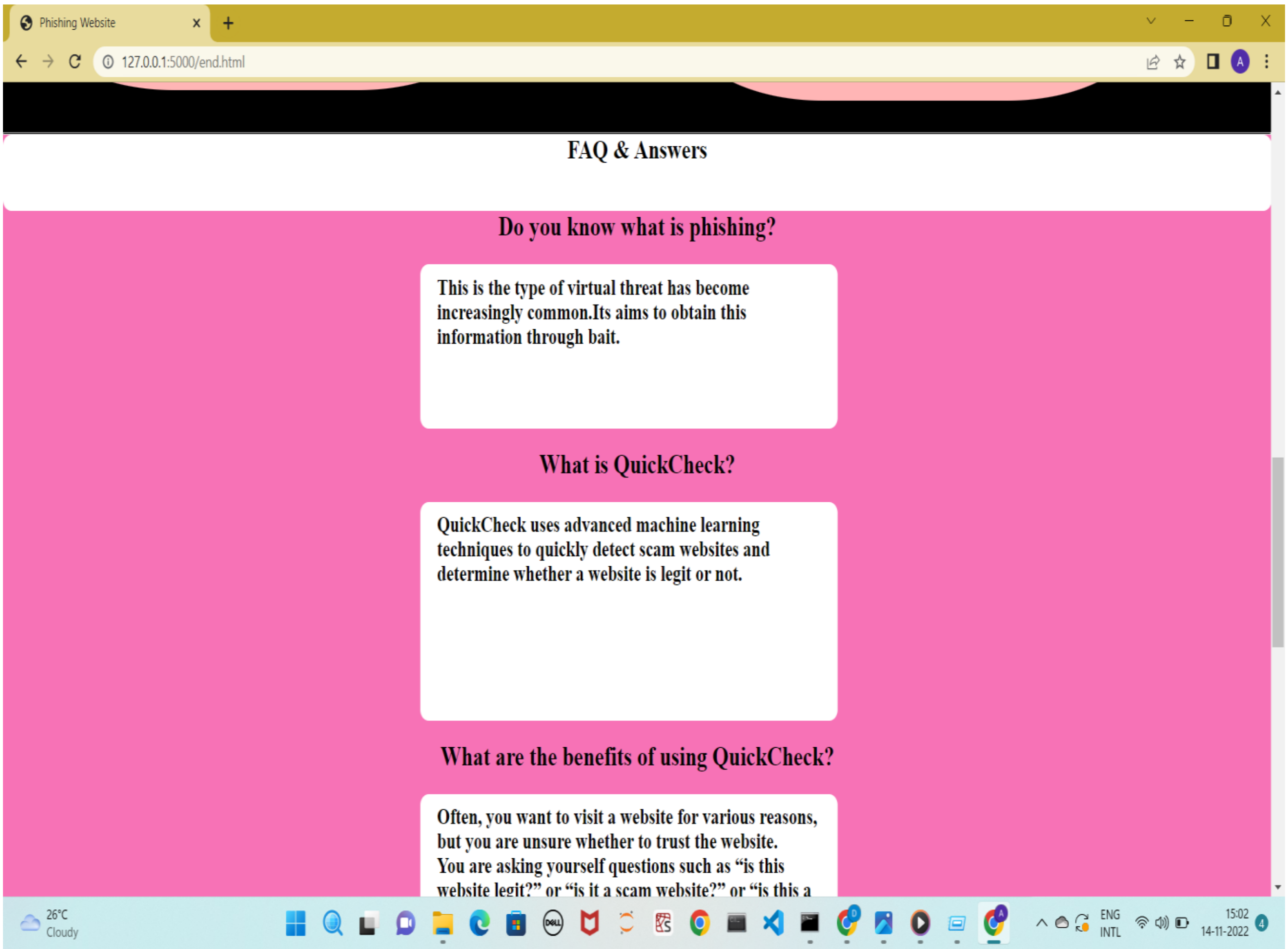
Using QuickCheck for fraudulent websites check or to check whether a website is safe is very easy.
Just enter the link in the search box and click the Search icon.
QuickCheck will check the website link a0nd quickly displays its results as whether this is a scam website or a safe website.

How QuickCheck works?

URL Checker is a safe link checker which uses advanced machine learning algorithms and natural language processing techniques to analyze website link characteristics and check the credibility of the users owning it.

Features

1. Advanced threat protection.
2. Thread intelligence.
3. Advanced threat analysis.
4. Threat mitigation.
5. Data loss protection.



FAQ & Answers

Do you know what is phishing?

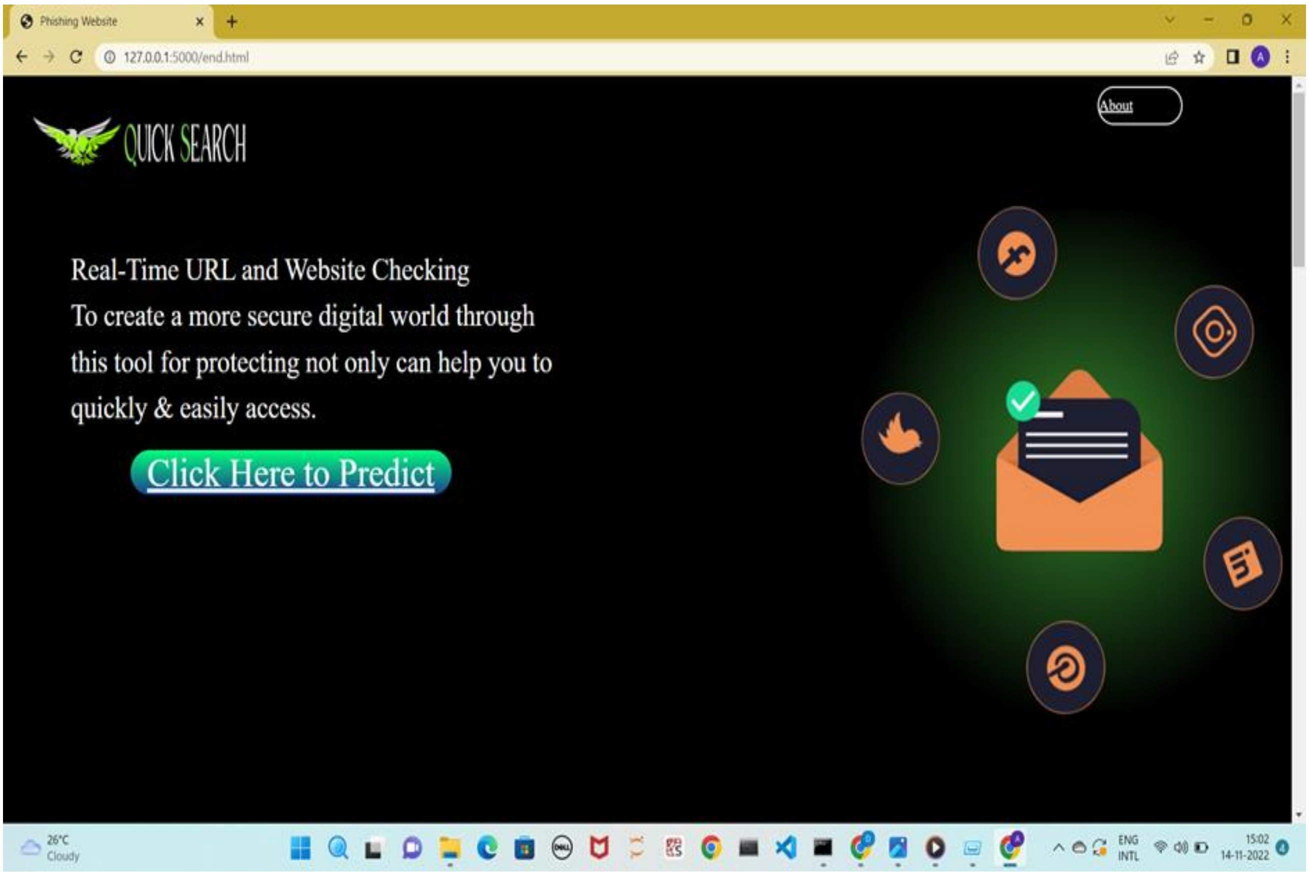
This is the type of virtual threat has become increasingly common.Its aims to obtain this information through bait.

What is QuickCheck?

QuickCheck uses advanced machine learning techniques to quickly detect scam websites and determine whether a website is legit or not.

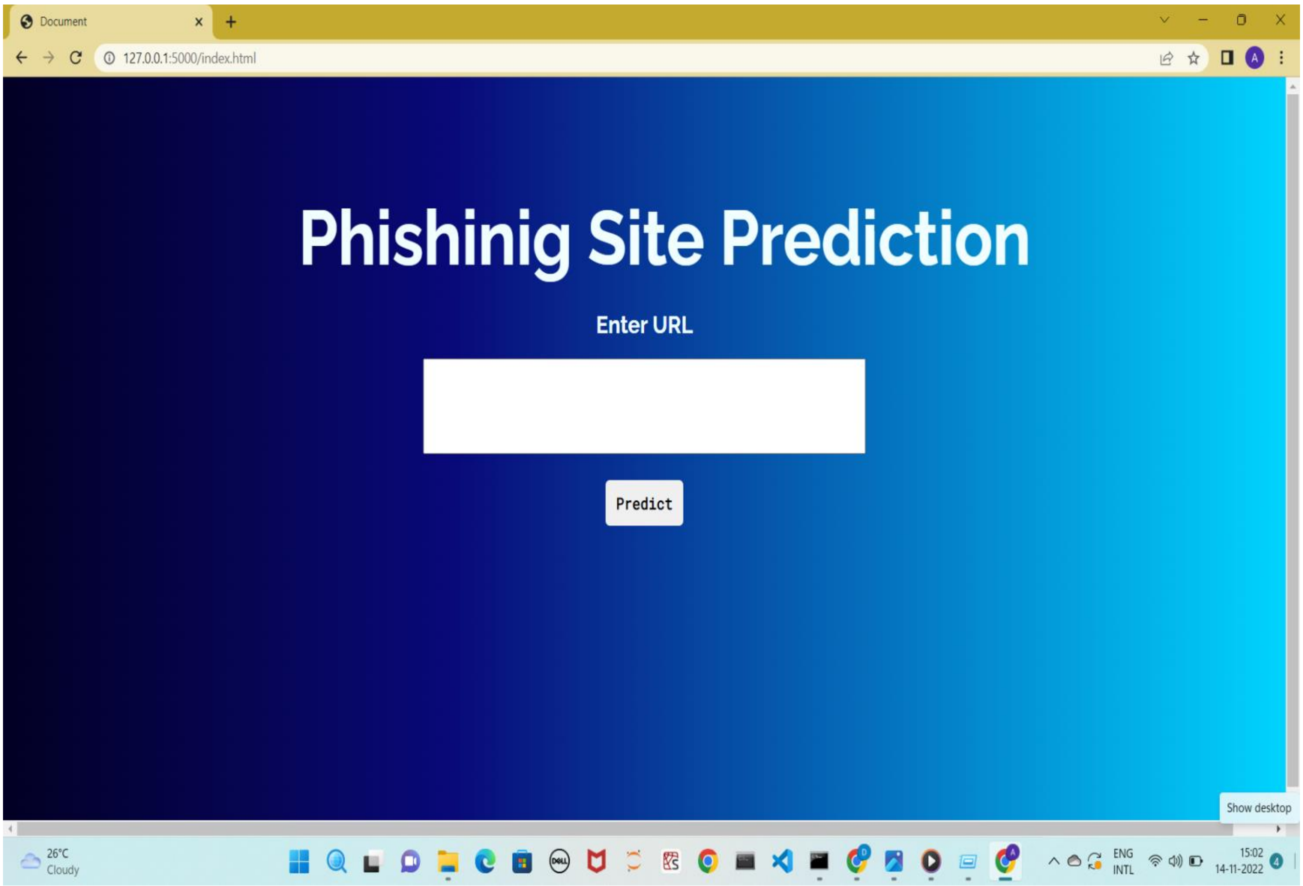
What are the benefits of using QuickCheck?

Often, you want to visit a website for various reasons, but you are unsure whether to trust the website. You are asking yourself questions such as “is this website legit?” or “is it a scam website?” or “is this a



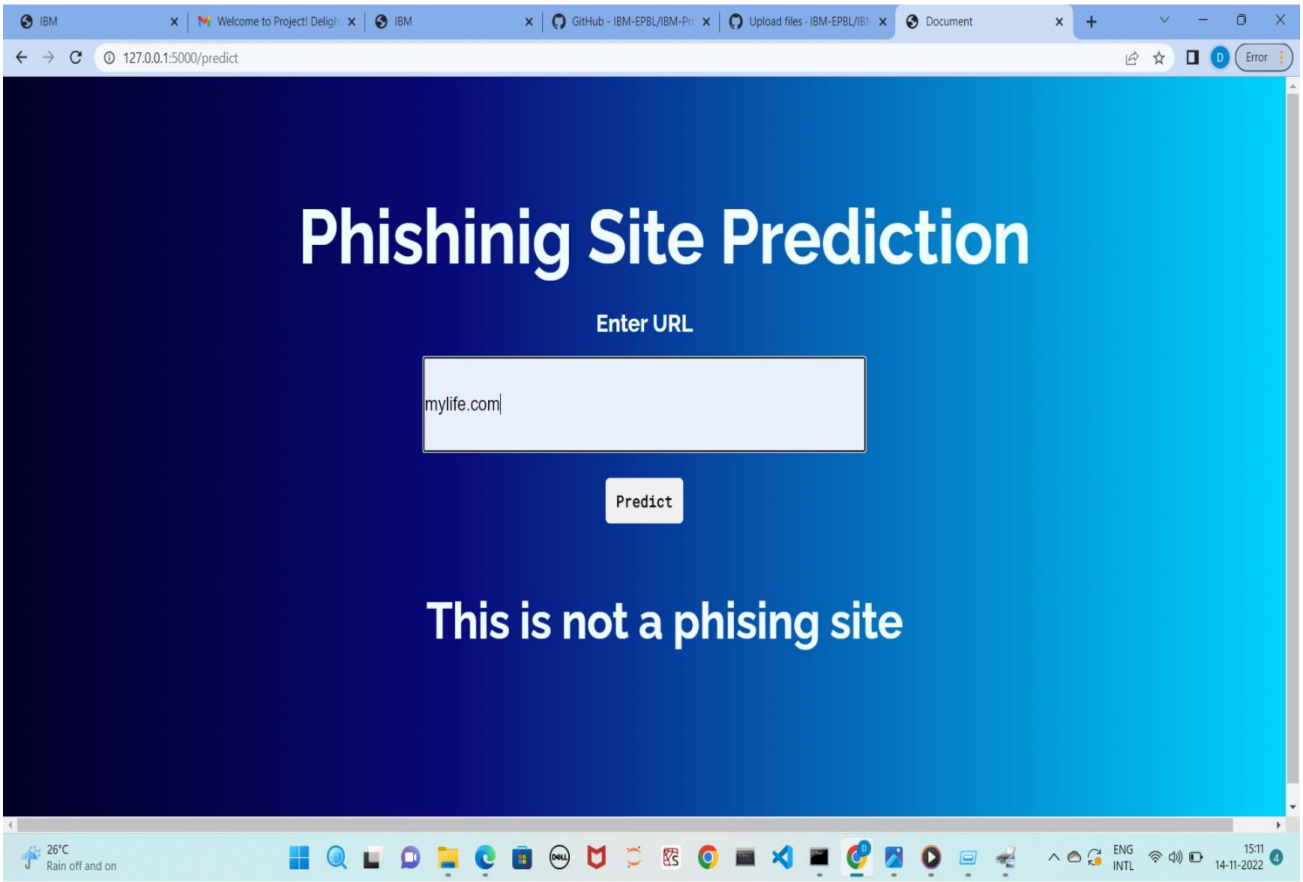
Real-Time URL and Website Checking
To create a more secure digital world through this tool for protecting not only can help you to quickly & easily access.

Click Here to Predict



Phishinig Site Prediction

Enter URL

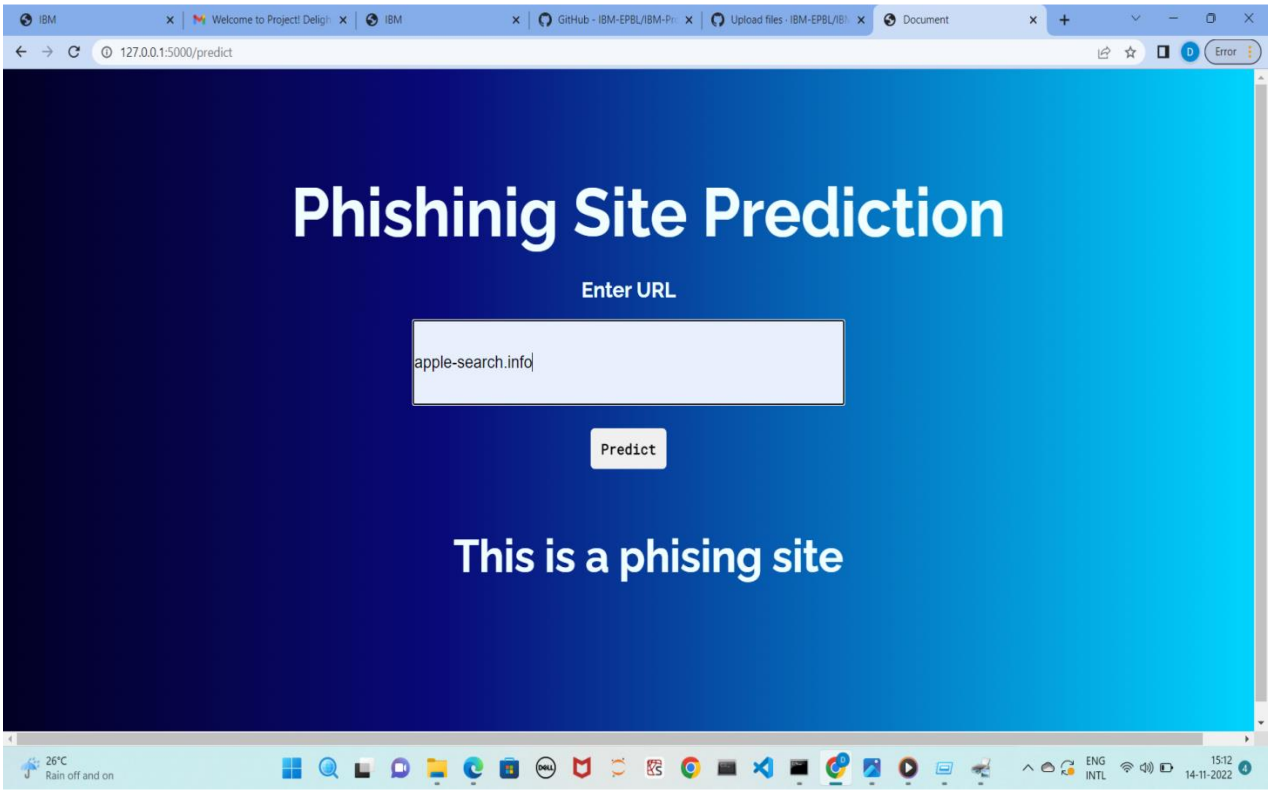


Phishinig Site Prediction

Enter URL

mylife.com

This is not a phising site



Phishinig Site Prediction

Enter URL

apple-search.info

This is a phising site

- **GITHUB LINK:**

  https://github.com/IBM-EPBL/IBM-Project-1835-1658417104

- **PROJECT DEMO LINK:**

  https://drive.google.com/file/d/1GuFHqKrZEXMVdTR1y8JruxiwsP4B3U0Y/view?usp=drivesdk