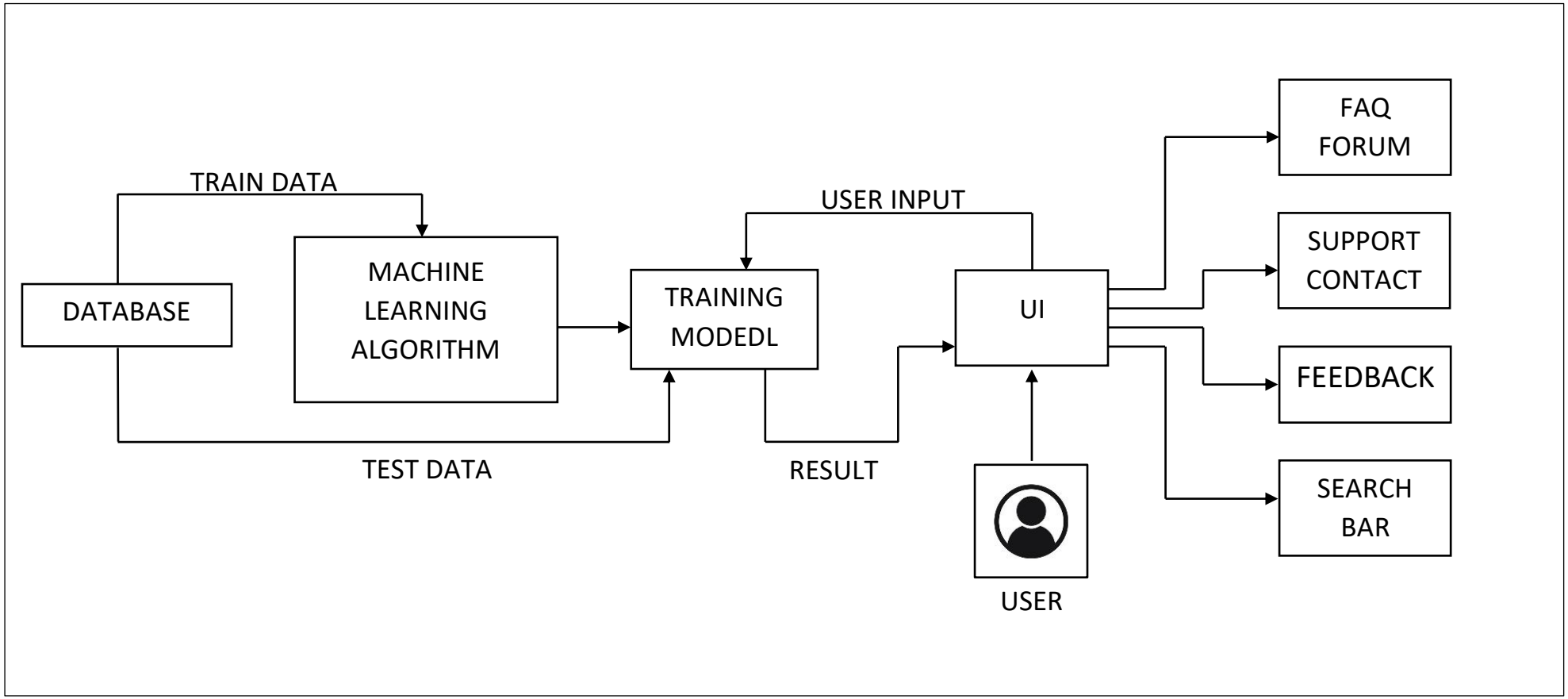
Project Design Phase-I

Solution Fit Document and Solution Architecture

Date	26 September 2022
Team ID	PNT2022TMID10135
Project Name	Project – Web Phishing Detection

SOLUTION ARCHITECTURE:



Define CS, fit into CC

1. CUSTOMER SEGMENT(S)

- In order to do e-banking and other type of payments online a webpage for an online platform is required
- Hackers/cyber thieves use this to their advantage and scams using web phishing sites
- These sites are hardly distinguishable from real sites in their appearance

6. CUSTOMER CONSTRAINTS

- It is hard for the users to e- banking and to do any kind of online transactions due to the possibility of entering a phishing site
- This led the user to lose money and confidential information to scams
- Thus, preventing them from using any kind of online transaction portals and banking

5. AVAILABLE SOLUTIONS

- To find these sites based on appearance is almost impossible hence we need a different method
- So, URL are used to find these sites using a blacklisting method they are stopped by the windows defender and helps the user from entering using warning

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE/PROBLEMS

- Blacklisting requires that the developer to update the newly added phishing site URL to the list every time a new one is discovered
- Thus, they cannot defend/protect the user from newly built of phishing web sites
- Which led to the issue again because when the hackers know that the sites are been discovered they change its URL to avoid detection

9. PROBLEM ROOT CAUSE

- Main problem in blacklisting is that it cannot stop fresh or zero-hour phishing attack
- And the list is need to be updated regularly to reduce the damage cause by web phishing
- So, this method can only reduce or stop the phishing after one or many users are attacked thus it is not an effective method

10. BEHAVIOUR

- The users need to report phishing sites to cyber security dept or respective offices
- So that it can be added to blacklist
- This not only inefficient some users even don't report it and they stop using the platforms altogether

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

Identify Strong TR & EM

3. TRIGGERS

- User's financial losses are really huge due to web phishing.
- Not only individuals even big companies are affected.
- It also leads to confidential information loss

4. EMOTIONS: BEFORE/AFTER

- BEFORE: Users were unsatisfied and highly anxious to use e-banking and online payment platforms.
- AFTER: They find it comfortable and secured to use e-banking and other transaction.

10. YOUR SOLUTION

- The solution proposed is to use a ML based system to detect the web phishing sites.
- Since the URLs can be treated as string, they can be split into different parts based on they attribute and features.
- Based on that we build a classification-algorithm based ML model to identify the web phishing site URLs.
- Its effectiveness can be automatically improved by training it at regular intervals.

8. CHANNELS of BEHAVIOUR

8.1 ONLINE

- Users are avoiding to use e-banking sites form link provided through mails and message due to fear of phishing

8.2 OFFLINE

- Users are visit banks even though they are busy and have even take leave from work

Extract online & offline CH of BE