Problem Statements:

Different Methodologies to identify Phishing websites and their Implementations using algorithms, machine learning and recorded datasets

Raya Rohith

- Non-Genuine Link appearance and brhaviour
- Misspelled keywords and unusual modifications in the webpage
- Prompting for Verification of unrelated credentials
- Visual check for secured web protocols such as "https"

Prasanna Srinivas

- Tracing link routes to detect Link Manipulation
- To check for Extended link to avoid link shortening as most phished websites do shorten with "bit.ly extension"
- Identification of Homograph Spoofing by comparing it with legitimate web domain names

Sakthivel

- Modelling to restrict "redirecting pages" as these URL can be hidden
- Intelligent Web security gateway to monitor all the possible tactical phishing methods
- Spam repository for maintaining web phishing records
- Advanced deployment for web phishing detection

Raghul C

- Filtering out Validation Period. Urge action using time duration
- Analytical juxtapose between legitimate and phishing websites
- Observation of time complexity of loading resources as phished website tends to convey only outlays than legitimate's functionality