VSB Engineering College, karur-639111

Project Design phase – I

Problem Solution fit

Project name: Web phishing detection

Team Id: PNT2022TMID33467

1.Customer segments: - **This project is mainly useful for the** • **Financial services firm** • **Online banking consumer** • **Social network user**	**6.Customer constrains:-** • **User can make online payment securely** • **With help of this system user can also purchase products online without any hesitation**	**5.Available solutions** • **Protect computer by using security software** • **Protect cell phone and computer by setting software to update automatically** • **Protect account by using multi-factor authentication** • **Protect your data by backing it up**
2.Jobs to be done :- **Using the Machine learning technology to detect the phishing attacks Machine learning is one of the critical mechanisms working in tandem with Artificial Intelligence (AI). It is based on algorithms focused on understanding and recognizing patterns from enormous piles of data to create a system that can predict unusual behaviors and anomalies. It evolves with time while learning patterns of normal behaviors. These characteristics make it helpful in identifying phishing emails, spam, and malware.**	**9.Problem route cause: -** **Phishing is a major problem, which uses both social engineering and technical deception to get users' important information such as financial data, emails, and other private information. Phishing exploits human vulnerabilities; therefore, most protection protocols cannot prevent the whole phishing attacks. Many of them use the blacklist whitelist approach, however, this cannot detect zero-hour phishing attacks, and they are not able to detect new types of phishing attacks**	**7.Behavior: -** **Millions of people are being affected and billions of dollars are getting stolen. Phishing is a technique used to extract personal information From victims by means of deceptive and fraudulent emails for identity theft.**

3.Triggers:- • **User lack security awareness** • **Criminals are following money** • **Stealing the sensitive data and login credentials** 4.Emotions:- • **Greed** • **Curiosity** • **Urgency** • **Fear** • **Insecure**	**10.Solution**: - **Using the Machine learning technology to detect the phishing attacks Machine learning is one of the critical mechanisms working in tandem with Artificial Intelligence (AI). It is based on algorithms focused on understanding and recognizing patterns from enormous piles of data to create a system that can predict unusual behaviors and anomalies. It evolves with time while learning patterns of normal behaviors. These characteristics make it helpful in identifying phishing emails, spam, and malware.**	**8.Channels of behavior: -** **To reduce the number of phishing email victims, the following three stages are critical: (1) provide education programs and security tools; this stage can improve victims' awareness about phishing emails and teach them to suspect phishing emails, which is the essential step for detection; (2) introduce victims to strong and immediate confirmation channels such as a website or security email address or a telephone number; and (3) increase the importance of private information by ensuring that there are negative consequences if users lose such information.**