**IDEATION**

**Web Phishing Detection Using Artificial Intelligence**

An increasingly prevalent security hazard nowadays is a cyberattack. Utilizing social engineering platforms, the attackers often aim to gain private information. Phishing has significantly increased online with the development of the internet over the past several years. The annual financial damage to Internet users from phishing is in the billions. The goal of phishing, a social engineering assault, is to identify the victim's personal information and steal it. It often uses email, text messaging, website spoofing, etc. We are unable to reduce the frequency of phishing attacks because attackers use classic approaches such as sending the target some alluring communications in order to deceive them and carry out an attack.

Phishing is a common method attackers employ to send their payloads via emails. The majority of users cannot figure out which received emails have a malicious attach mentor payload. In this case, Al and ML could play a pivotal role in identifying and preventing such phishing attacks. They can scan and identify phishing emails much faster than a human being can. They can also quickly differentiate malicious websites from legitimate websites.

The researcher is thus concentrating on switching from the traditional method to Artificial Intelligence approaches to safeguard internet access.