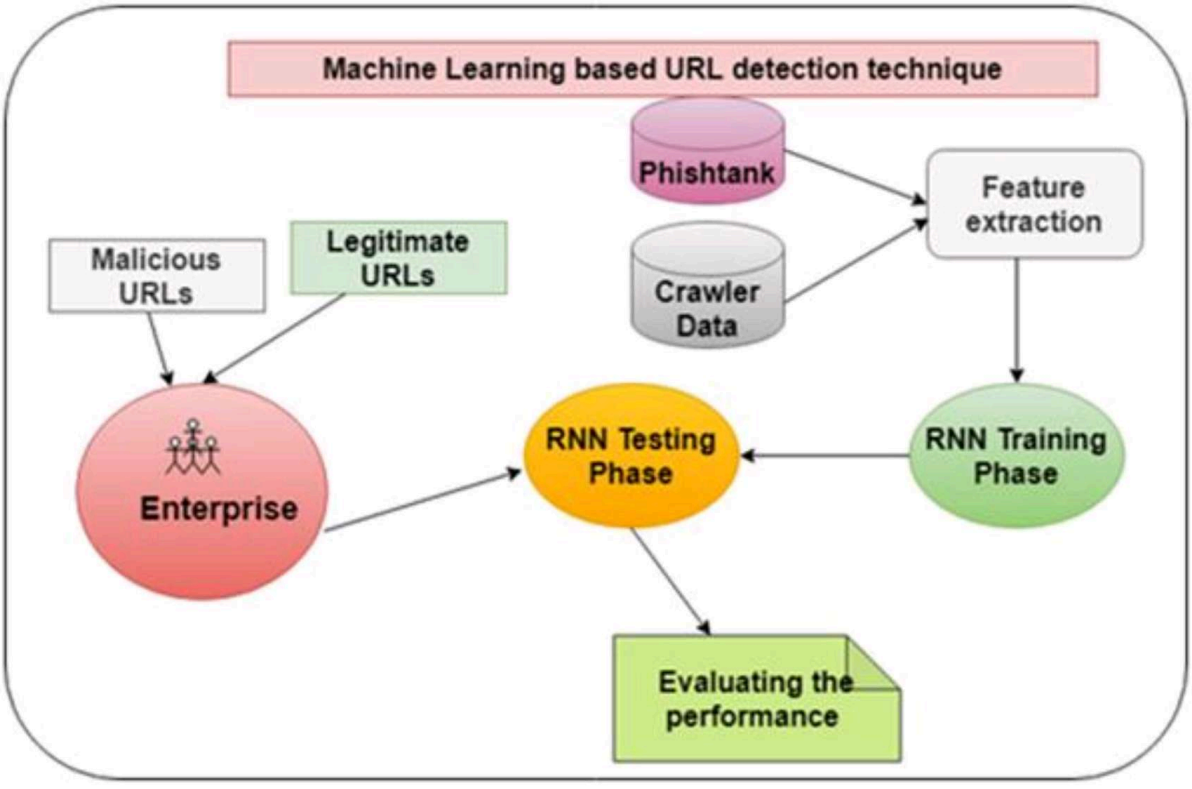
Problem statement

Internet has dominated the world by dragging half of the world's population exponentially into the cyber world. With the booming of internet transactions, cybercrimes rapidly increased and with anonymity presented by the internet, Hackers attempt to trap the end-users through various forms such as phishing, SQL injection, malware, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Among all these attacks, phishing reports to be the most deceiving attack. Our main aim of this paper is classification of a phishing website with the aid of various machine learning techniques to achieve maximum accuracy and concise mode.

Model for web phishing detection :



Question	Description
How can I identify a Phishing scam?	The first rule to remember is to **never give out any personal information in an email.** No institution, bank or otherwise, will ever ask for this information via email. It may not always be easy to tell whether an email or website is legitimate and phishing emails are using social engineering tactics to make create sophisticated scams.
Why is understanding the risk of Phishing important?	• Cause financial loss for victims • Put their personal information at risk • Put university data and systems at risk
How do I report a Phishing or suspicious email?	Reporting suspicious emails can dramatically reduce the duration and impact of an active phishing attack. **Using the EMail web interface:** 1. Open the message 2. To the right of 'Reply' arrow, select 'More' (typically denoted with three vertical dots) 3. Then 'Report phishing'