## Details are in the caption following the image

**Abstract:**

Phishing attacks have recently posed a serious risk to the security of the internet.A phishing attack is a type of cyber attack where the attacker attempts to trick the victim into believing that they are interacting with a legitimate entity, such as a bank, government agency, or well-known company. The attacker does this by sending the victim an email, text message, or other type of communication that contains a link or attachment. When the victim clicks on the link or opens the attachment, they are taken to a fake website or prompted to download malware that gives the attacker access to their personal information or computer systems.Phishing attacks are often used to steal sensitive information such as login credentials, financial information, or personal identification numbers (PINs). They can also be used to spread malware or ransomware, which can cause damage to computer systems or hold data hostage until a ransom is paid.Phishing attacks are a major threat to individuals and organizations because they are often difficult to detect and can have serious consequences. It is important to be cautious when interacting with unfamiliar emails or websites, and to use security measures such as two-factor authentication and antivirus software to protect against these types of attacks.Deep Learning is widely acknowledged as a viable remedy. One way that deep learning can be used for detecting phishing attacks is by training a model to classify URLs or other online communications as either legitimate or phishing attacks based on various features of the communication, such as the sender's address , the content of the message, or the presence of suspicious links. The model can then be used to automatically identify and flag potential phishing attacks, allowing people to protect themselves from falling victim to these scams. There are several datasets that can be used for training deep learning models for detecting phishing attacks baased of the most dataset as phishTank and alexa dataset of URLs with a total of 11430 entries was used.

**Introduction:**

**Proposed Method**

This study used a four-stage technique to accomplish its objectives. Figure 1 depicts the progression of these phases, together with the block diagram for the suggested paradigm.

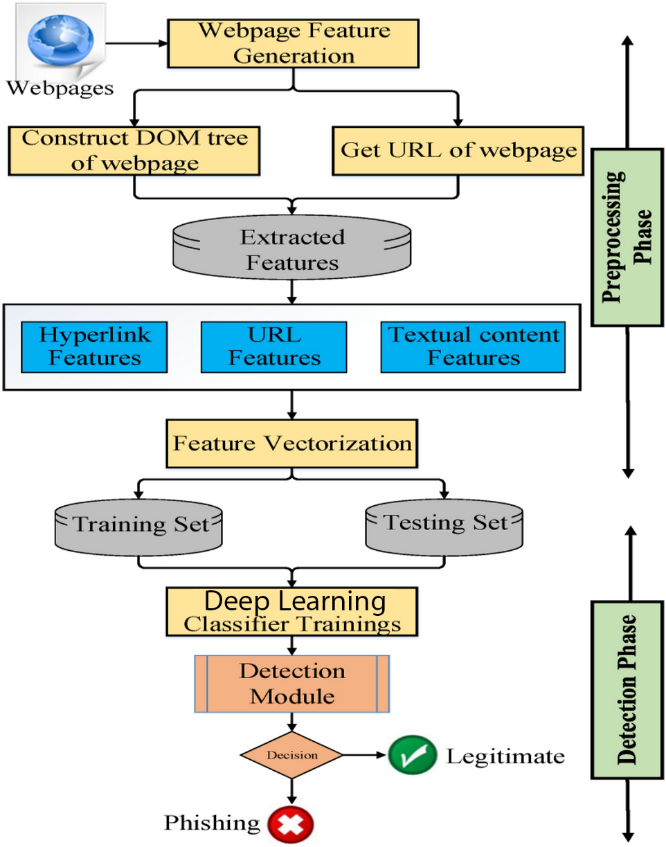


Figure 1Stages of the proposed method

**Stage 1. URL phishing dataset**

The phishing site predict dataset was prepared at this point. Table 2 displays information about the data characteristics (two columns). Additionally, a portion of the data was shown as rows. The table's rows and columns were as follows:

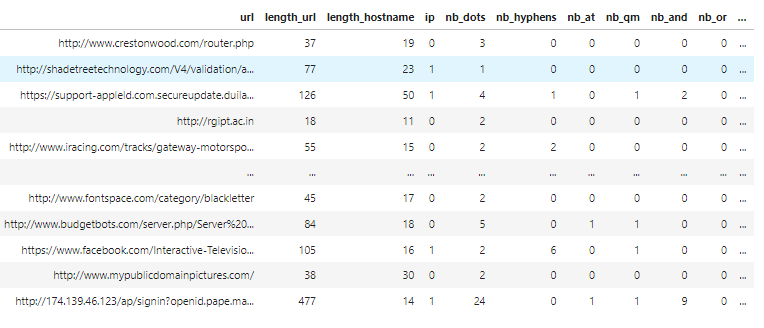


Figure 2Dataset sample records

**Stage 1. URL phishing dataset**

The phishing site predict dataset was prepared at this point. The specifics of the data attributes are shown in Table 2. (two columns). Additionally, a portion of the data was shown as rows. The table's rows and columns were as follows:

1. The URL column: contained **87 Features** around URL , **all Numerical** ,are from three different classes.

- 56 extracted from the Structure and Syntax of URLs (fields starting with *nb\_* , *shortest/longest* , *ratio/length* etc)

- 24 extracted from the Content of their correspondent pages

- 7 are extracted by querying External Services

1. The Label column: contained the corresponding URL detection—phishing or legitimate.

**Stage 2. Data preparation**

The phishing site predict dataset was prepared at this point. The specifics of the data attributes are shown in Table 2. (two columns). Additionally, a portion of the data was shown as rows. The table's rows and columns were as follows:

Python is used to carry out all of the data pre-processing. The following summarizes the model's chosen dataset pre-processing: