**Detecting and Classifying Malicious Uniform Resource Locations Using Advanced Machine Learning**

**ABSTRACT**

In today's digital age, the World Wide Web has become the primary platform for sharing knowledge and conducting economic activities. However, with this undeniable prominence comes the ever-growing concern of cybersecurity. Companies and governments are constantly researching ways to enhance their security measures. Symantec's 2023 Internet Security Report is a comprehensive resource that sheds light on various global threats. These threats range from corporate data breaches and attacks on browsers and websites to spear phishing attempts, ransomware, and other forms of fraudulent cyber activities. The report also exposes the cunning tactics employed by scammers to carry out their malicious deeds. Among the most common cybersecurity vulnerabilities is the existence of malicious websites or Unified Resource Locations (URLs). Every year, billions of rupees are lost due to hosting gratuitous material like spam, malware, unsuitable adverts, and spoofing. These sites often target unsuspecting visitors, luring them into falling for scams through emails, ads, web searches, or connections from other websites. It's crucial to have a reliable system in place that can accurately identify and categorize dangerous URLs as incidents of phishing, spamming, and malware continue to rise. However, implementing such a system is no easy task. The sheer volume of data, ever-changing patterns and technologies, complex relationships between characteristics, lack of sufficient training data, non-linearity, and the presence of outliers make classification challenging. In the proposed work, malicious URLs are detected and classified using advanced machine learning i.e., ensemble modelling. The dataset has been categorized into four types i.e., Phishing, Benign, Defacement and Malware. Here, logistic regression, and ensemble modeling are implemented to detect and classify malicious URLs.