Malicious URL Detection using Deep Learning

ABSTRACT :

With the rapid expansion of internet usage across various sectors, cyber threats have become more frequent and sophisticated. Malicious URLs—disguised to appear legitimate—are widely used to launch phishing attacks, spread malware, and execute data breaches. Traditional detection methods, such as blacklists and rule-based filters, often fall short as they cannot adapt to newly generated or obfuscated URLs. Machine learning techniques have shown improvement but still rely heavily on handcrafted features, limiting their adaptability and automation. This project explores a hybrid deep learning-based approach to malicious URL detection, integrating **BERT** for semantic understanding, **Bi-LSTM** for sequential pattern learning, and a **2D Bloom Filter** for memory-based pattern recognition. The system is designed to analyse URLs directly from their raw structure, detect suspicious patterns, and output a threat probability score. Experimental results show that the proposed model achieves high accuracy while maintaining low false positive and false negative rates. Its performance on both training and validation datasets indicates strong generalization and practical applicability. The project highlights the advantages of combining multiple deep learning strategies to improve detection accuracy, reduce reliance on manual feature engineering, and enable real-time implementation. This work contributes to the development of intelligent cybersecurity solutions capable of adapting to modern online threats.

Keywords: Malicious URL Detection, Deep Learning, BERT, Bi-LSTM, 2D Bloom Filter, Phishing, Cybersecurity, Real-time Detection, Hybrid Model