




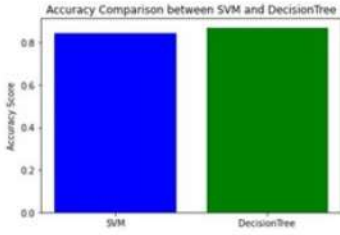
ENHANCING URL REPUTATION FOR MALICIOUS DETECTION USING ML

Srinivasan V - 312420104159

Vamsi G D N - 312420104177

USING MACHINE
LEARNING TO
DETECT
MALICIOUS URLS

Detecting malicious urls with 98% accuracy

OBJECTIVE		ARCHITECTURE DIAGRAM		MODULES							
<p>The primary objective of enhancing URL reputation for malicious detection using machine learning is to develop a robust and adaptive system that effectively identifies and mitigates malicious URLs in real-time.</p>				<p>1.DATA COLLECTION MODULE</p> <p>Responsible for collecting a diverse dataset of URLs, including both benign and malicious samples, from various sources such as web crawlers, threat intelligence feeds, and user reported data.</p> <p>2. MACHINE LEARNING MODEL DEVELOPMENT MODULE</p> <p>Develops and trains machine learning models using the prepared dataset and extracted features. This module explores various machine learning algorithms such as decision trees, random forests, support vector machines (SVM), or deep neural networks to identify the most effective approach for malicious URL detection.</p> <p>3.ADVERSARIAL ROBUSTNESS MODULE</p> <p>Integrates techniques to enhance the system's resilience against adversarial attacks and evasion techniques employed by malicious actors.</p>							
				<p>This module may include adversarial training, input perturbation, or model distillation to mitigate the impact of adversarial manipulations on the system's performance.</p> <p>4.PRIVACY PRESERVATION MODULE</p> <p>Implements privacy-preserving techniques such as data anonymization, encryption, or differential privacy to protect user privacy and sensitive information during URL analysis. This module ensures compliance with data protection regulations and user trust by prioritizing privacy preservation measures.</p> <p>5.SCALABILITY AND DEPLOYMENT MODULE</p> <p>Designs the system to be scalable and deployable in various environments, such as on-premises servers or cloud platforms. This module ensures compatibility with different operating systems, hardware configurations, and network infrastructures, facilitating seamless deployment and integration with existing security infrastructure.</p>							
KEY ASPECTS											
<p>It involves several key aspects to develop an effective and robust system. These aspects encompass various stages of the system's design, implementation, and operation. It also improves the generality of malicious URL detectors.</p>											
REQUIREMENTS											
<table><tr><th>HARDWARE</th><th>SOFTWARE</th></tr><tr><td>Computational Resources</td><td>Programming Languages</td></tr><tr><td>Network Connectivity</td><td>Machine Learning Libraries</td></tr><tr><td>Security Measures</td><td>Data Processing and Analysis</td></tr><tr><td>Backup Systems</td><td>Tools</td></tr></table>	HARDWARE					SOFTWARE	Computational Resources	Programming Languages	Network Connectivity	Machine Learning Libraries	Security Measures
HARDWARE	SOFTWARE										
Computational Resources	Programming Languages										
Network Connectivity	Machine Learning Libraries										
Security Measures	Data Processing and Analysis										
Backup Systems	Tools										
PROPOSED SYSTEM OUTPUT		PERFORMANCE ANALYSIS		CONCLUSION							
<div><p>The proposed system for enhancing URL reputation for malicious detection using machine learning is designed to provide a robust and adaptive solution for identifying and mitigating malicious URLs in real-time. The system encompasses several key components and functionalities to achieve its objectives effectively.</p></div>		<div><p>Performance was measured in terms of the accuracy score between the SVM and Decision tree. Our proposed system aims to utilize the inputs links from any platform and verifies whether the following link is original or fake. Switching algorithm from SVM to Decision Tree increases the accuracy, thereby providing more safer to use the web links and alerts the user if any malicious function detected.</p></div>		<p>In conclusion, the pursuit of enhancing URL reputation for malicious detection using machine learning represents a significant advancement in cybersecurity defense mechanisms. Through the integration of machine learning techniques, this approach offers several compelling benefits, including adaptability to dynamic threats, improved accuracy in detection, real-time threat mitigation, and scalability to handle large volumes of data.</p>							