International Journal of Computer
Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 13, Issue 2, Jul–Dec 2024; 11–18


International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

# COMPREHENSIVE CYBER THREAT ANALYSIS AND PREDICTION: IMPLEMENTING MACHINE LEARNING MODELS IN A DJANGO FRAMEWORK

***Likhita. Y[1], Bandi Naga Vamsi Krishna[2] & Narni Rojesh[3]***

*[1]Department of CSE, SRM Institute of Science and Technology, Kattankulathur, Chennai*

*[2]Department of ECE, Vels Institute of Science Technology, Vellore*

*[3]Department of CSE, SRM Institute of Science and Technology, Kattankulathur, Chennai*

## *ABSTRACT*

*The need for more sophisticated methods of threat identification and prevention arises from the growing intricacy and complexity of cyberattacks. The innovative malware intelligence (CTI) mining architecture presented in this research aims to offer a proactive and all-encompassing cybersecurity defensive strategy. The suggested solution makes use of a variety of data sources and cutting-edge analytic methods to enable businesses to recognize new risks, characterize malevolent individuals, comprehend attack strategies, and make wise security decisions. When integrated into a web application built with Django, the framework provides an easy-to-use interface for organizing and evaluating threat information. Preparing data, implementing models with neural networks (artificial neural networks), support vector machines (SVM), and gradient-boosting algorithms, and predicting threats in real time are some of the main features. Thorough tests are used to assess the system's performance and show how well it can identify and anticipate cyber-attacks.*

*The approach provides timely and actionable intelligence, hence addressing major gaps in current cybersecurity measures. It increases an organization's capacity to implement proactive defense tactics, which lowers the likelihood and severity of cyberattacks. This work makes a substantial contribution to the realm of cybersecurity by providing an in-depth examination of current CTI mining methods and suggesting novel methodologies. The system's ability to strengthen an organization's entire security posture is demonstrated by the testing findings, which make it an invaluable weapon in the battle against emerging cyberthreats. The goal of this research is to close current gaps in the field of cybersecurity and open the door for further developments in proactive cyber protection tactics.*

***KEYWORDS:*** *Cyber Threat Intelligence (CTI), Proactive Cyber Security, Threat Detection, Threat Prevention, Data Mining*

## *Article History*

***Received:*** *26 Jul 2024* **|** ***Revised:*** *30 Jul 2024* **|** ***Accepted:*** *31 Jul 2024*