IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, May 2025
Impact Factor: 7.67

Cybersecurity Threat Detection Using Machine Learning Technique

Prof. Ashwini Mahajan[1], Prof. Komal Naxine[2], Ms. Yashoda More[3]
Assistant Professor, Department of Computer Science and Engineering[1,2]
U.G. Student, Department of Computer Science and Engineering[3]
Tulsiramji Gaikwad-Patil Institute of Engineering & Technology, Mohgaon, Nagpur, Maharashtra, India
ashwini.cse@tgpcet.com, komal.cse@tgpcet.com, achalmore48@gmail.com

Abstract: *The ultramodern world has become fully reliant on cyberspace in all areas of everyday life. Cyber space operations are increasing day by day. moment, the world spends more time online compared to history. With this, the pitfalls of cyberattacks and cybercrimes are increasing. The word' cyber trouble' is known as an unlawful act carried out through the Internet. Traditional styles are unfit to identify zero-day attacks and advanced attacks. To date, mountains of machine learning styles have been created to identify cybercrimes and fight against cyber threats. The end of this exploration work is to put forward the analysis of some of the popular machine literacy styles employed to identify some of the most dangerous cyber pitfalls to cyberspace. We've made a terse overview to measure the performance of these machine literacy styles in the intrusion discovery, spam discovery, and malware discovery based on popularly used and standard datasets.*

Keywords: Cyber trouble; Cybercrime; Performance Evaluation; Machine Learning operation; Intrusion Discovery System; Malware Discovery; Spam Bracket

DOI: 10.48175/IJARSCT-26421