IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, August 2024

Predictive Shield: Harnessing Machine Learning to Forecast Vulnerability Exploitability

Dr Priya P Sajan[1], Sanketan Ashok Mohate[2], Sarthak Kishor Thorat[3], Shakeel Sheikh[4], Shivam Dilip Naik[5], Shivam Kailas Pagar[6]

Senior Project Engineer, C-DAC, Thiruvananthapuram, India[1]

PG-Diploma in Cyber Security and Forensics, C-DAC, Thiruvananthapuram, India[23456]

Abstract*:* *In today's world, cybersecurity risks are getting trickier. It's super important to think ahead about how vulnerable systems might be taken advantage of. This is all about making smart defense tactics. The goal here is to build a system that predicts how weak certain vulnerabilities can be when it comes to attacks. We're using the Common Vulnerability scoring System (CVSS) metrics for this task.*

By digging into a detailed dataset from the National Vulnerability Database (NVD), this project turns the data from JSON format into a CSV table. After that, it finds key characteristics and uses machine learning to guess how likely vulnerabilities are to be exploited. The process involves breaking down CVSS info to identify crucial parts like Attack Vector (AV), Attack Complexity (AC), Privileges Needed (PR), User Involvement (UI), Scope (S), Confidentiality (C), Integrity (I), and Availability (A). All these elements become inputs for our model, which we then tweak and check using various methods to ensure it's accurate & reliable.

The results reveal just how important the selected features & the predictive model are for calculating vulnerability susceptibility. This gives valuable insights for everyone in cybersecurity. Our initiative stresses the importance of preprocessing data, picking relevant features, and using predictive models to make cybersecurity strategies stronger. Going forward, we'll work on improving the model with more data & explore advanced algorithms to boost prediction accuracy. In short, our project shows how data-driven approaches can really help improve cybersecurity defenses and lessen the risks linked with exploitable weaknesses.

Keywords: Exploitability Prediction, Cybersecurity, Machine Learning, CVSS Metrics

DOI: 10.48175/IJARSCT-19378