ABSTRACT

The rising number of information security vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database each year indicates the need for deeper insight into their characteristics and emerging patterns. This study aims to analyze CVE data from 2020 to 2024 to identify vulnerability characteristics, the most common types, and evaluate how these trends affect information security mitigation strategies. The analysis involves data cleaning and transformation, statistical analysis, time series modeling using ARIMA, and classification of vulnerability types based on CWE codes. Results show an increasing trend in CVE occurrences with seasonal fluctuations, with the most frequent vulnerability being CWE-79 (Cross-site Scripting). The optimal model obtained is ARIMA(2,0,2), evaluated with a MAE of 256, RMSE of 256, and MAPE of 13.1%. This study contributes a solid foundation for developing more contextual and responsive risk mitigation strategies aligned with current vulnerability trends.

Keywords : ARIMA, CVE, CWE, risk mitigation, security trends, vulnerability