National Conference on Latest Innovations in Engineering, Science, Management and Humanities (NCLIESMH – 2024)

26th May, 2024, Raipur, Chhattisgarh, India.

CERTIFICATE NO : NCLIESMH /2024/C0524573

A Study of Efficient Detection of SQL - Based Attacks Through Machine Learning

Amarnath Chadchankar

Research Scholar, Department of Computer Science and Engineering,
P.K University, Shivpuri, M.P., India.

ABSTRACT

The efficient detection of SQL-based attacks through machine learning represents a transformative approach to modern database security. As SQL databases remain central to organizational data management, they are frequent targets of attacks such as SQL injection, unauthorized data manipulation, and privilege abuse. Traditional security approaches often rely on static rules or signature-based methods that struggle to detect newly emerging threats or subtle anomalies. Machine learning provides a dynamic and adaptive solution by learning patterns of legitimate database use and distinguishing them from malicious behaviors. By analyzing query structures, user activity logs, access frequencies, and behavioral deviations, machine learning models—such as neural networks, naïve Bayes classifiers, random forests, and clustering algorithms—can efficiently identify suspicious activities in real time. These models continuously improve with exposure to new data, allowing them to adapt to evolving attack techniques. Moreover, machine learning reduces the burden of manual monitoring and significantly lowers false positives, enabling security teams to focus on high-risk incidents. The use of predictive analytics further strengthens the ability to anticipate and mitigate threats before they compromise the system. Thus, machine learning offers an efficient, scalable, and proactive framework for safeguarding SQL databases against increasingly sophisticated cyberattacks.