INTERNATIONAL CONFERENCE ON ADVANCES IN SCIENCE, ENGINEERING, MANAGEMENT AND HUMANITIES (ICASEMH – 2023)

26TH FEBRUARY, 2023

CERTIFICATE NO : ICASEMH /2023/C0223251

Intelligent Intrusion Detection Models for SQL Database Security Using Machine Learning

Amarnath Chadchankar

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

ABSTRACT

Machine learning–based intelligent intrusion detection models have emerged as a highly effective solution for strengthening SQL database security in modern digital environments. As organizations increasingly rely on SQL databases to store sensitive information, threats such as SQL injection, data manipulation, privilege escalation, and unauthorized access have become more sophisticated. Traditional rule-based security mechanisms often fail to identify new or evolving attacks, making adaptive and intelligent systems essential. Machine learning models—such as decision trees, random forests, support vector machines, and deep learning networks—analyze large volumes of database logs, query patterns, and user behaviors to automatically identify anomalies that may indicate malicious activity. These models continuously learn from historical attack data and legitimate usage patterns, improving their accuracy in detecting subtle deviations. Intelligent intrusion detection systems not only enhance real-time monitoring but also reduce false alarms by distinguishing between normal and suspicious SQL operations. Features like anomaly detection, pattern recognition, and predictive analytics allow these systems to proactively prevent potential breaches before significant damage occurs. As cyber threats grow more complex, integrating machine learning into SQL database security provides a scalable, automated, and resilient defense mechanism, ensuring data integrity, confidentiality, and overall organizational security.