# ABSTRACT

SQL injection attacks pose a serious threat to databases as they exploit vulnerabilities in the database layer by injecting SQL codes into user databases. The consequences of a successful attack cause unauthorized access to databases and attackers can gain access to sensitive data. So to avoid the data breach and unauthorized access we have to detect whether the executed SQL code at the user side is malicious or not. Even though some methods like parameterized queries, escaping characters and input validation are some traditional techniques to detect SQL injection, they have their own limitations. These methods often rely on manual coding practices and may not identify new attacks. As attackers continuously evolve their techniques to attack and gain access to sensitive data there is a need for advanced solutions that can proactively identify and mitigate SQL injection attacks. AI has the capacity to analyze vast amounts of data, detect patterns, and learn from previous attacks. AI brings significant benefits to the prediction of SQL injection attacks. Its ability to detect anomalies, learn from new attack patterns, recognize complex patterns, reduce false positives, provide real-time protection, and scale to handle large applications makes it an indispensable tool. Here we use count vectorizer to create tokens and give these tokens to a Neural Network Algorithm i.e., Multilayer Perceptron to detect the malicious SQL code. By leveraging artificial Intelligence, we can detect and mitigate malicious SQL codes swiftly and accurately to ensure the safety of databases.

**KEYWORDS:** Artificial Intelligence, Natural Language Processing, Prediction, Malicious SQL codes, Machine Learning, Threat Detection, SQL Injection, Neural Networks, count vectorizer, Multilayer Perceptron.