**4.1 Introduction**

In this chapter, we present our detection of SQL injection attacks using the BERT language model. BERT is distinct from machine learning and deep learning approaches since it is able to both understand context and syntactic patterns of input queries. Therefore, it is more capable of detecting fine-grained differences and underlying malicious patterns which are often embedded in SQL statements. We begin by laying down BERT's architecture and the reasons behind choosing it for this task. We then move on to explaining the preprocessing that must be done in order to make our dataset compatible with BERT's input requirements, and then move on to explaining the fine-tuning process employed in order to train the model for binary classification.

**4.2 Why BERT for SQL Injection Detection**

Machine learning approaches that existed before deep learning systems along with traditional deep learning models frequently encounter difficulties in detecting SQL injection attacks. The models depend on human-engineered features and produce superficial data representations which prevent them from grasping the full meaning of SQL statements. These models find it difficult to recognize intricate malicious patterns which developers purposely hide inside SQL queries.

BERT utilizes its bidirectional transformer architecture to solve these challenges by processing token context from both directions. The system reaches a superior level of semantic analysis which enables BERT to understand the complete syntax and context of SQL queries. BERT demonstrates a substantial enhancement in detection performance for complex SQL attack patterns which earlier models were unable to detect.