(Web applications became a critical part of our routine, supporting everything from e-commerce via social networks and banking to even healthcare services. Their spread has brought about a revolutionary change in the way we relate to each other, communicate, and do business. At the same time, this growing dependency on web platforms also makes them very attractive targets for cyberattacks. Among these threats, SQL injection remains the highest and most dangerous vulnerability, posing a few severe dangers to data security and user privacy.

To counter SQL injection attacks, input validation and parameterization of queries have been used as base security measures, in addition to the extra firewalls for protection. While some of these older techniques can protect against risks, many examples of detection have eluded them when it comes to smarter and ever-evolving attacks. Given the very dynamic trends in the cyber world, there lies a need for more advanced and flexible measures for detecting real-time malicious SQL queries.

Modern breakthroughs in AI and deep learning have created new room for cybersecurity with intelligent models capable of learning and adapting toward highly complex patterns of attack behavior. Among them, transformer architectures, especially BERT (Bidirectional Encoder Representations from Transformers), can truly be said to stand out in their ability to understand textual patterns and contextual relationships. Although intended for NLP tasks, BERT has potential applications in cybersecurity, including intrusion detection and malice query classification.

This research aims to apply deep learning techniques to establish an intelligent detection system for SQL injection. The focus of training on real-world datasets is to create a highly robust detection framework that distinguishes between legitimate SQL queries and malicious ones with great precision. The principal advantage of our method is its ability to dynamically adapt to new attack patterns, thus adding enhanced security to web applications, unlike the conventional rule-based approach.

 **Chapter 1** is devoted to SQL injection attacks, covering their definition, various classifications, and common techniques employed for their detection.

 **Chapter 2** turns to machine learning and deep learning, examining key algorithmic approaches relevant to intrusion detection. Here, deep learning architectures are considered, and their applicability to cybersecurity is discussed.

 **Chapter 3** covers the overall design of the proposed system, including dataset choice, the chosen deep learning framework, and preprocessing steps necessary to optimize detection accuracy and efficiency.

 **Chapter 4** is allocated for performance evaluation, where we assess our model using several metrics: accuracy, precision, recall, and the F1-score. Additionally, we conduct a comparative analysis against traditional machine learning approaches and existing studies to demonstrate the efficacy of our model.