Secure Pipeline For Machine Learning With Homomorphic Encryption

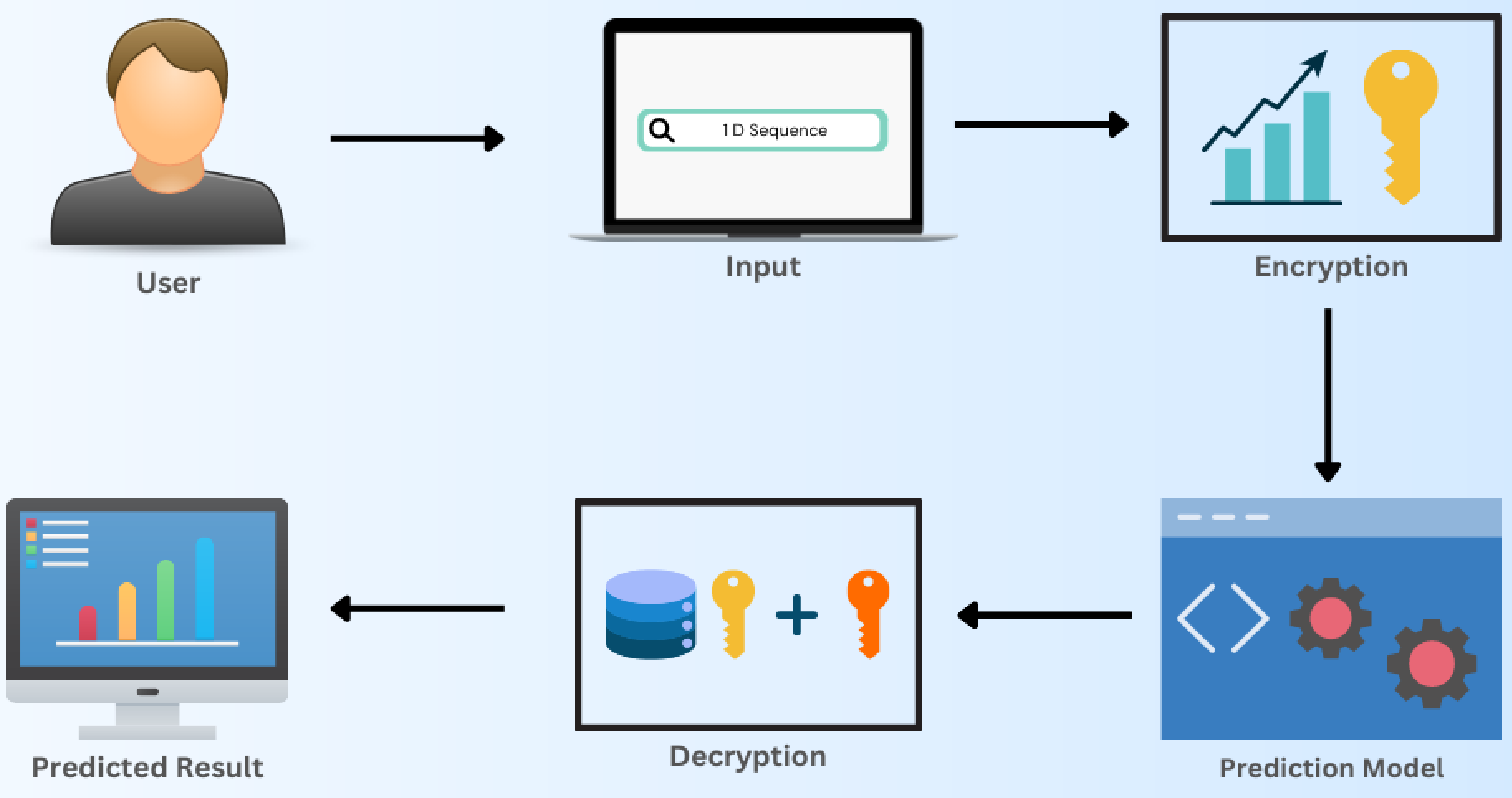
Introduction

In recent years, machine learning algorithms have become highly successful in various fields, but they require access to large datasets that may contain sensitive information. The data collected can provide significant benefits, but it also presents a significant risk, as it can be vulnerable to attacks by malicious actors. Protecting the privacy and security of this data has become a crucial concern for businesses, governments, and individuals.

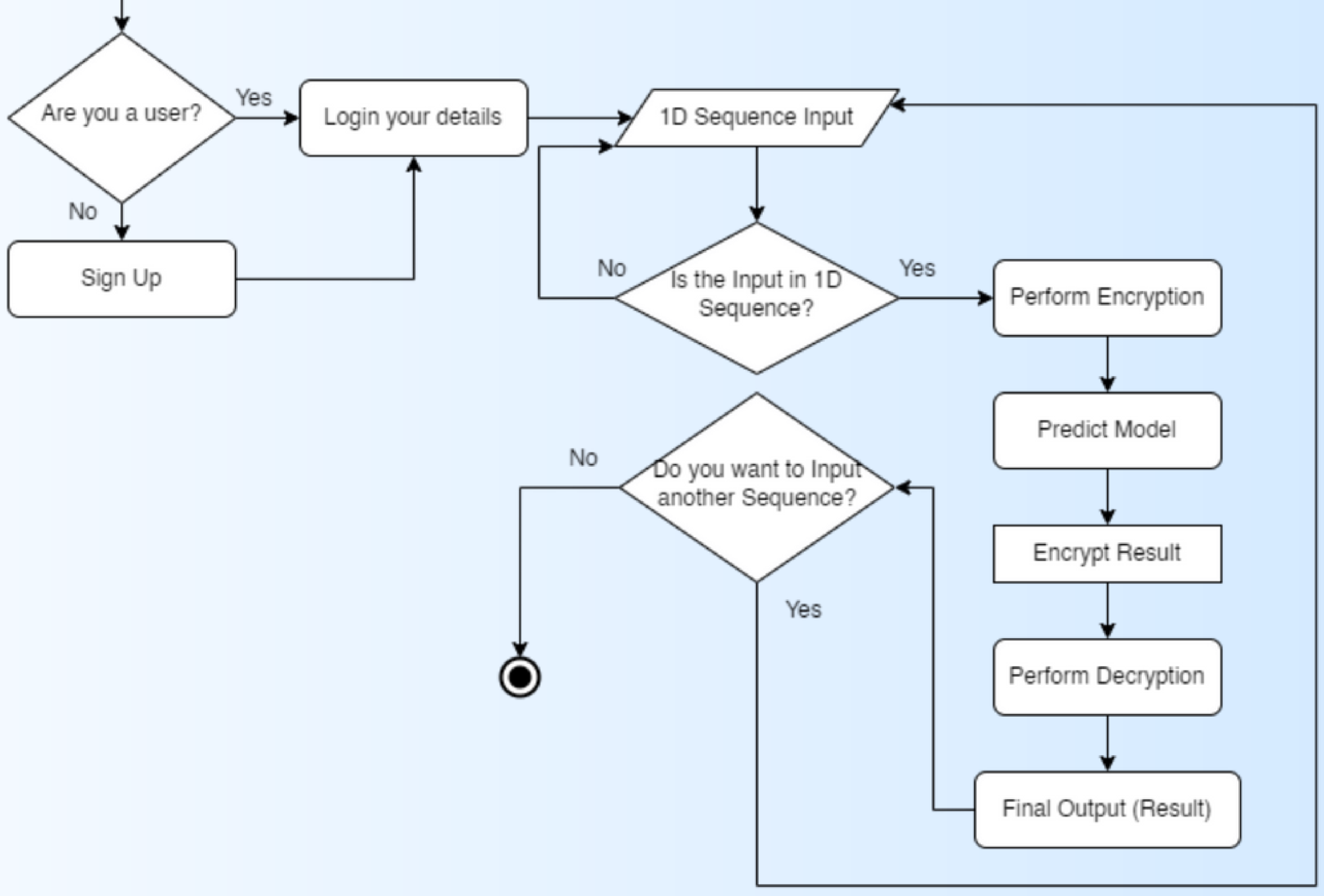
Goal

To address this issue, this final year project introduces secure machine learning as a potential solution. With secure machine learning, data contributors can have peace of mind knowing that their sensitive information remains private, while still benefiting from the insights and analysis provided by machine learning models. By exploring and implementing secure machine learning techniques, this project aims to contribute to the development of effective security measures for machine learning applications.

Workflow



Activity Diagram



Technologies

Supervisor

Mr. Muhammad Amin

Members

Tahawar Ihsan (19P-0097)
Muhammad Abubakar (19P-0027)
Muhammad Javed Iqbal (19P-0088)