**Chapter Four Diagrams**

## 

## 4.3 Use Case Diagram

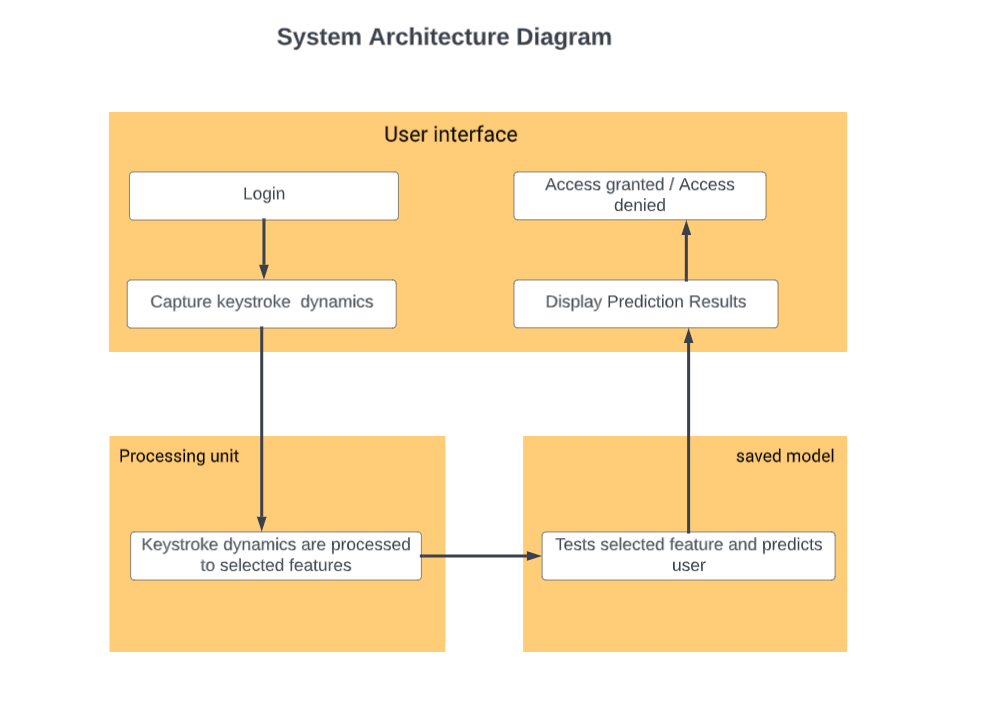
The diagram is an illustration of how the users (actors) interact with various parts of the authentication system. The user enters their credentials on the graphical user interface while their dynamics are captured. The system, controlled by t, generates unique patterns or selected features from the user dynamics, and compares them to the saved model to determine whether it’s the true user or not. If it proves to be the true user, they are thus authenticated.

A diagram of a user case diagram

Description automatically generated

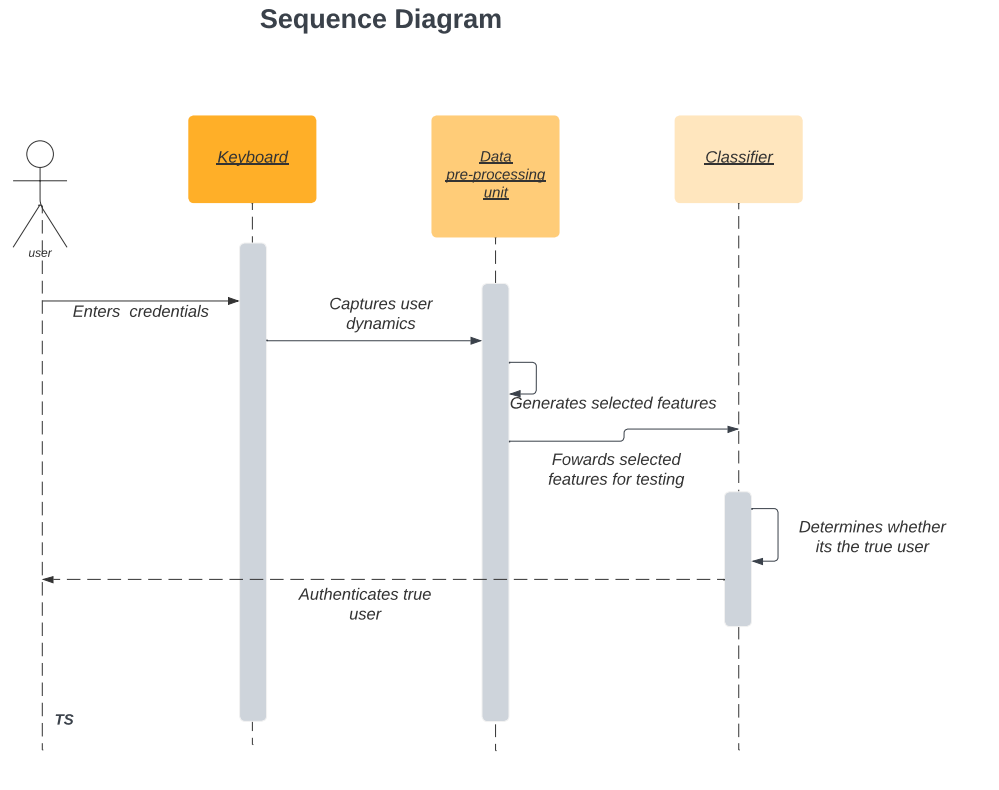
## 4.4 System Architecture Diagram

This system architecture diagram illustrates the flow of data and components in the user authentication system. The graphic user interface (GUI) captures the user’s dynamics during data entry. The captured data is then passed to the data preprocessing unit, which generates unique user patterns or features from the user dynamics. The generated features are then forwarded to the machine learning unit, which learns from these features to make predictions on new input data. The predictions are then evaluated to determine if the authentication is successful. If the authentication is successful, the system grants access to the user. Otherwise, if the authentication fails, the system denies access.



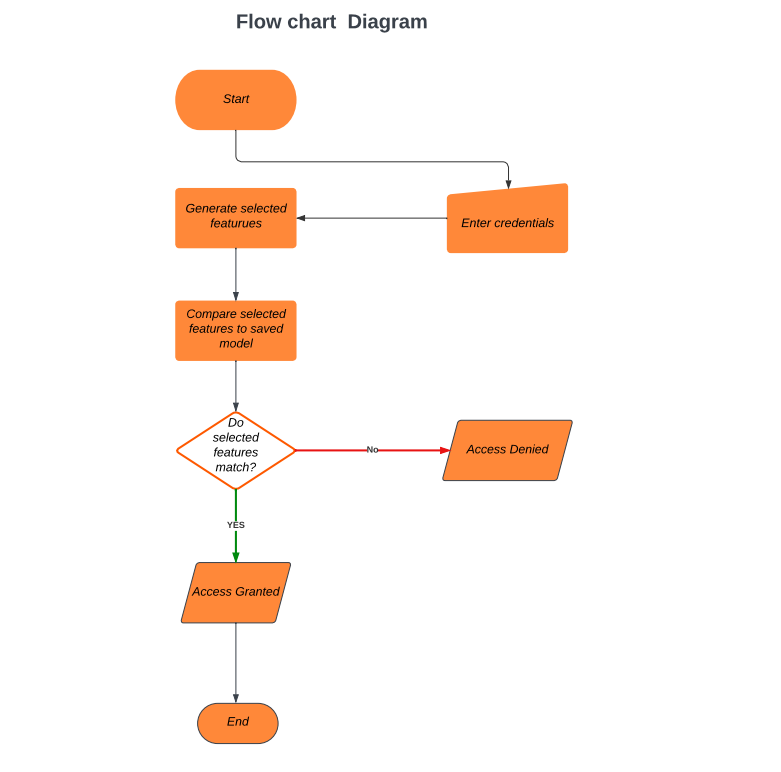
**4.5 Sequence Diagram**

This sequence diagram showcases the flow of interaction between different parts of the user authentication system. The graphic user interface captures the user's keystroke dynamics during data entry. The data pre-processing unit then generates unique user patterns or features from the captured keystroke dynamics. These patterns are sent to the machine learning unit for prediction on new input data. In the diagram, the user interface requests a prediction from the machine learning unit, which uses the trained model to make the prediction. The result is then sent back to the user interface.



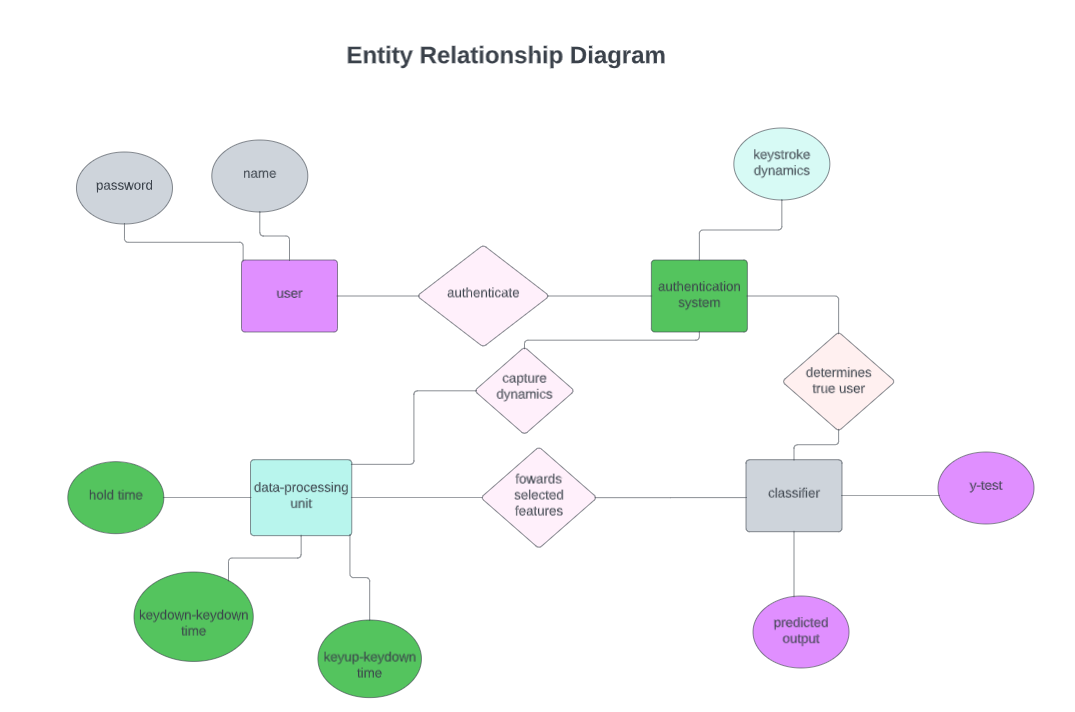
## 4.6 Flowchart Diagram

This flowchart illustrates the flow of actions in the user authentication system. The process begins at the when the user enters their card details and their keystroke dynamics are captured.. The captured keystroke dynamics are then passed to the "Generate selected Features" step, where features are extracted from the keystroke dynamics. Next, the system proceeds to the make predictions, where the machine learning unit uses the selected features to make predictions on the new input data. The result of the prediction is access is either granted or denied depending whether it is the true user or not.



## 4.7Entity-Relationship Diagram

This ER diagram represents the entities and their relationships in the user authentication system. The "User" entity represents the user's information, including the username, password. The "data-processingUnit" entity represents the data processing unit, responsible for generating features from the user dynamics. The "classifier" entity represents the machine learning unit, which learns from the processed features and uses the trained model for making predictions on new input data. The relationships between the entities indicate the flow of data and operations.

****

## 

## 4.8 Class Diagram

This class diagram represents the different classes and their relationships in the user authentication system. The "UserInterface" class captures the KMT dynamics through the captureuserdynamics() method. The "DataPreprocessing" class generates unique user patterns using the generateUniquePatterns() method. The "Classifier" class contains a trained model and has method “determinetrueuser()” that is predicts whether it’s the true user or not

A diagram of a class

Description automatically generated

## 

## 4.9State Machine Diagram

This finite state diagram illustrates the flow of states and actions in the user authentication system. The process begins at the graphic user interface (GUI) where the user captures their dynamics during data entry. The system starts in the "Idle" state. A user then enters their input to the system. The system moves to the "Preprocessing" state to generate unique user patterns or features from the keystroke dynamics. The features are forwarded to the saved ML model then the system moves to the "Predict" state (F) to make predictions on the new input data. After the prediction is made, the system checks if the authentication is successful.If the authentication is successful, the system transitions to the "Logged In" state (H) and grants access to the user . If the authentication fails, the system also transitions to the "Access Denied" state the returns to the "Idle" state (B) to wait for valid input.

A diagram of a state diagram

Description automatically generated