Functional Test Case Template

Feature	Test Case	Steps to execute test case	Expected Output
User Authentication	**Valid User Login**	Open the application's login page. Enter a valid username. Enter a valid password. Click on the "Login" button.	The user should be successfully logged into the system. The application should redirect the user to the home page.
Attack Detection (KNN	**Detection of DDoS attack via KNN**	Feed network traffic data with DDoS patterns to the KNN model.	KNN model should detect the DDoS attack and log the event.
Attack Detection (XGB	**Detection of MITM**	Feed network traffic data with MITM characteri	XGBoost should identify MITM attack and log it.
Session Management	**Session Timeout Han**	Log in, remain idle until session timeout.	Session should expire, redirecting user to login page
Real-time Threat Mitiga	**Automatic Response**	Simulate an attack and observe system response.	System should log the attack and adjust configuratio

Actual Output	Status	More Information
The user is successfully logged in. The application redirects the user to the home page.	Pass	No error messages are displayed. The user profile information is correctly displayed on the home page. Check if the login time is recorded for the user.
KNN model detected the DDoS attack successfully, logging the event with a timestamp and classification label.	Pass	Verify detection accuracy by comparing model output with expected attack classification.
XGBoost model accurately classified and log	Pass	Validate detection effectiveness based on accuracy and proper logging behavior.
User session expired as expected after idle tir	Pass	Confirm no data leakage upon session expiration.
System identified the simulated attack, logged	Pass	Verify logs and configuration adjustments match attack classification.