Table 5.1: Unit Test - 1

|  |  |
| --- | --- |
|  |  |
| Title | Login and Authentication check |
|  |  |
| Test Item | Username, Password,Data packets |
|  |  |
| Input Specification | Test Item containing alphanumeric characters |
|  |  |
| Description | Specified details of Login/Register are entered and stored in database |
|  |
|  |
|  |  |
| Expected Results | Entry for Test Item is created in Database. |
|  |  |
| Result | Pass |
|  |  |

|  |  |
| --- | --- |
|  | Table 5.1: Unit Test - 2 |
| Title | Network Connection Check |
|  |  |
| Test Item | IOT devices,zigbee adapter |
|  |  |
| Input Specification | Test Item containing alphanumeric characters |
|  |  |
| Description | Zigbee protocol is used for connection,communication and sending the sensed data to base station |
|  |
|  |
|  |  |
| Expected Results | Data sensed is sent to the server. |
|  |  |
| Result | Pass |
|  |  |

|  |  |
| --- | --- |
|  | Table 5.1: Unit Test - 3 |
|  |  |
| Title | Intrusion Detection System processing check |
|  |  |
| Test Item | Sensed based data of specified sensor |
|  |  |
| Input Specification | Test item containing various ongoing intrusions on IOT network |
|  |
|  |
|  |  |
| Description | Intrusion detection data is used to detect malicious attacks on the IOT network and ignore normal behavior of the system |
|  |  |
|  |  |
|  |  |
| Expected Results | Category of the attack is determined |
|  |  |
| Result | Pass |
|  | c |

Table 5.1: Unit Test - 4

|  |  |
| --- | --- |
|  |  |
| Title | Notification Check |
|  |  |
| Test Item | Notification page of web application(GUI) |
|  |  |
| Input Specification | Test Item containing processed data |
|  |  |
| Description | Alert only for abnormal behavior of the system |
|  |
|  |
|  |  |
| Expected Results | Alert to the user on the notification page if malicious attacks are detected |
|  |  |
| Result | Pass |
|  |  |

Table 5.2: Integration Test - 1

|  |  |
| --- | --- |
|  |  |
| Title | Intrusion Detection System |
|  |  |
| Description |  |
| Web Application is used to provide an interface between the network connection and the frontend |
|  |
|  |  |
| Test Steps | Run the program for detection of any intrusion on the IOT network |
|  |  |
| Expected Results | Detect the category of an attack |
|  |
|  |
|  |  |
| Result | Pass |
|  |  |

Table 5.2: Integration Test -2

|  |  |
| --- | --- |
|  |  |
| Title | Web Application. |
|  |  |
| Description |  |
| Web Application is used to provide an interface between the frontend and the user |
|  |
|  |  |
| Test Steps | Run the application program |
|  |  |
| Expected Results | Notification on the web page of if any abnormal behavior of the attack is detected |
|  |
|  |
|  |  |
| Result | Pass |
|  |  |

Table 5.3: Acceptance Test -1

|  |  |
| --- | --- |
|  |  |
|  |  |
| Title | Sensed Availability data |
|  |  |
| Description | Ultrasonic sensor and temperature sensor are used to sense data and is processed to gather sensed availability data in the database |
|  |
|  |
|  |  |
|  | Sensed Availability data is sent to the base station using the zigbee protocol |
| Expected Output |  |
|  |  |
|  |  |
| Result | Pass |
|  |  |

Table 5.3: Acceptance Test -2

|  |  |
| --- | --- |
|  |  |
|  |  |
| Title | Performance |
|  |  |
| Description | The time required to transfer data from IOT devices to base station should be as little as possible and the time between the occurrence and detection of the attack should be minimum |
|  |
|  |
|  |  |
|  | Real time functioning of the system is achieved |
| Expected Output |  |
|  |  |
|  |  |
| Result | Pass |
|  |  |