# 5. TESTING

## 5.1 Unit Test Cases

|  |  |  |
| --- | --- | --- |
| Component | Test Case Description | Expected Outcome |
| Sensor Node | Check sensor readings for accuracy under different conditions | Sensor values closely match real-world values |
| Communication Module | Test data packet delivery over MQTT/ZigBee protocols | Packets are delivered reliably without loss |
| Cloud API | Verify data upload and retrieval from cloud storage | Data is stored, retrieved, and consistent |
| Intrusion Detection Unit | Feed known attack patterns to AI-based IDS | Threat is detected and flagged accurately |
| Blockchain Logger | Log sensor transactions in blockchain | Entries are immutable and verifiable |
| Fuzzy Inference Engine | Input fuzzy variables to test rule-based decisions | Decision output aligns with fuzzy logic rules |

## 5.2 Integration Test Cases

|  |  |  |
| --- | --- | --- |
| Integration Scenario | Test Description | Expected Outcome |
| Sensor → Edge → Cloud | Test end-to-end flow from sensing to storage | Data flows seamlessly with low latency |
| Cloud → AI Model → Dashboard | Test DL/ML models analyzing sensor data and visualizing output | Real-time analytics displayed accurately |
| WSN + IDS | Simulate network attacks on WSN and test detection | IDS detects intrusion and system remains stable |
| IoT Devices + Blockchain | Log device data on blockchain and verify immutability | Tamper-proof logs are created and validated |
| Fog Node Response | Test local fog node processing when cloud is unavailable | Fog handles requests and delivers expected services locally |
| Smart Contract Access Control | Deploy contract to control device access | Only authorized devices/users are granted control |