ARCHITECTURE DOCUMENT
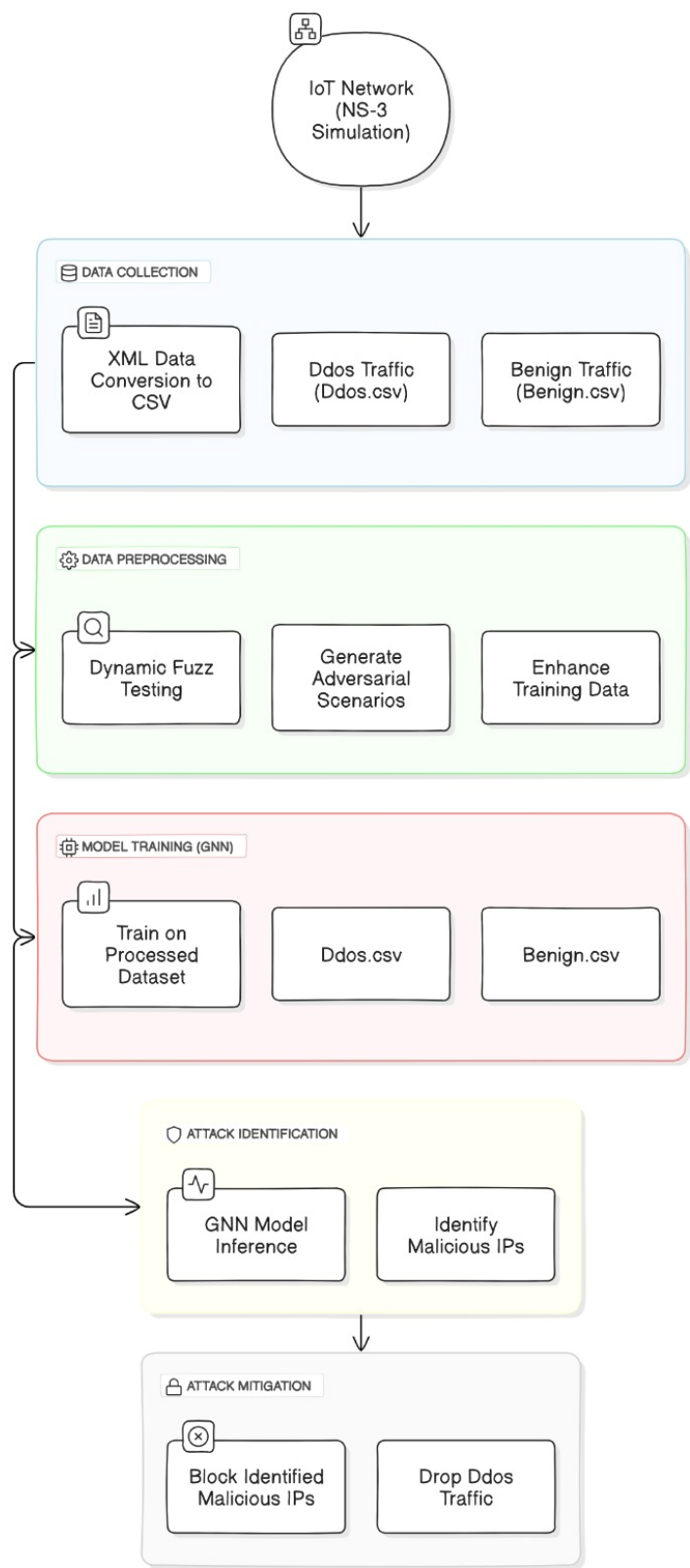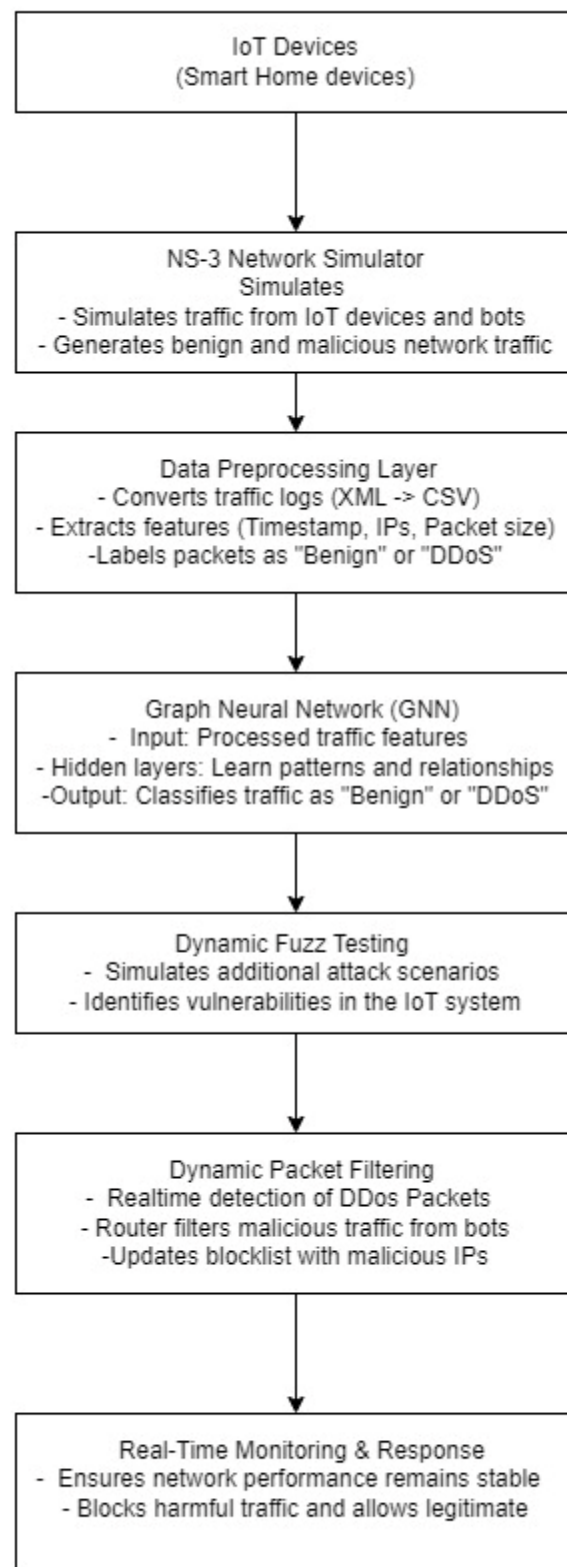
Architecture Diagram:

<u>Scheme Diagram:</u>

```
┌─────────────────────────────────────────────────┐
│              IoT Devices                         │
│          (Smart Home devices)                    │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│            NS-3 Network Simulator                │
│                 Simulates                        │
│   - Simulates traffic from IoT devices and bots  │
│   - Generates benign and malicious network traffic│
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│            Data Preprocessing Layer              │
│     - Converts traffic logs (XML -> CSV)         │
│   - Extracts features (Timestamp, IPs, Packet size)│
│      -Labels packets as "Benign" or "DDoS"       │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│          Graph Neural Network (GNN)              │
│         - Input: Processed traffic features      │
│   - Hidden layers: Learn patterns and relationships│
│   -Output: Classifies traffic as "Benign" or "DDoS"│
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│            Dynamic Fuzz Testing                  │
│      - Simulates additional attack scenarios     │
│     - Identifies vulnerabilities in the IoT system│
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│           Dynamic Packet Filtering               │
│      - Realtime detection of DDos Packets        │
│    - Router filters malicious traffic from bots  │
│        -Updates blocklist with malicious IPs     │
└─────────────────────────────────────────────────┘
                        │
                        ▼
┌─────────────────────────────────────────────────┐
│         Real-Time Monitoring & Response          │
│   - Ensures network performance remains stable   │
│    - Blocks harmful traffic and allows legitimate │
└─────────────────────────────────────────────────┘
```

E-R Diagram:

IoT Devices
- Device_ID (PK)
- Device_Type
- Location
- Status

Traffic Data
- Traffic_ID (PK)
- Source_IP
- Dest_IP
- Packet_Size
- Timestamp
- Label (Benign/Ddos)

Preprocessing
- Preprocess_ID (PK)
- Traffic_ID (FK)
- Features Extracted
- Converted_Format

GNN Model
- GNN_ID (PK)
- Traffic_Features
- Prediction (Label)

Dynamic Fuzz Testing
- Fuzz_ID (PK)
- Attack_Type
- Traffic_Scenario_ID (PK)

Dynamic Packet Filtering
- Filter_ID (PK)
- Blocked_IPs
- Router_ID
- Detection_Timestamp

Real-Time Monitoring & Response
- Monitor_ID (PK)
- Traffic_Anomalies_Detec
- Response_Action