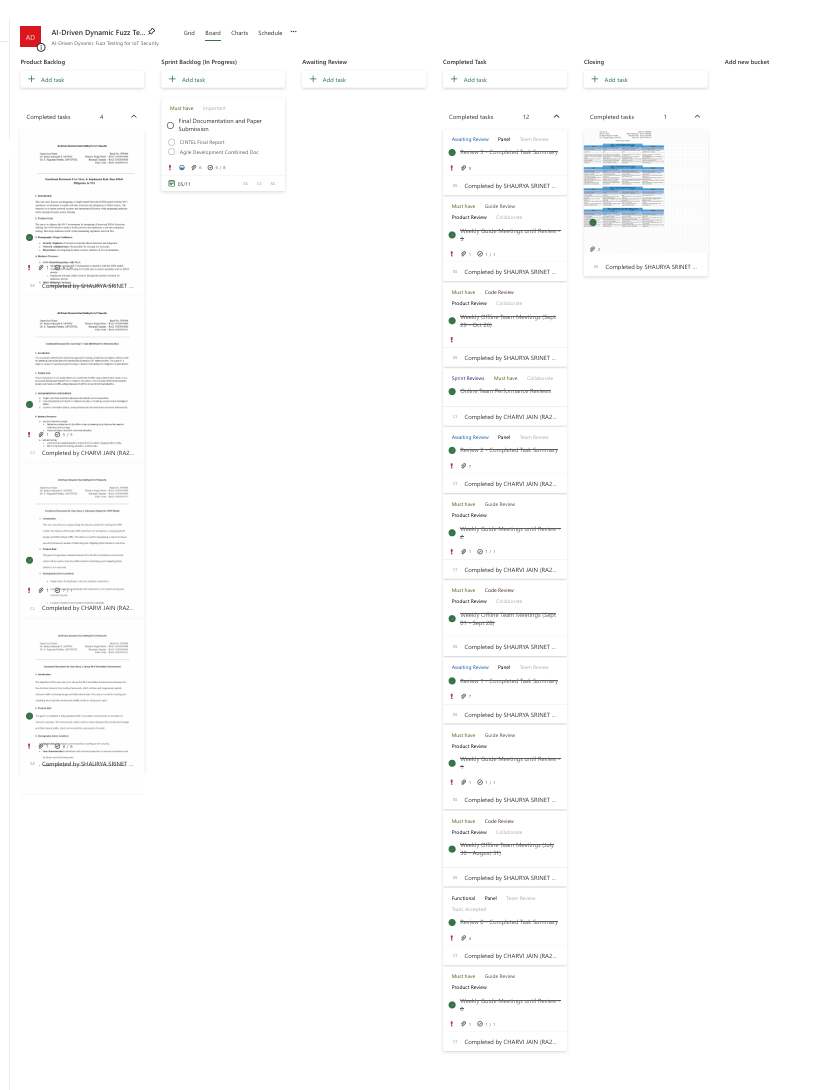
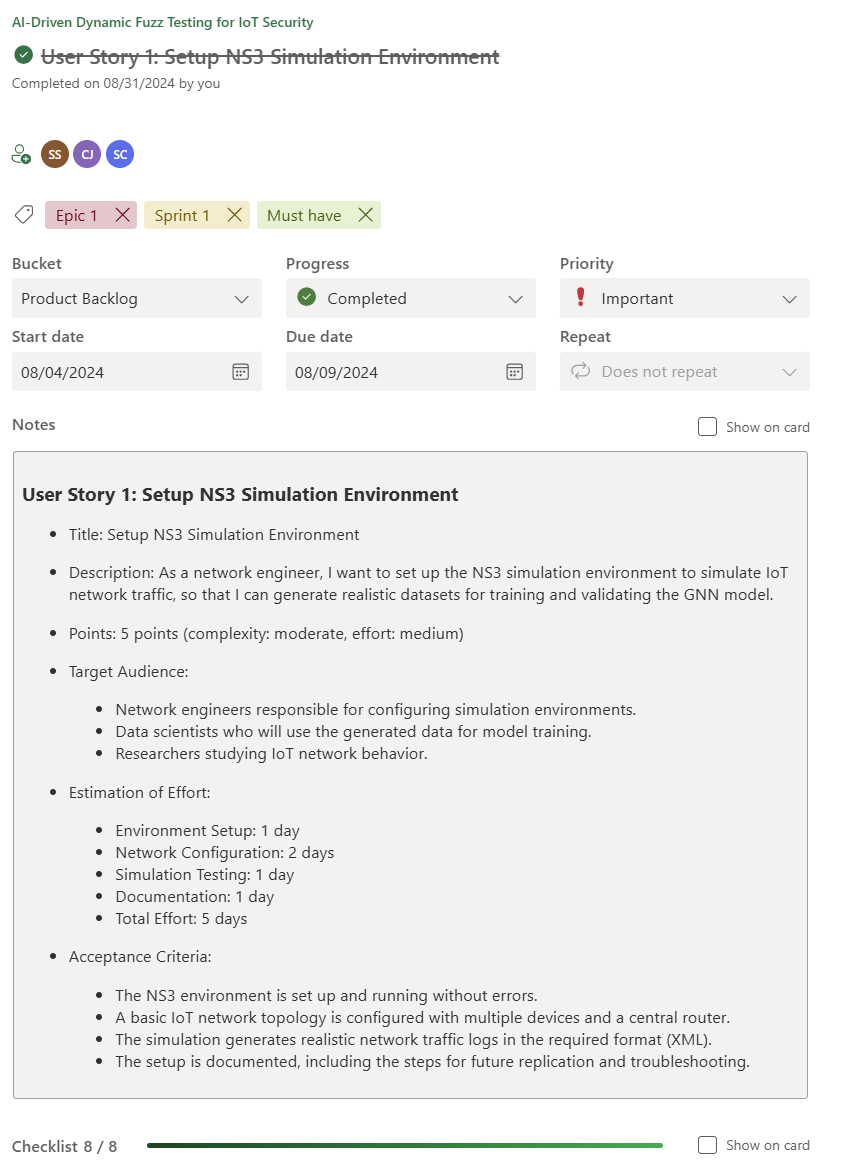
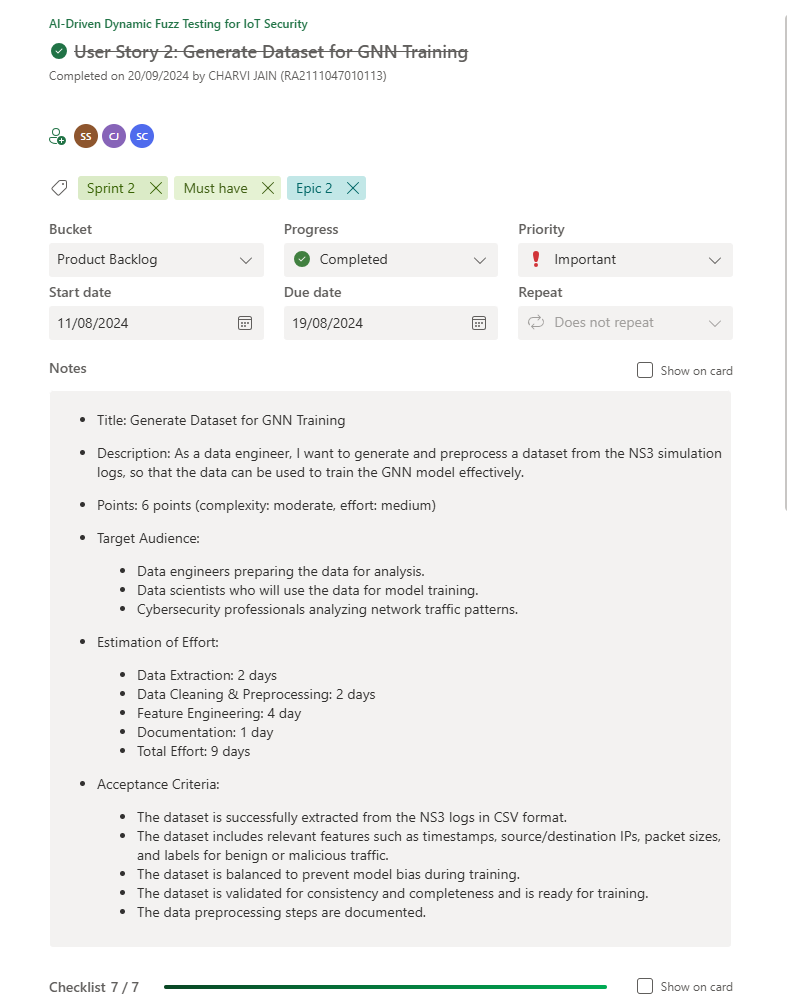
**AGILE DEVELOPMENT**

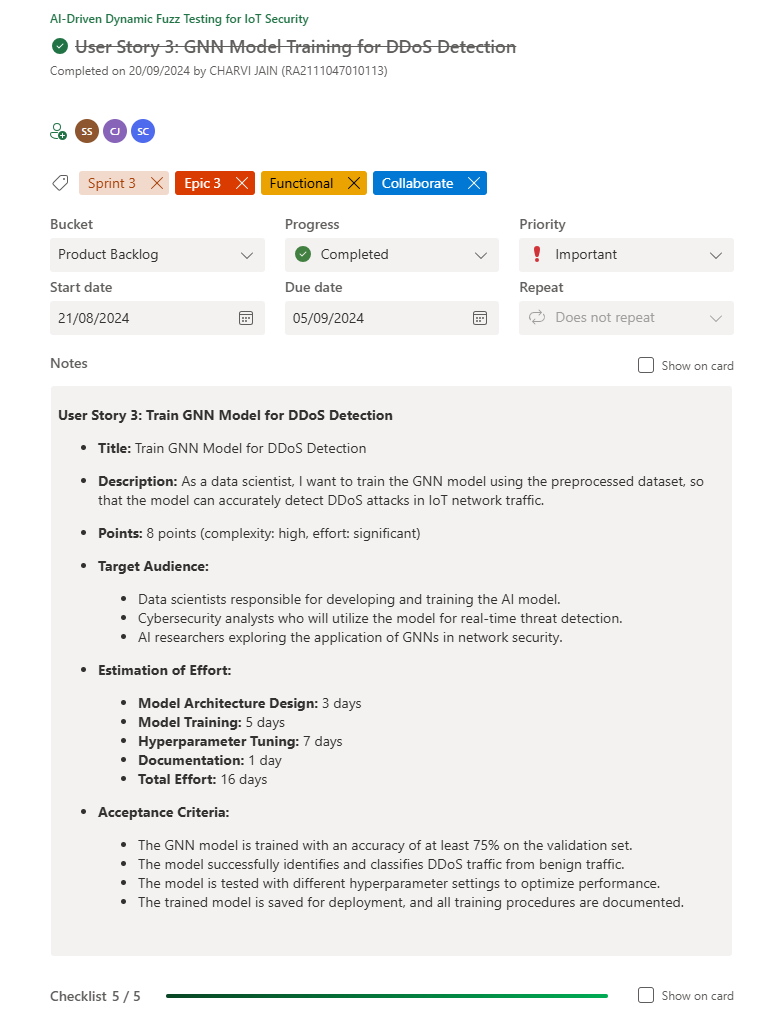
1. **Agile MS Board**
2. **Product Backlog**
   1. **User Story 1**

****

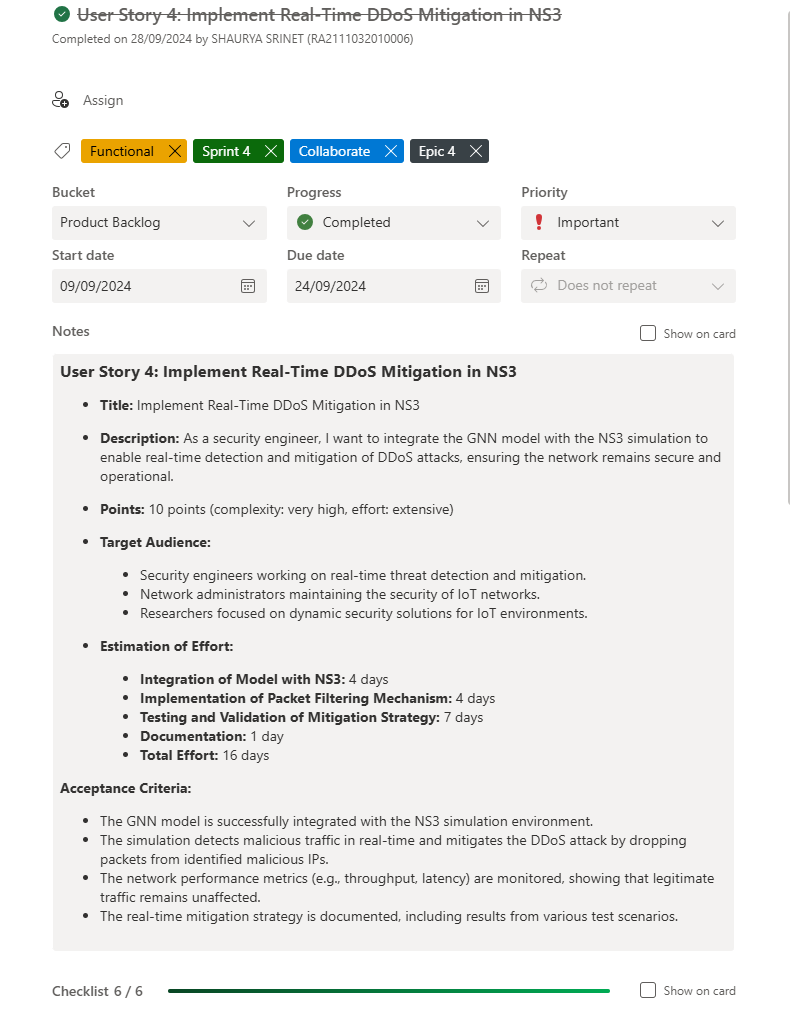
* 1. **User Story 2**

****

* 1. **User Story 3**

****

* 1. **User Story 4**

****

1. **Functional Documents**
   1. **User Story 1**

* **Introduction**

The objective of this user story is to set up the NS-3 simulation environment necessary for the AI-driven dynamic fuzz testing framework, which will be used to generate realistic network traffic, including benign and DDoS attack data. This step is crucial for training and validating the Graph Neural Network (GNN) model in subsequent tasks.

* **2. Product Goal**

The goal is to establish a fully operational NS-3 simulation environment to simulate IoT network scenarios. The environment will be used to create datasets that include both benign and DDoS attack traffic, which are essential for training the AI model.

* **Demography (Users Location)**
  + **Target Users:** Developers and researchers working on IoT security.
  + **User Characteristics:** Individuals with technical expertise in network simulations and AI-driven security frameworks.
  + **Location:** Global usage with an emphasis on research and academic environments.
* **Business Processes**
  + **Simulation Environment Setup:**
    - Install NS-3 on a Linux-based system.
    - Integrate necessary libraries and modules for IoT simulations.
    - Configure network topologies to mimic IoT environments.
  + **Data Generation:**
    - Execute network simulations to generate traffic data.
    - Capture traffic logs in a format suitable for further analysis and model training.
* **Features**
  + **NS-3 Installation and Configuration:**
    - Install NS-3 on the chosen platform.
    - Ensure compatibility with necessary network protocols and IoT configurations.
  + **Network Topology Setup:**
    - Design and implement network topologies that simulate IoT networks.
  + **Traffic Log Generation:**
    - Capture network traffic in logs for analysis and model training.

|  |  |
| --- | --- |
| **ROLE** | **Access Level** |
| Developer | Full access to configure and run NS-3 simulations |
| Researcher | Access to network traffic logs and simulation results. |
| Admin | Full access to system and simulation environment. |

* **Authorization Matrix**
* **Assumptions**
* The development environment remains stable during the setup process.
* The team has access to necessary hardware resources for running simulations.
* Necessary libraries and dependencies are available and compatible with NS-3.
* **Target Audience**
* **Audience:** Developers, Researchers, Academic Institutions.
* **Effort Estimation:** Approximately 3 days to 1 week, depending on complexity and resource availability.
* **Acceptance Criteria**
* NS-3 is successfully installed and configured on the system.
* Network topologies representing IoT networks are implemented.
* Simulation runs successfully, generating traffic logs in the desired format.
* **Checklist**
* NS-3 installed and configured.
* Necessary libraries and dependencies integrated.
* Network topologies designed and implemented.
* Traffic logs generated and verified.
  1. **User Story 2**
* **Introduction**

This user story focuses on generating the dataset needed for training the GNN model. The dataset will include traffic data from IoT simulations, comprising both benign and DDoS attack traffic. This data is crucial for developing a robust AI-driven security framework capable of detecting and mitigating DDoS attacks in real-time.

* **Product Goal**

The goal is to generate a labelled dataset from the NS-3 simulation environment, which will be used to train the GNN model for identifying and mitigating DDoS attacks in IoT networks.

* **Demography (Users Location):**
  1. Target Users: AI developers, security analysts, researchers.
  2. User Characteristics: Individuals with experience in AI model training and network security.
  3. Location: Academic and research institutions globally.
* **Business Processes:**
* **Data Collection:**
  1. Run network simulations to generate diverse traffic patterns.
  2. Capture network logs in XML format.
* **Data Processing:**
  1. Convert XML logs to CSV format.
  2. Label data entries as either benign or DDoS traffic.
* **Data Balancing:**
  1. Ensure the dataset has a balanced representation of benign and DDoS traffic.
* **Features:**
* Traffic Simulation: Execute simulations in NS-3 to generate IoT traffic data.
* Data Conversion: Convert and process XML logs to CSV for model training.
* Data Labelling: Label data entries based on the traffic source as benign or DDoS.
* **Authorization Matrix:**

|  |  |
| --- | --- |
| **Role** | Access Level |
| Developer | Access to raw simulation data and conversion tools. |
| Researcher | Access to the labelled dataset for analysis. |
| Data Scientist | Full access to processed and labelled datasets. |

* **Assumptions:**
* NS-3 simulations are run successfully without errors.
* The XML to CSV conversion script is functional and accurate.
* Labelling criteria are clearly defined and adhered to during data processing.
* **Target Audience:**
* **Audience**: Data Scientists, AI Developers, Researchers.
* **Effort Estimation**: Approximately 1 week for complete dataset generation and processing.
* **Acceptance Criteria:**
* Simulation data is captured and logged correctly.
* XML logs are converted to CSV format without errors.
* Data is accurately labelled as benign or DDoS traffic.
* The dataset is balanced and ready for model training.
* **Checklist:**
* Traffic data generated via NS-3 simulations.
* XML logs converted to CSV format.
* Data entries labelled correctly.
* Dataset reviewed for balance and accuracy.
  1. **User Story 3**
* **Introduction**

This document outlines the functionality required for training a Graph Neural Network (GNN) model for detecting Distributed Denial-of-Service (DDoS) attacks in IoT network traffic. This is part of a larger AI-driven IoT security project focusing on dynamic fuzz testing and mitigation of cyberattacks.

* **Product Goal**

The primary goal is to accurately detect and classify DDoS traffic using a GNN model trained on pre-processed datasets generated from IoT network simulations. The model will differentiate between benign and malicious traffic, aiding cybersecurity efforts in real-time threat detection.

* **Demography (Users and Locations)**
* Target Users Data scientists, cybersecurity analysts, and AI researchers.
* User Characteristics Proficient in network security, AI modelling, and working knowledge of GNNs.
* Location Intended for global use by professionals and researchers involved in cybersecurity.
* **Business Processes**
* Model Architecture Design
* Define the architecture for the GNN model, considering input features like network traffic flow and topology.
* Implement layers tailored for anomaly detection.
* Model Training
* Use the pre-processed dataset to train the GNN model to recognize DDoS traffic.
* Split the dataset into training, validation, and test sets.
* Model Testing and Saving
  + Evaluate the model on a separate validation dataset to assess its detection accuracy.
  + Store the trained model for deployment and further testing.
* **Features**
  + Model Training and Evaluation
  + Training process using supervised learning on labelled IoT network traffic data.
  + Validation to ensure the model achieves at least 75% accuracy in detecting DDoS attacks.
  + Utilize cross-validation to ensure robustness.
* **Hyperparameter Optimization**
  + Various settings tested for optimal model performance such as:
    - Learning Rate
    - Epochs
    - Hidden Layers
    - Batch Size
    - Optimizer
    - Weight Initialization
    - Regularization
    - Activation Functions
    - Loss Function
    - Early Stopping
    - Number of Layers
* **Model Saving**
  + Save the final model for use in deployment environments, enabling real-time detection.
* **Authorization Matrix**

|  |  |
| --- | --- |
| **Role** | **Access Level** |
| Data Scientist | Full access to model training and tuning processes |
| Analyst | Access to trained model and its outputs for threat analysis |
| Admin | Full access to system resources and document |

* **Assumptions**
* The dataset is pre-processed and contains relevant traffic patterns for benign and DDoS scenarios.
* Adequate computational resources are available for training the GNN.
* Model evaluation metrics (accuracy, precision, recall) are pre-defined for validation.
* **Target Audience**

Audience Data Scientists, AI Researchers, Cybersecurity Analysts.

* **Effort Estimation**
* Model Architecture Design: 3 days
* Model Training: 5 days
* Hyperparameter Tuning: 7 days
* Documentation: 1 day
* Total: 16 days
* **Acceptance Criteria**
* The GNN model achieves at least 75% accuracy in detecting DDoS attacks.
* Hyperparameters are tuned to optimize performance.
* The model differentiates between DDoS and benign traffic.
* Training procedures are well documented, and the trained model is saved for deployment.
* **Checklist**
* Model architecture designed and implemented.
* Dataset pre-processed and ready for training.
* GNN model trained and validated.
* Hyperparameters tuned to optimize detection performance.
* Model saved for deployment.
* Documentation completed.
  1. **User Story 4**
* **Introduction:**

This user story focuses on integrating a Graph Neural Network (GNN) model with the NS-3 simulation environment to enable real-time detection and mitigation of DDoS attacks. The objective is to ensure network security and operational efficiency while mitigating malicious traffic through dynamic packet filtering.

* **Product Goal:**

The aim is to enhance the NS-3 environment by integrating AI-powered DDoS detection, utilizing the GNN model to analyse traffic patterns and implement a real-time mitigation strategy that drops malicious traffic while maintaining legitimate network flow.

* **Demography (Target Audience):**
* **Security Engineers:** Focused on real-time threat detection and mitigation.
* **Network Administrators:** Responsible for securing IoT networks.
* **Researchers:** Investigating dynamic security solutions in IoT environments.
* **Business Processes:**
* **GNN Model Integration with NS-3:**

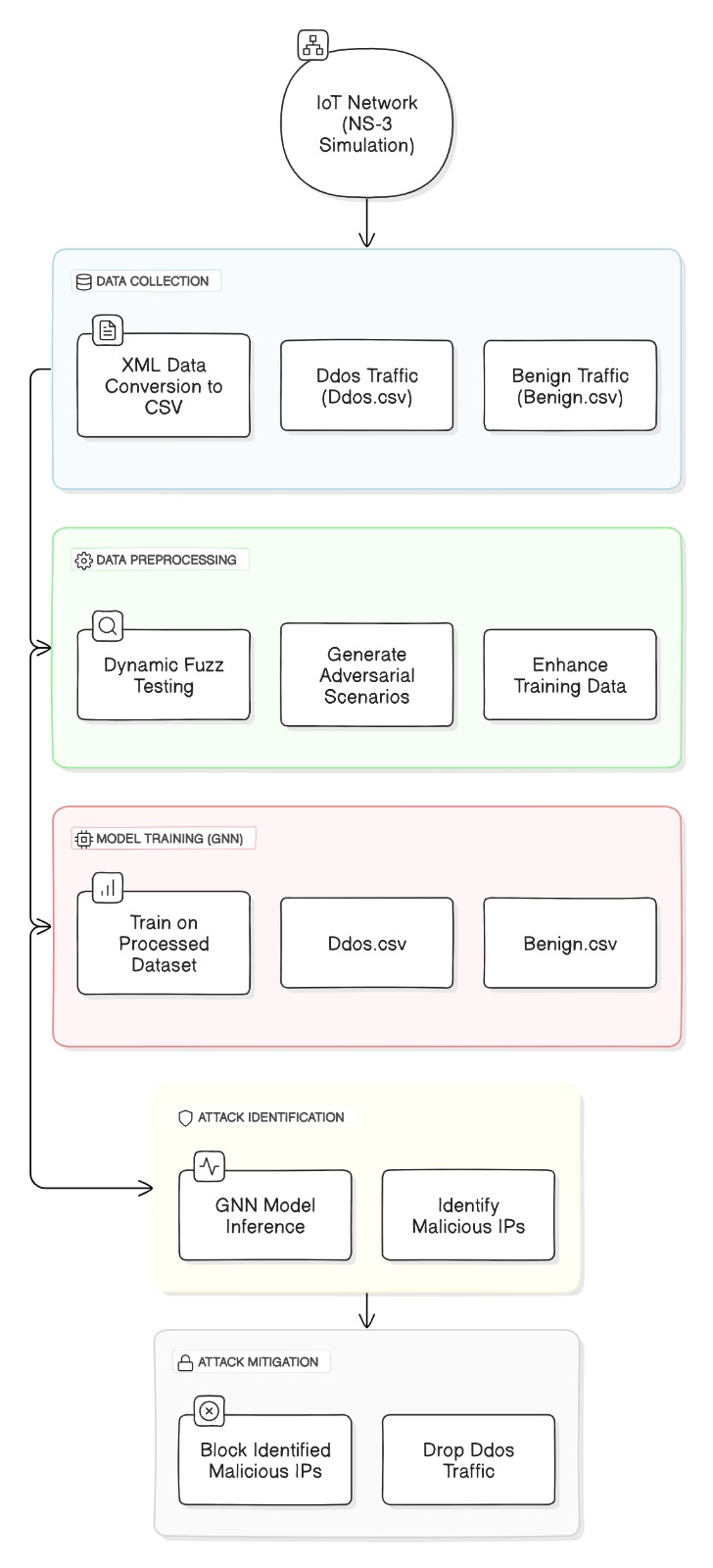
1. Modify the existing NS-3 environment to interface with the GNN model.
2. Train the GNN model using IoT traffic data to detect anomalies such as DDoS attacks.
3. Implement real-time traffic analysis through the model to monitor for malicious activity.

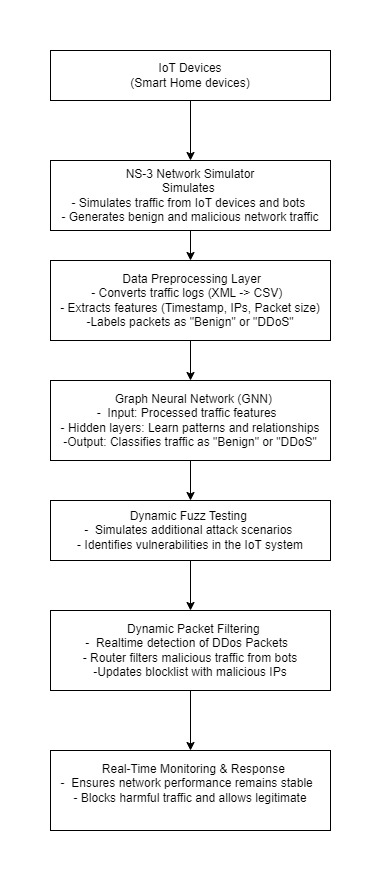
* **DDoS Mitigation Strategy:**
  1. Employ dynamic packet filtering to block malicious IP addresses.
  2. Ensure minimal impact on legitimate traffic by optimizing the filtering mechanism.
  3. Monitor network metrics (latency, throughput) during mitigation.
* **Features:**
* **Integration of GNN with NS-3:**
  + Establish communication between NS-3 and the trained GNN model.
  + Facilitate real-time traffic analysis during simulation runs.
* **Dynamic Packet Filtering:**
  + Real-time detection and packet drop for malicious IP addresses.
  + Monitor and optimize the performance of the packet-filtering mechanism.
* **Monitoring Network Performance:**
  + Measure throughput, latency, and other performance indicators to ensure network stability.
  + **Roles & Authorization Matrix:**

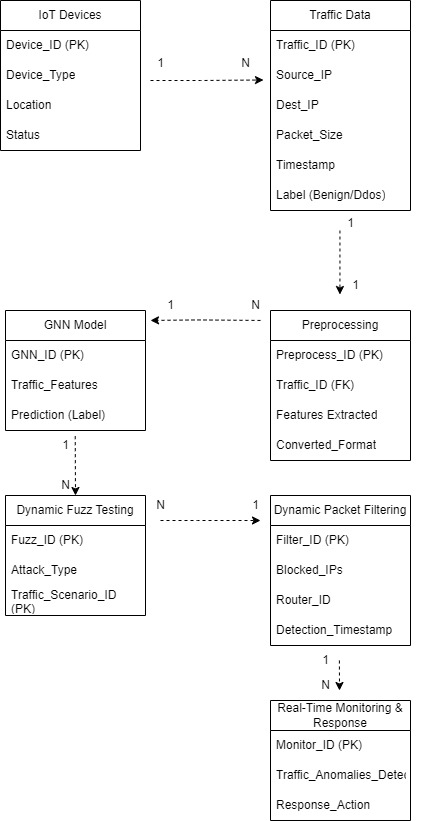
|  |  |
| --- | --- |
| **Role** | **Access Level** |
| **Security Engineer** | Full access to configure real-time detection and mitigation. |
| **Network Administrator** | Monitoring access to ensure network security is maintained. |
| **Researcher** | Access to performance data and logs for testing purposes. |

* **Assumptions:**
* The NS-3 simulation environment is stable and configured for IoT simulations.
* The GNN model has been trained with relevant datasets (including benign and DDoS traffic).
* Packet filtering libraries and dependencies are compatible with NS-3.
* **Effort Estimation:**
* **GNN Model Integration with NS-3:** 4 days
* **Packet Filtering Mechanism Implementation:** 4 days
* **Testing & Validation:** 7 days
* **Documentation:** 1 day
* **Total:** 16 days
* **Acceptance Criteria:**
* Successful integration of the GNN model with NS-3.
* Real-time detection of DDoS attacks and mitigation through packet filtering.
* The network performance remains stable with legitimate traffic unaffected.
* Full documentation of the real-time mitigation strategy and test results.
* **Checklist:**
* GNN model integrated with NS-3.
* Real-time DDoS detection implemented.
* Packet filtering for malicious traffic configured and operational.
* Network performance metrics logged and analysed.
* Documentation of results and findings completed.

1. **Architecture Document**
   * **Architecture Diagram:**

****

* + **Scheme Diagram:**
  + **E-R Diagram:**

****

1. **Sprint Retrospective Document**

****