**CHAPTER 3**

**SPRINT PLANNING AND EXECUTION METHODOLOGY**

**3.1 SPRINT I**

**3.1.1 Objective of User Story of Sprint I**

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.

**3.1.2 Functional Document**

**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.

**Authorization Matrix**

|  |  |
| --- | --- |
| **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. |

**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.

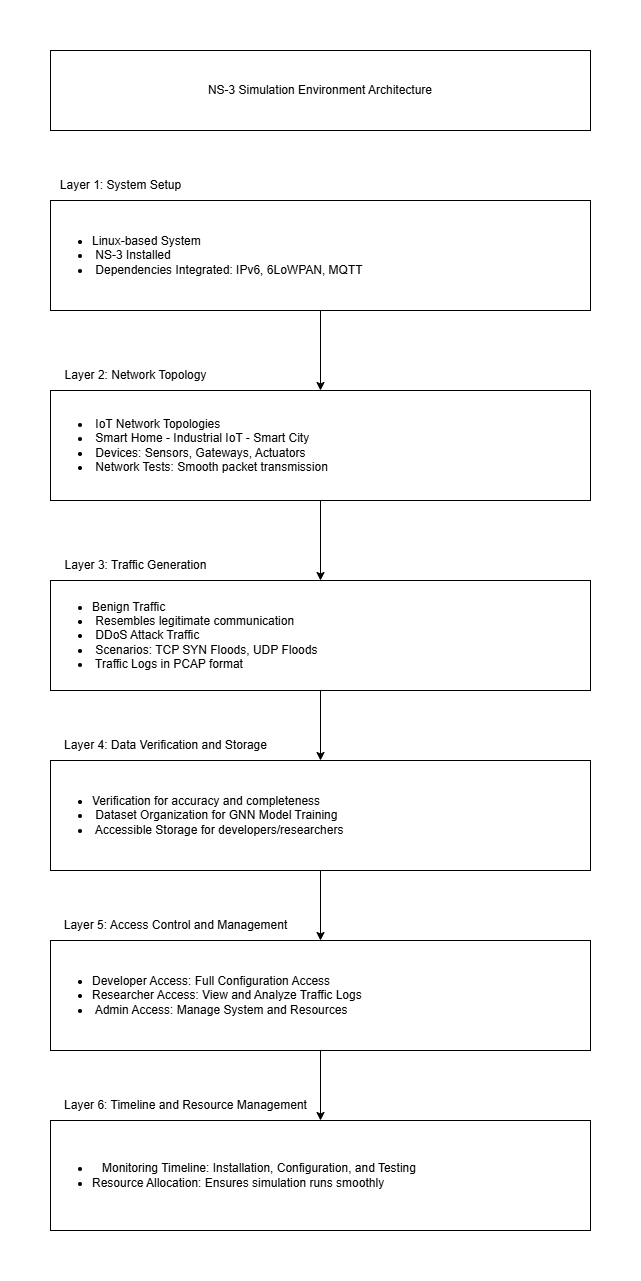
**Acceptance Criteria**

* 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.

**3.1.3 Architecture Diagram**



**Fig. 3.1 Sprint I Architecture Diagram**

**3.1.4 Outcome of Objectives/Result**

**Successful Installation and Configuration of NS-3**

* NS-3 is installed on a Linux-based system and configured correctly.
* All necessary dependencies and modules for IoT simulations are integrated without errors (e.g., integration of IPv6, 6LoWPAN, MQTT protocols, etc.).
* Compatibility between the NS-3 version and the hardware/software environment is validated to ensure a stable setup.

**Implementation of IoT Network Topologies**

* Multiple network topologies representing real-world IoT environments (e.g., smart home, industrial IoT, or smart city setups) are designed and implemented.
* Simulation of specific network devices, such as sensors, gateways, and actuators, is achieved to mirror real IoT systems.
* The topologies are tested to ensure smooth packet transmission under normal conditions.

**Generation of Benign and DDoS Attack Traffic Logs**

* Simulations generate benign traffic resembling legitimate communication within the IoT networks.
* DDoS attack scenarios are simulated (e.g., TCP SYN Floods, UDP Floods) to produce realistic attack traffic.
* All traffic logs are captured and stored in a format that is suitable for further analysis and training of AI models (e.g., PCAP format).

**Verified Data Logs for Model Training and Evaluation**

* The traffic logs generated are verified for accuracy and completeness. This ensures that both benign and malicious traffic patterns are included.
* The datasets meet the requirements for training and validating the Graph Neural Network (GNN) in subsequent stages.
* Logs are organized and stored systematically for ease of access by developers and researchers.

**Fulfilment of Access and Authorization Requirements**

* The developer has full access to configure and run simulations within the NS-3 environment.
* Researchers have limited access to only view and analyse the generated traffic logs.
* Admins retain control over the overall system, managing the environment, access control, and resources.

**Timeline and Resource Management**

* The entire setup, including installation, configuration, network design, and simulation, is completed within the estimated 3 days to 1 week window.
* Hardware and software resources were sufficient, ensuring the simulation environment ran smoothly without delays or interruptions.

**Acceptance Criteria Met**

* NS-3 was successfully installed and configured with all necessary libraries and dependencies.
* IoT network topologies were implemented, and simulations ran without errors.
* Traffic logs (benign and attack data) were generated successfully and are ready for use in AI model training and testing.

**Conclusion**

The NS-3 simulation environment is now fully operational and meets all functional requirements outlined in the user story. The generated traffic logs, including benign and DDoS data, are available for use in the next steps of the project—training and validating the AI-driven dynamic fuzz testing framework with the Graph Neural Network (GNN) model.

**3.1.5 Sprint Retrospective**

|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| *Share aspects of the sprint that you enjoyed or found particularly effective.* | *Discuss lessons learned, whether they are related to processes, technical aspects, or teamwork.* | *Identify areas where the team felt a lack of resources, support, or information.* | *Discuss any desires or expectations that the team had but were not met during the sprint.* |
| Successfully set up the NS3 environment without any major errors. | Learned the nuances of configuring an IoT network in NS3. | Lacked sufficient examples for simulating complex IoT devices. | Desired more efficient methods for configuring and simulating diverse IoT environments. |
| Collaboration between network engineers and data scientists led to efficient environment configuration. | Gained insights into how network simulations can generate valuable data for GNN model training. | Missing support for advanced network configurations out-of-the-box in NS3. | Wished for a more integrated system for logging and analysing simulation data. |
| The initial IoT network topology was established smoothly. | Discovered best practices for organizing simulation files and settings. | Faced delays due to a lack of clear guidelines for generating XML traffic logs. | Hoped for additional modules in NS3 for simulating real-time network behaviour. |
| Realistic traffic generation was accurate as per simulation requirements. | Enhanced knowledge on the limitations of default NS3 modules and the need for customization. | Insufficient time was allocated for testing the simulation setup under various scenarios. | Longed for more structured sprint planning and resource allocation to avoid last-minute rushes. |
| Detailed documentation was well-structured and comprehensive. | Understood the importance of proper testing procedures in simulation environments. | More powerful computing resources would have made simulation faster. | Desired quicker feedback from the testing phase, as it took longer than anticipated. |

**3.1 SPRINT II**

**3.2.1 Objectives with user stories of sprint II**

The objective of this user story is to create a labelled dataset for GNN model training by generating IoT traffic data through NS-3 simulations. This dataset will include both benign and DDoS attack traffic, forming a core component for the AI-driven security framework, which detects and mitigates DDoS attacks in IoT networks.

**3.2.2 Functional Document**

**Product Goal**

The goal is to create a labelled and balanced dataset through NS-3 simulations, incorporating both benign and DDoS attack traffic. This dataset will be crucial for training the GNN model, allowing it to effectively identify and mitigate DDoS attacks in IoT environments.

**Demography (Users Location)**

* Target Users: AI developers, security analysts, researchers.
* User Characteristics: Individuals with experience in AI model training, network security, and traffic analysis.
* Location: Global, with a focus on academic and research institutions.

**Business Processes**

* Data Collection:
  + Run NS-3 network simulations to generate diverse traffic patterns.
  + Capture network traffic logs in XML format.
* Data Processing:
  + Convert XML logs to CSV for ease of analysis and processing.
  + Label the dataset entries as either benign or DDoS based on traffic type.
* Data Balancing:
  + Ensure equal representation of benign and DDoS entries in the dataset to facilitate unbiased GNN model training.

**Features**

* Traffic Simulation in NS-3:
  + Set up and execute IoT traffic simulations.
  + Capture traffic logs for both benign and DDoS attack scenarios.
* Data Conversion and Labelling:
  + Convert XML logs to CSV format for improved accessibility.
  + Label data entries as benign or DDoS based on predefined criteria.

**Authorization Matrix**

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

.

**Assumptions**

* NS-3 simulations run successfully without errors.
* The XML to CSV conversion script is functional and accurate.
* Labelling criteria for benign and DDoS traffic are well-defined and consistently applied.

**Target Audience**

* Audience: Data Scientists, AI Developers, Researchers.
* Effort Estimation: Approximately 1 week for complete dataset generation and processing.

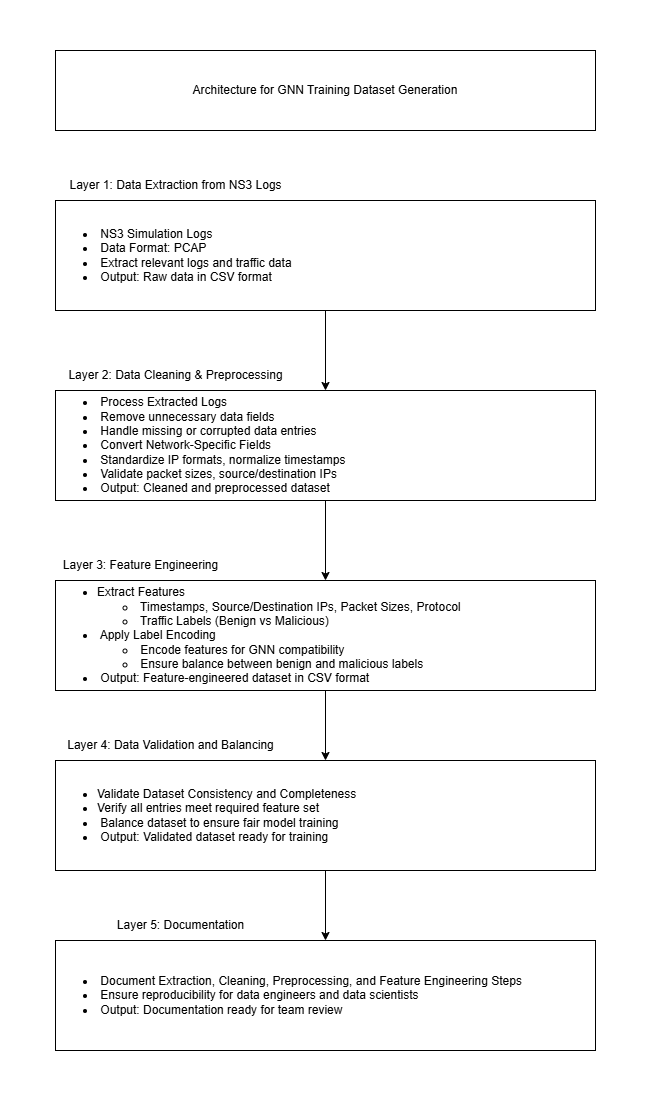
**Acceptance Criteria**

* Simulation data is successfully captured and logged.
* XML logs are converted to CSV format without errors.
* Dataset entries are accurately labelled as benign or DDoS traffic.
* The dataset is balanced and ready for GNN model training.

**Checklist**

* Generate traffic data through NS-3 simulations.
* Convert XML logs to CSV format.
* Label data entries correctly as benign or DDoS.
* Review dataset for balance and accuracy.

**3.2.3 Architecture Document**



**Fig. 3.2 Sprint II Architecture Diagram**

**3.2.4 Outcome of Objectives/Result**

**Generated Dataset**

* A labelled dataset is created with a balanced representation of benign and DDoS traffic.

**XML-to-CSV Conversion**

* XML logs from NS-3 simulations are successfully converted to CSV format.

**Data Labelling Accuracy**

* Entries are accurately labelled as benign or DDoS traffic.

**Balanced Dataset**

* Dataset meets the 1:1 ratio of benign to DDoS traffic, ready for GNN model training.

**3.2.5 Sprint Retrospective**

|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| *Share aspects of the sprint that you enjoyed or found particularly effective.* | *Discuss lessons learned, whether they are related to processes, technical aspects, or teamwork.* | *Identify areas where the team felt a lack of resources, support, or information.* | *Discuss any desires or expectations that the team had but were not met during the sprint.* |
| The dataset was successfully extracted and processed for model training. | Gained experience in transforming raw simulation data into useful training datasets. | Lack of real-world IoT traffic patterns limited the diversity of the dataset. | Wanted more detailed simulation logs with additional network parameters. |
| Collaboration between network engineers and data scientists improved data quality. | Understood the importance of balancing datasets to avoid model bias. | Insufficient feature documentation slowed down the feature engineering process. | Desired automated tools to expedite data extraction and cleaning processes. |
| Feature engineering helped in deriving relevant insights from the simulation logs. | Learned how to extract relevant features (e.g., timestamps, packet sizes) for GNN training. | Limited access to automated tools for dataset balancing. | Hoped for easier integration of external data sources for richer training datasets. |
| Preprocessing steps ensured that the dataset was well-balanced and usable. | Realized the necessity of ensuring dataset consistency for effective model performance. | Lacked predefined templates for preprocessing and feature extraction. | Wished for more comprehensive test datasets to check the feature quality. |
| Documentation of the data extraction and preprocessing steps was clear and concise. | Explored techniques for handling missing data in network traffic logs. | More team communication was needed during the dataset validation process. | Desired quicker feedback cycles from the data validation phase to avoid bottlenecks. |

**3.1 SPRINT III**

**3.3.1 Objective of User Story of Sprint III**

The objective of this user story is to develop and train a Graph Neural Network (GNN) model capable of detecting DDoS attacks in IoT network traffic. The GNN model will learn to differentiate between benign and malicious traffic patterns, contributing to real-time DDoS detection and mitigation within IoT networks.

**3.3.2 Functional Document**

**Product Goal**

The goal is to train and validate a GNN model using a labelled dataset derived from IoT network simulations. The model will focus on identifying DDoS attacks with high accuracy, leveraging dynamic traffic features to support real-time IoT security frameworks.

**Demography (Users and Locations)**

* Target Users: Data scientists, cybersecurity analysts, AI researchers.
* User Characteristics: Skilled in network security, AI modelling, and GNN architecture.
* Location: Global, intended for research institutions and cybersecurity teams.

**Business Processes**

* Model Architecture Design:
  + Define GNN architecture to accommodate input features from IoT network data.
  + Configure model layers to detect traffic anomalies.
* Model Training:
  + Use the pre-processed dataset, splitting it into training, validation, and testing sets.
  + Train the model using supervised learning techniques to classify benign and DDoS traffic.
* Model Testing and Saving:
  + Evaluate the model’s performance on a validation dataset to ensure a minimum accuracy of 75%.
  + Save the trained model for future deployment and testing.

**Features**

* Model Training and Evaluation:
  + Train and validate the GNN model using labelled IoT network traffic data.
  + Perform cross-validation to ensure robustness.
* Hyperparameter Optimization:
  + Tune parameters such as learning rate, number of epochs, hidden layers, batch size, optimizer, weight initialization, regularization, activation functions, and loss function to maximize model performance.
* Model Saving:
  + Save the final trained model, preparing it for deployment in real-time environments.

**Authorization Matrix**

|  |  |
| --- | --- |
| **ROLE** | **Access Level** |
| Data Scientist | Full access to model training and hyperparameter tuning |
| Analyst | Access to the trained model and outputs for threat analysis |
| Admin | Full access to system resources and documentation |

**Assumptions**

* Dataset is pre-processed and labelled for benign and DDoS traffic scenarios.
* Adequate computational resources are available to support GNN training.
* Metrics for evaluating model performance (accuracy, precision, recall) are pre-defined.

**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

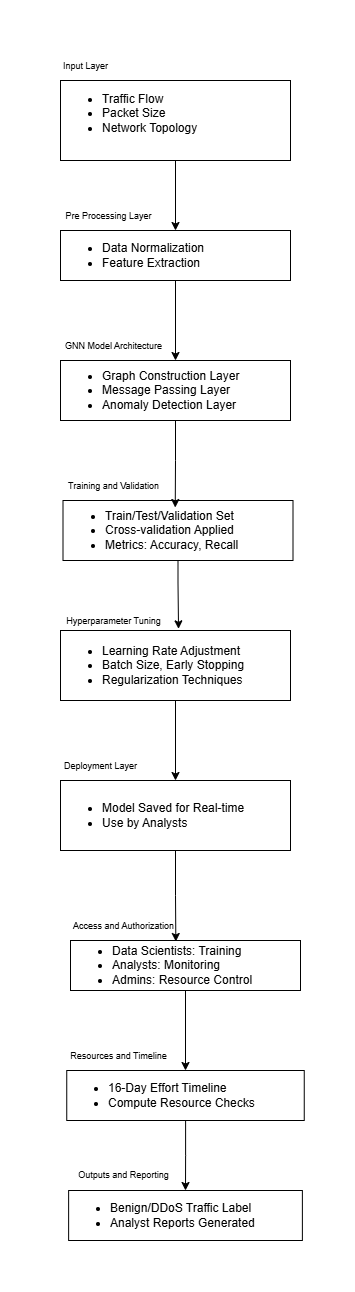
**Acceptance Criteria**

* The GNN model achieves a minimum accuracy of 75% in DDoS detection.
* Hyperparameters are optimized to enhance performance.
* Model accurately differentiates between benign and DDoS traffic.
* Training procedures are documented, and the model is saved for deployment.

**Checklist**

* Design and implement the model architecture.
* Ensure the dataset is pre-processed and ready for training.
* Train and validate the GNN model.
* Tune hyperparameters for optimal detection performance.
* Save the model for deployment.
* Complete documentation.

**3.3.3 Architecture Document**



**Fig. 3.3 Sprint III Architecture Diagram**

**3.3.4 Outcome of Objectives/Result**

**Model Architecture Design:**

* A GNN model architecture tailored for DDoS detection is designed and implemented successfully.

**Model Training and Validation:**

* GNN model is trained on labelled IoT network traffic data and validated, achieving over 75% accuracy.

**Hyperparameter Tuning:**

* Optimal hyperparameters are selected, ensuring robust model performance in differentiating DDoS and benign traffic.

**Model Saving:**

* The final trained model is saved, ready for integration into real-time IoT security applications.

**3.3.5 Sprint Retrospective**

|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| Share aspects of the sprint that you enjoyed or found particularly effective. | Discuss lessons learned, whether they are related to processes, technical aspects, or teamwork. | Identify areas where the team felt a lack of resources, support, or information. | Discuss any desires or expectations that the team had but were not met during the sprint. |
| The model training process was smooth, and early results were promising. | Understood the impact of hyperparameters on GNN performance. | Lacked real-time evaluation during the model testing phase. | Wanted faster results from hyperparameter tuning using better computational resources. |
| Team collaboration improved during hyperparameter tuning efforts. | Learned techniques to fine-tune the model for different network traffic patterns. | Limited computational power made the hyperparameter tuning slow. | Desired real-time traffic to test the model on live data. |
| Reached the target accuracy of 75% on the validation set. | Gained experience in handling large datasets during model training. | Faced challenges in finding optimal learning rates and other parameters. | Hoped for a more intuitive visualization of model performance over time. |
| The GNN model was able to classify DDoS traffic effectively. | Explored how GNN architectures can be customized for IoT traffic analysis. | Needed more test data with various DDoS attack patterns for robust training. | Wished for better tools to automate model performance monitoring. |
| Good progress was made in documenting model architecture and training procedures. | Realized the importance of validation in reducing overfitting during training. | Lack of comprehensive documentation on hyperparameter tuning strategies. | Desired quicker model validation feedback to avoid prolonged tuning cycles. |

**3.4 SPRINT IV**

**3.4.1 Objective of User Story of Sprint IV**

The objective of this user story is to integrate the GNN model with the NS-3 simulation environment, enabling real-time detection and mitigation of DDoS attacks in IoT networks. By using dynamic packet filtering, this integration aims to secure the network by dropping malicious traffic while preserving the flow of legitimate data.

**3.4.2 Functional Document**

**Product Goal**

The goal is to enhance the NS-3 simulation environment by integrating it with the GNN model for real-time DDoS detection and mitigation. This setup will allow IoT networks to be monitored and protected dynamically, ensuring legitimate traffic flows uninterrupted while filtering out malicious traffic.

**Demography (Target Audience)**

* Target Users: Security Engineers, Network Administrators, Researchers.
* User Characteristics: Experienced in real-time threat detection, network management, and dynamic IoT security research.

**Business Processes**

* GNN Model Integration with NS-3:
  + Modify the NS-3 environment to communicate with the trained GNN model.
  + Configure the GNN model to analyse network traffic for DDoS detection.
  + Implement real-time traffic analysis for ongoing monitoring and anomaly detection.
* DDoS Mitigation Strategy:
  + Apply dynamic packet filtering to block malicious IP addresses.
  + Optimize the filtering mechanism to minimize the impact on legitimate traffic.
  + Monitor key network metrics (latency, throughput) to ensure stable performance during mitigation.

**Features**

* Integration of GNN with NS-3:
  + Enable real-time communication between NS-3 and the GNN model.
  + Allow continuous traffic analysis during simulations.
* Dynamic Packet Filtering:
  + Detect and drop packets from malicious IPs in real time.
  + Continuously monitor and optimize the packet-filtering mechanism’s performance.
* Monitoring Network Performance:
  + Measure and log throughput, latency, and other indicators to ensure network stability during DDoS mitigation.

**Roles & Authorization Matrix:**

|  |  |
| --- | --- |
| **ROLE** | **Access Level** |
| Security Engineer | Full access to configure real-time detection and mitigation |
| Network Administrator | Monitoring access to validate and ensure network security |
| Researcher | Access to performance data and logs for analysis and testing |

**Assumptions**

* The NS-3 environment is stable and configured for IoT simulations.
* The GNN model is pre-trained with a relevant dataset (including benign and DDoS traffic).
* Required 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

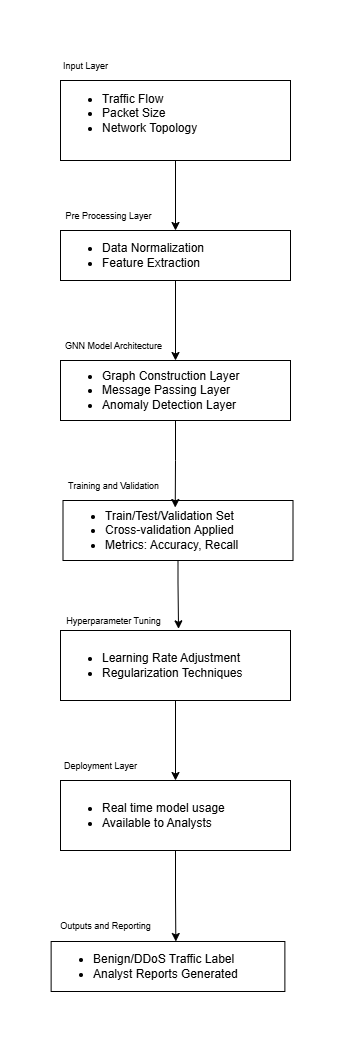
**Acceptance Criteria**

* The GNN model is successfully integrated with NS-3.
* Real-time detection and mitigation of DDoS attacks via packet filtering are functional.
* Network performance remains stable, with legitimate traffic unaffected.
* Documentation of the real-time mitigation strategy and test results is complete.

**Checklist**

* GNN model integrated with NS-3.
* Real-time DDoS detection and mitigation implemented.
* Packet filtering mechanism for malicious traffic is operational.
* Network performance metrics logged and analysed.
* Documentation of results and findings is completed.

**3.4.3 Architecture Document**



**Fig. 3.4 Sprint IV Architecture Diagram**

**3.4.4 Outcome of Objectives/Result**

**GNN Model Integration with NS-3:**

* The GNN model is successfully integrated with NS-3, allowing real-time traffic analysis and DDoS detection.

**Dynamic Packet Filtering Mechanism:**

* The packet filtering mechanism is implemented, effectively blocking malicious IPs while preserving legitimate network traffic.

**Network Performance Monitoring:**

* Throughput, latency, and other network metrics are logged and analysed, ensuring that network stability is maintained throughout DDoS mitigation.

**Documentation and Testing:**

* Comprehensive documentation of the mitigation strategy, testing procedures, and performance results is completed.

**3.4.5 Sprint Retrospective**

|  |  |  |  |
| --- | --- | --- | --- |
| **Liked** | **Learned** | **Lacked** | **Longed For** |
| Share aspects of the sprint that you enjoyed or found particularly effective. | Discuss lessons learned, whether they are related to processes, technical aspects, or teamwork. | Identify areas where the team felt a lack of resources, support, or information. | Discuss any desires or expectations that the team had but were not met during the sprint. |
| Successfully integrated the GNN model with NS3 for real-time mitigation. | Learned how to integrate a GNN model within a network simulation environment. | Lacked real-time logging tools to monitor the mitigation process more effectively. | Desired quicker ways to simulate different types of DDoS attacks in NS3. |
| The packet filtering mechanism worked as expected to block malicious traffic. | Gained insights into real-time packet filtering and its effects on network performance. | Required more comprehensive test cases to validate the mitigation strategy under varied conditions. | Wished for more advanced visualization tools to monitor traffic in real-time. |
| Team communication was efficient during the integration and testing phases. | Understood the importance of balancing security measures with network throughput. | Lacked sufficient documentation on integrating machine learning models in NS3. | Hoped for seamless integration of the mitigation strategy into live network environments. |
| Network performance was monitored closely, and legitimate traffic was unaffected. | Learned how to implement dynamic filtering based on the model’s predictions. | Faced delays due to insufficient knowledge about real-time packet filtering techniques. | Wanted more advanced packet filtering options that are easily configurable. |
| Clear documentation of the mitigation strategy helped in replicating the process. | Realized the challenges of maintaining performance while mitigating attacks. | Required more scenarios to fully test the GNN model’s effectiveness in diverse traffic conditions. | Desired more real-world IoT traffic data for more accurate mitigation testing. |