Sprint-wise Retrospective

AI - Driven Fuzz Testing for IoT Security

Panel No. 06
Supervisor Name
Dr. Balaji Srikaanth P, AP/NWC
Dr. S. Nagendra Prabhu, AP/CINTEL

Batch No. NW000156
Shaurya Singh Srinet – RA2111032010006
Shounak Chandra – RA2111032010026
Charvi Jain – RA2111047010113

Product Category: Research

Sprint 1 : Setup NS3 Simulation Environment			
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 analyzing 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 behavior.
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.

Sprint 2 : Generate Dataset for GNN Training			
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.

Sprint 3 : Train GNN Model for DDoS Detection			
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.

Sprint 4 : Implement Real-Time DDoS Mitigation in NS3			
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.