**Project ID :**

24-25J-120

1. Topic (12 words max)

SDN-based Intelligent Intrusion Detection System (IIDS) using Machine Learning

1. Research group the project belongs to

**Computing Infrastructure and Security (CIS)**

1. Research area the project belongs to

**Cyber Security (CS)**

1. If a continuation of a previous project:

|  |  |
| --- | --- |
| Project ID |  |
| Year |  |

1. Brief description of the research problem including references (200 – 500 words max) – references not included in word count.

The growing complexity and scale of modern networks have made traditional intrusion detection systems (IDS) increasingly inadequate in addressing advanced cybersecurity threats. Conventional IDS are often static, unable to adapt quickly to new and sophisticated attack patterns and can be overwhelmed by the massive volume of network traffic. The integration of Software-Defined Networking (SDN) provides a promising solution by centralizing control and enabling dynamic network management. However, there is a need for an intelligent, adaptive, and automated system that leverages SDN to enhance real-time intrusion detection and response capabilities. The research problem focuses on developing an SDN-based Intelligent Intrusion Detection System (IIDS) using machine learning to address these challenges by providing real-time, adaptive, and automated security management.

1. Brief description of the nature of the solution including a conceptual diagram (250 words max)

The proposed solution involves the development of an SDN-based Intelligent Intrusion Detection System (IIDS) that integrates machine learning for advanced threat detection and adaptive security policy enforcement. SDN-based Cybersecurity Information Collection and Management involves designing and developing a system for centralized and dynamic collection of cybersecurity-related information using SDN. It will integrate with network devices, sensors, and logs to enable real-time data collection and processing. SDN-based Cybersecurity Action and Response focuses on developing mechanisms to translate SDN outputs into actionable security responses, such as blocking malicious traffic or reconfiguring network paths. It aims to automate response strategies based on predefined security policies. Machine Learning-based Intrusion Detection Engine utilizes advanced machine learning algorithms to detect anomalies and potential threats in real-time. It involves data collection, preprocessing, model development, and integration with the SDN controller for continuous monitoring and analysis of network traffic. Adaptive Security Policy Enforcement Module develops a dynamic policy enforcement engine that adjusts security policies in real-time based on detected threats and network conditions. It ensures seamless integration with the SDN controller and the intrusion detection engine to provide a integrated and responsive security framework.

1. Brief description of specialized domain expertise, knowledge, and data requirements (300 words max)

The development of the SDN-based Intelligent Intrusion Detection System (IIDS) requires specialized expertise and knowledge in several domains: Software-Defined Networking (SDN): Understanding the principles, architecture, and operation of SDN, including SDN controllers, protocols, and network virtualization. Cybersecurity: In-depth knowledge of cybersecurity principles, threat landscapes, attack vectors, and defense mechanisms, particularly in network security. Machine Learning: Proficiency in developing and applying machine learning models for anomaly detection and pattern recognition. Network Traffic Analysis: Expertise in capturing, preprocessing, and analyzing network traffic data to identify features relevant to intrusion detection. System Integration and Development: Skills in integrating various modules and components, ensuring seamless communication and compatibility between the SDN controller, intrusion detection engine, and policy enforcement module. Performance Optimization: Ability to optimize algorithms and systems for real-time processing, high performance, and scalability.

Data Requirements- Network Traffic Data: Extensive datasets of network traffic, both normal and malicious, for training and testing machine learning models. Cybersecurity Threat Intelligence: Access to threat intelligence feeds and databases to update and refine detection models and security policies. System Logs and Event Data: Logs from network devices, servers, and security appliances to provide comprehensive visibility into network activities and potential threats. Simulated Attack Scenarios: Synthetic data representing different types of cyberattacks for testing the system's detection and response capabilities.

1. Objectives and Novelty

|  |  |  |  |
| --- | --- | --- | --- |
| Main Objective  The main objective of the SDN-based Intelligent Intrusion Detection System (IIDS) is to enhance real-time cybersecurity through a unified, adaptive, and automated approach. It aims to establish a centralized system for the dynamic collection and management of cybersecurity data using SDN, providing comprehensive network visibility, focuses on developing an automated response mechanism that utilizes SDN outputs to enforce real-time security actions, such as traffic blocking and network reconfiguration, leverages advanced machine learning models for real-time intrusion detection, integrating with the SDN controller to continuously monitor and analyze network traffic for anomalies and threats. Lastly aims to implement an adaptive policy enforcement module that dynamically adjusts security policies in real-time, based on ongoing threat intelligence and network conditions, to maintain robust network security. | | | |
| Member Name | Sub Objective | Tasks | Novelty |
| Parthika.K | SDN-based Cybersecurity Information Collection and Management | 1. **Literature Review and Requirement Analysis**   Conduct a comprehensive literature review on the use of SDN in cybersecurity.  Identify specific requirements for collecting and managing cybersecurity-related information using SDN.   1. **Design and Architecture Development**   Design the architecture for cybersecurity information collection and management using SDN.  Define the interaction between the SDN controller and various data sources (network devices, sensors, logs).   1. **Development and Integration**   Develop modules for collecting and managing cybersecurity-related information.  Integrate these modules with the SDN controller to enable real-time data collection and processing.   1. **Testing and Optimization**   Test the information collection and management system in a simulated environment.  Optimize the system for performance, reliability, and security   1. **Documentation and Reporting**   Document the development process, challenges, and solutions.  Prepare detailed reports on the system’s performance and impact on cybersecurity data management | Leveraging SDN for centralized and dynamic collection of cybersecurity-related information.  Enhanced real-time data management capabilities to support advanced security analytics and decision-making |
| Satkurulingam.S | SDN-based Cybersecurity Action and Response | 1. **Requirement Analysis and Design**   Analyze requirements for utilizing SDN outputs to take cybersecurity actions and responses.  Design the architecture for a system that uses SDN outputs to trigger security actions and responses.   1. **Development of Response Mechanisms**   Develop mechanisms for translating SDN outputs into actionable security responses (e.g., blocking traffic, reconfiguring network paths).  Implement automated response strategies based on predefined security policies.   1. **Integration and Communication**   Integrate response mechanisms with the SDN controller and other security components.  Ensure seamless communication and coordination between SDN outputs and security actions.   1. **Testing and Optimization**   Test the response mechanisms in various attack scenarios to evaluate effectiveness.  Optimize the system for quick and accurate response actions.   1. **Documentation and Reporting**   Document the development process and performance of the response mechanisms.  Prepare detailed reports on the system’s effectiveness and impact on cybersecurity. | Development of automated response mechanisms leveraging SDN outputs for dynamic and real-time threat mitigation.  Integration of SDN-based actions with existing security infrastructure to enhance overall network security posture. |
| Sriskandarajah J.P | Develop Machine Learning based Intrusion Detection Engine | 1. **Data collection and preprocessing**   Gather extensive network traffic data from reliable sources. Preprocessing the data include cleaning it to remove the noise, handling missing values, and normalizing features to ensure consistency. Ensure that the dataset is in an optimal format for training machine learning models, enhance their performance and reliability.   1. **Develop machine learning model**   Select the appropriate algorithms for learning, train using the preprocessed dataset where they learn to distinguish between normal and malicious network traffic based on the extracted features, develop models that not only achieve high accuracy but also generalize well to unseen data by effectively identifying intrusions in real-world network environments   1. **Integrate the trained model with SDN controller**   use the machine learning models to continuously monitor and inspect traffic for anomalies and potential threats. ensure that the intrusion detection system can immediately identify and respond to security incidents, leveraging the agility and centralized control of the SDN architecture to enhance overall network security.   1. **Evaluate and optimize the model**   test the models on separate validation and test datasets to assess their accuracy and recall. analyze to identify any areas for improvement using performance metrics. enhance the model’s performance using optimization techniques. Test the robustness and reliability of the system by exposing it to various attack scenarios. | Real time intrusion detection in SDN environment  By integrating machine learning models directly with the SDN controller, the system can dynamically and continuously analyze network traffic, detect anomalies, and respond to threats in real-time. This approach significantly improves traditional intrusion detection systems by offering enhanced visibility, centralized control, and rapid adaptability to new and evolving threats. The integration of SDN's centralized management capabilities with sophisticated machine learning algorithms provides a robust and efficient solution for maintaining network security through continuous monitoring and adaptive policy enforcement. |
| Dassanayake E. D. | Adaptive Security Policy  Enforcement Module | * **Requirement Analysis and Design**   **o Analyze Requirements:**   * Perform a detailed analysis of current security policy   enforcement methods in SDN environments.   * Identify requirements for   dynamic, real-time policy  adjustments.   * Determine the specific cybersecurity threats and   network conditions that  will trigger policy changes.   * **Design Architecture:** * Design a robust architecture for the adaptive policy enforcement module. * Define the interaction between the policy module, SDN controller, and intrusion detection engine. * Ensure the architecture supports real-time data processing and policy updates. * **Development of Policy Engine**   **o Develop Core Engine:**   * Develop the core engine of the adaptive policy enforcement module. * Implement algorithms for dynamic policy adjustments based on detected threats and real-time network conditions. * **Implement Policy Adjustment Mechanisms:** * Create mechanisms to allow real-time updates of security policies. * Ensure policies can be modified, added, or removed without disrupting network operations. * **Integration and Communication** * **Integrate with SDN Controller:** * Integrate the policy enforcement module with the SDN controller to enable seamless communication. * Ensure the policy engine can receive real-time data from the SDN controller and the intrusion detection engine. * **Ensure Real-time Policy Enforcement:** * Implement communication protocols to ensure the policy engine can enforce policies in real-time. * Validate the integration with test data to ensure accuracy and reliability. * **Testing and Optimization** * **Test in Simulated Environment:** * Conduct extensive testing of the policy engine in various attack scenarios. * Evaluate the effectiveness of dynamic policy adjustments in mitigating detected threats. * **Optimize Performance:** * Identify and resolve any performance bottlenecks in the policy engine. * Optimize algorithms for faster response times and more accurate policy enforcement. * Ensure the module can handle high traffic volumes and complex threat scenarios without degradation in performance. * **Documentation and Reporting** * **Document Development Process**: * Maintain detailed documentation throughout the development and testing phases. * Include descriptions of the architecture, algorithms, and integration processes. * **Prepare Reports:** * Compile comprehensive reports on the effectiveness and impact of the adaptive policy enforcement module. * Include performance metrics, case studies from testing scenarios, and recommendations for future improvements. | **Real-time Adaptation:**  Development of an adaptive policy enforcement module that can dynamically adjust security policies in real time based on continuous threat intelligence and changing network conditions.  **Enhanced Security Response:**  Implementation of advanced algorithms and mechanisms to ensure that the SDN environment can quickly and accurately respond to emerging threats.  **Seamless Integration:**  Integration with the SDN controller and intrusion detection engine to provide a cohesive and responsive security framework.  **Comprehensive Testing and Optimization:**  Extensive testing in simulated environments to ensure the module’s effectiveness and robustness, followed by optimization to handle real-world network conditions. |

1. Supervisor checklist
2. Does the chosen research topic possess a comprehensive scope suitable for a final-year project?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes |  | No |  |

1. Does the proposed topic exhibit novelty?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes |  | No |  |

1. Do you believe they have the capability to successfully execute the proposed project?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes |  | No |  |

1. Do the proposed sub-objectives reflect the students' areas of specialization?

|  |  |  |  |
| --- | --- | --- | --- |
| Yes |  | No |  |

1. Supervisor's Evaluation and Recommendation for the Research topic:
2. Supervisor details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Title | First Name | Last Name | Signature |
| Supervisor |  |  |  |  |
| Co-Supervisor |  |  |  |  |
| External Supervisor |  |  |  |  |
| Summary of external supervisor’s (if any) experience and expertise | | | | |

**This part is to be filled by the Topic Screening Panel members.**

Acceptable: Mark/Select as necessary

|  |  |
| --- | --- |
| Topic Assessment Accepted |  |
| Topic Assessment Accepted with minor changes (should be followed up by the supervisor)\* |  |
| Topic Assessment to be Resubmitted with major changes\* |  |
| Topic Assessment Rejected. Topic must be changed |  |

\* Detailed comments given below

Comments

The Review Panel Details

|  |  |
| --- | --- |
| **Member’s Name** | **Signature** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

\***Important**:

1. According to the comments given by the panel, make the necessary modifications and get the approval by the **Supervisor** or the **Same Panel**.
2. If the project topic is rejected, identify a new topic, and request the RP Team for a new topic assessment.
3. The form approved by the panel must be attached to the **Project Charter Form**.