

SDN-BASED INTELLIGENT INTRUSION DETECTION SYSTEM (IIDS) USING MACHINE LEARNING

Parthika. K

BSc (Hons) Degree in Information Technology Specialized in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology Sri Lanka

August 2024

SDN-BASED INTELLIGENT INTRUSION DETECTION SYSTEM (IIDS) USING MACHINE LEARNING

Project ID: 24-25J-120

Project Proposal Report

Parthika. K - IT20601638

Supervised by Mr. Kanishka Prajeewa Yapa

Co-supervised by Mr. Tharaniyawarma.K

BSc (Hons) Degree in Information Technology Specialized in Cyber Security

Department of Information Technology


Sri Lanka Institute of Information Technology Sri Lanka

August 2024

Declaration


We declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Additionally, we hereby grant to Sri Lanka Institute of Information Technology the nonexclusive right to reproduce and distribute my dissertation, in whole or in part, in future works (such as articles or books).


Name	Student ID	Signature
Parthika.K	IT20601638	

The supervisor should certify the proposal report with the following declaration

The above candidate is carrying out research for the undergraduate dissertation


.....
Signature of the supervisor

29/08/2024
.....
Date


.....
Signature of the co-supervisor

29/8/2024
.....
Date

Acknowledgement

I would like to express my sincere gratitude to my supervisor, Mr. Kanishka Yapa, for his invaluable guidance, support, and encouragement throughout the course of this project. His expertise and insights have been instrumental in shaping the direction and outcome of this research.

I would also like to extend my heartfelt thanks to my co-supervisor, Mr. Tharaniyawarma. K, for his continuous assistance, constructive feedback, and dedication, which have significantly contributed to the completion of this proposal.

Finally, I am grateful to my family, friends, and colleagues for their unwavering support and understanding during this time.

Abstract

In the evolving network security landscape, software-defined networking (SDN) offers a flexible and systematic way to manage complex network environments, but this paradigm shift also introduces additional vulnerabilities, internally one is the ease with which SDN turns to Flow Table Overflow attacks, resulting in dropped packets and interrupted services. This project proposes the development of an SDN-based Intrusion Detection System (IDS) specifically designed to detect and mitigate Flow Table Overflow attacks the application of machine learning techniques will analyze flow table usage and network traffic patterns to detect IDS attacks about the first signs More than that There is no damage. Through extensive testing and development, the project aims to deliver a robust security solution capable of protecting SDN environments from one of the most critical threats The results of this project will contribute to SDN design has been upgraded, ensuring its reliability in real-world applications

Key words – SDN, IDS, Flow table overflow, ML

Table of content

Table of Contents

Declaration.....	i
Acknowledgement.....	ii
Abstract	iii
Table of content	iv
List Of Figures.....	v
List Of Table.....	v
List of Abbreviations	v
1. INTRODUCTION	1
1.1. Background and Purpose.....	1
1.2. Scope	2
1.3. Literature Review	2
1.4. Research Gap.....	4
1.5. Research Problem	4
2. Objectives.....	5
3. Methodology	6
3.1. Technologies	7
4. Requirements.....	8
4.1. Functional Requirements.....	8
4.2. Non-Functional Requirements	8
4.3. System Diagram	10
4.4. Timeline	10
5. Conclusion.....	11
6. Commercialization.....	11
7. Approximate Budget Analysis	12
8. References	12

List Of Figures

Figure 1Flow table overflow attack.....	3
Figure 2 Individual system diagram	10

List Of Table

Table 1Gantt chart	v
Table 2 budget	12

List of Abbreviations

SDN	Software defined Network
IDS	Intrusion Detection System
ML	Machine Learning

1. INTRODUCTION

As the demand for more dynamic and flexible network management increases, software-defined networking (SDN) has emerged as a transformational technology, providing centralized control and systems for managing network infrastructure a complex Decoupling the control plane from the data plane, SDN network administrators configured network resources in real time s, can monitor and optimize network operations for agility and efficiency Provides significant improvements but these architectural changes also introduce additional security challenges , because centralized control becomes the main weak point.

One of the most important security concerns in SDN environments is the risk of Flow Table Overflow attacks. One of these attacks causes an adversary to flood the flow table of the SDN switch with many flow entries, exceeding its capacity and causing the legitimate traffic to be denied This not only degrades network performance but can cause service disruption there has also been a serious problem. Given the critical role of flow tables in routing network traffic, protecting them against such attacks is essential to maintaining SDN-based network integrity and reliability This role focuses on advanced intrusion detection systems (IDS) that use machine learning to detect and mitigate Flow Table Excessive attacks

1.1. Background and Purpose

Software-defined networking (SDN) represents a revolutionary approach to network management, providing unprecedented flexibility and centralized control over network resources Decoupling the control plane from the data plane SDN provides dynamic network reconfiguration and enhanced visibility, which is essential for modern network environments but also poses additional security challenges Advantages to be addressed It is quite advantageous.

One such challenge is the vulnerability of Flow Table Overflow attacks. In SDN, network switches use flow tables to store packet forwarding and processing rules. These tables have limited capacity, and if they are overwhelmed by excessive or malicious flow entries, packet loss, increased latency, and possible service outages can occur in the network Detection and

mitigation of Flow Table Overflow attacks are critical to maintain performance and reliability of SDN -based networks.

Current security mechanisms for SDN often fail to detect and properly handle Flow Table Overflow attacks. Traditional intrusion detection systems may not be well suited for the unique characteristics of SDN environments, where flow tables and traffic patterns differ significantly from flow tables. A dedicated Flow Table IDS is needed to address the unique challenges of overflow attacks.

1.2. Scope

The project will be structured across phases, including simulation and data collection, feature engineering and model development, real-time detection and response, evaluation and optimization. Each phase will include intensive research, development and testing to ensure that The IDS meets the required performance standards and effectively addresses identified problems.

1.3. Literature Review

Introduction to SDN and Flow Table Overflow

Software-defined networking (SDN) represents a major shift from the traditional networking model of centralizing control through an SDN controller, managing the network infrastructure through a programmable interface. This approach increases scalability and control but creates security weaknesses. Another comes along. Flow table overflow attacks exploit the limited capabilities of flow tables in SDN switches, degrading network performance and potentially disrupting this service. Understanding these attacks and existing detection mechanisms is important for we have found effective security solutions.

Flow table overflow attack

Flow table overflow attacks occur when an attacker overflows a switch's flow table with too many flow entries, causing the table to reach its capacity. This causes legitimate traffic to be dropped or routed incorrectly, resulting in network instability. Researchers have analyzed various aspects of this attack:

Description and characterization: Preliminary studies, such as those of Kreutz et al. (2015), identify key weaknesses in SDN flow tables and demonstrate the potential impact of overflow attacks on network performance. Their work has highlighted the need for a specialized detector.

Invasive attacks and impact: A follow-up review, including papers by Nunes et al. (2014) and Hu

et al. (2018), investigate how attackers use flow table restrictions to degrade network services. These studies provide insights into the causes and consequences of attacks and emphasize the importance of a proactive safety net.

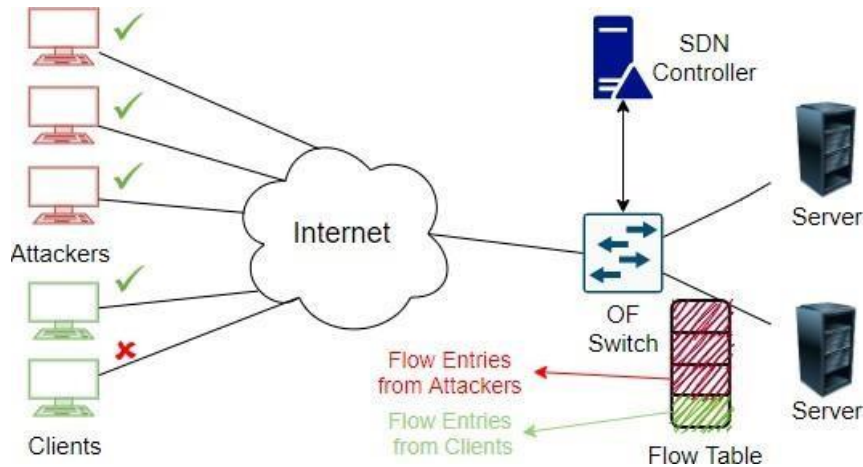


Figure 1 Flow table overflow attack

Intrusion Detection Systems in SDN

The purpose of Intrusion Detection Systems (IDS) in an SDN environment is to detect and mitigate various types of attacks including Flow Table Overflow. Several approaches have been proposed

Traditional IDS methods - Zhang et al. (2017) review traditional IDS techniques and adapt them to SDN scenarios. Their study shows that while traditional approaches provide foundation, they often require significant flexibility to effectively address SDN-specific threats.

Machine learning-based IDS - Recent studies, such as Wang et al. (2019) and Chen et al. (2020), investigate the use of machine learning algorithms for intrusion detection in SDN. These methods use pattern recognition and anomaly detection to increase detection accuracy. However,

challenges remain in ensuring real-time performance and addressing the dynamic nature of the SDN environment.

Flow table overflow detection - Specific studies on flow table overflow detection, such as the work by Sharma et al. (2021), focuses on IDS devices designed for this type of attack. This study has proposed various methods, including flow table monitoring and traffic analysis, to detect extreme conditions. However, the effectiveness and scalability of these methods in real-world settings remains an area of active research.

1.4. Research Gap

Despite advances in SDN security and IDS development, many gaps remain:

Scalability: Many existing solutions struggle with scalability, especially in large, complex SDN environments. Research is needed to develop scalable detection mechanisms that can handle high traffic volumes and large network topologies.

Real-time detection and response: Achieving real-time detection and automated response to flow table overflow attacks is challenging. Current methods may suffer from latency or limited responsiveness, and further research will be required to find effective and timely solutions.

Adaptive and robust systems: Adaptive IDS systems that can adapt to changing network conditions and evolving attack patterns are needed. Current research generally lacks the flexibility to effectively address attacks.

Connectivity with Existing Infrastructure: Integrating new IDS solutions into existing SDN infrastructure can be challenging. Analytics must address compatibility issues and ensure seamless integration with current security tools and protocols.

1.5. Research Problem

Current security mechanisms for SDN often fail to detect and properly handle Flow Table Overflow attacks. Traditional intrusion detection systems may not be well suited for the unique characteristics of SDN environments, where flow tables and traffic patterns differ significantly

from flow tables A dedicated Flow Table IDS is needed to address the unique challenges of overflow attacks

2. Objectives

The main objective of this project is to develop an Intrusion Detection System (IDS) designed to detect and mitigate Flow Table Overflow attacks in SDN environments The IDS will attempt to achieve the following objectives.

2.1. Specific objectives

2.1.1. Data Collection and Preprocessing

Gather large-scale network traffic data that includes scenarios of Flow Table Overflow attacks and normal traffic patterns. Preprocess the data by cleaning it to remove noise, handling missing values, and normalizing features to ensure consistency. Ensure that the dataset is in an optimal format for training machine learning models, thereby enhancing their performance and reliability

2.1.2. Develop Detection Mechanisms:

The goal of creating detecting mechanisms is to examine the state of flow tables and related network traffic by applying sophisticated machine learning techniques. These algorithms identify subtle characteristics that point to a Flow Table Overflow attack by examining the flow table states and network traffic behavior in both normal and attack conditions. By using the gathered and preprocessed data to train models, the procedure enables the system to distinguish between legal traffic and possible attack vectors. The SDN environment's security and resilience are improved by the IDS's ability to precisely detect and anticipate overflow threats in real-time.

2.1.3. Implement Real-Time Response

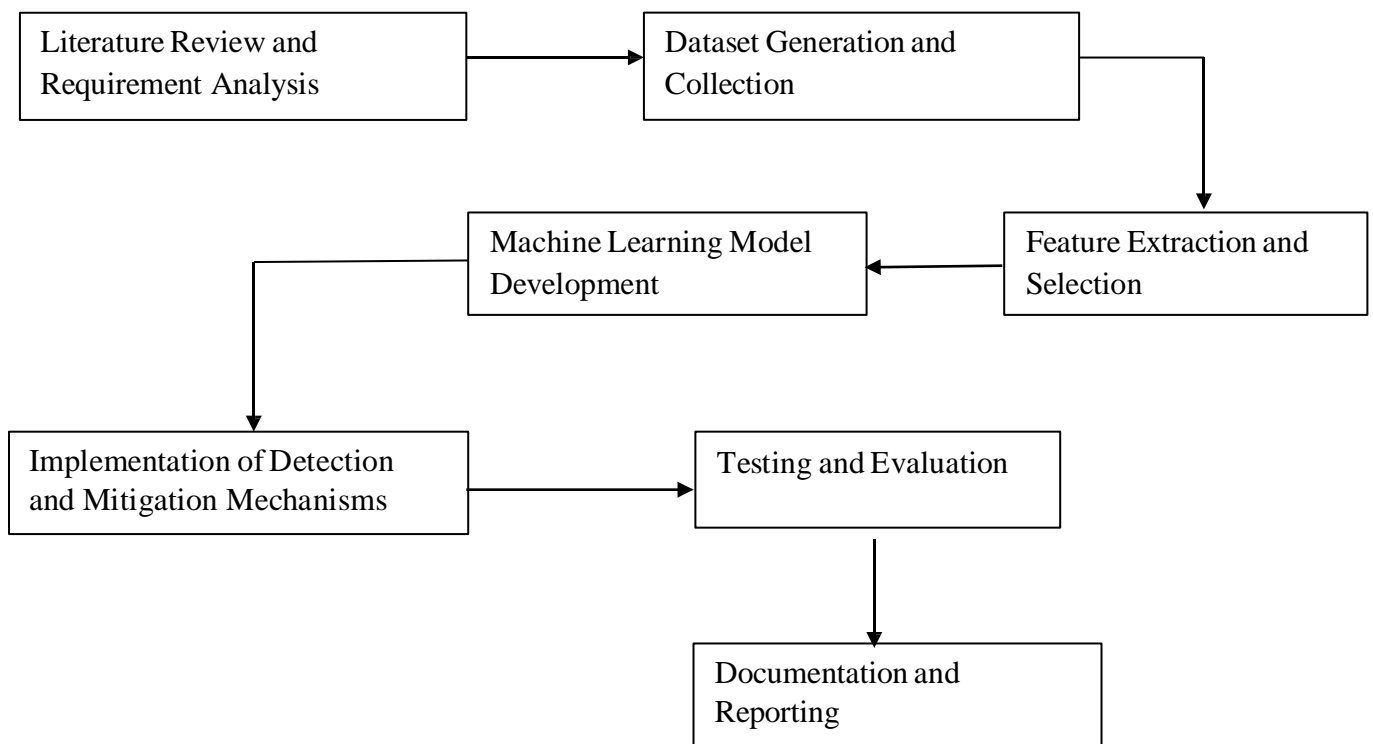
The goal of putting real-time response into practice is to create and deploy a detection framework that can quickly identify and stop Flow Table Overflow attacks as they happen. The SDN controller will be integrated with this framework, which will continuously monitor network traffic and flow table conditions. The system will automatically initiate predefined reaction

actions, such rerouting traffic, modifying flow table entries, or alerting administrators, upon recognizing patterns that point to an overflow attack. These automated reactions are intended to quickly lessen the attack's effects while preserving network stability and avoiding additional interruption.

2.1.4. Evaluate System Performance

The goal of evaluating system performance is to fully test the Intrusion Detection System (IDS) to determine its efficacy and efficiency. To assess the intrusion detection system's accuracy, responsiveness, and resource efficiency, a range of situations, such as regular network operations and simulated Flow Table Overflow attacks, are thrown at it. To find areas of strength and possible improvement, performance indicators like false positive rates, detection latency, and system overhead will be studied. The goal is to ensure that the IDS not only detects and mitigates attacks effectively but also operates efficiently without significantly impacting the overall network performance.

3. Methodology



This project's methodology is based on a Systematic approach to creating and assessing an SDN-based intrusion detection system (IDS) with the goal of identifying Flow Table Overflow attacks. A thorough review of the literature is part of the first phase, which aims to comprehend the present state of the field and identify any gaps in the detection procedures for Flow Table Overflow. The development and gathering of suitable data sets that mimic both regular and malicious traffic in an SDN context comes next. After that, to make sure these datasets are prepared for machine learning model training, they are cleaned, labeled, preprocessed, and normalized. As the project moves forward, important elements are extracted and chosen from the data, with an emphasis on those that are most suggestive of Flow Table Overflow attacks. A machine learning model is trained using these characteristics.

Once the model developed, Flow Table Overflow attacks can be detected and mitigated in real time by integrating the created model with the SDN controller. In a simulated SDN environment, the detection and response mechanisms are put through an exhaustive testing procedure to assess the system's performance in different scenarios. During this phase, possible vulnerabilities are also found, and the system is optimized appropriately. In the last phase, every step of the project—from design to testing—must be well documented. Additionally, a report detailing the system's development and assessment must be prepared. This report will act as a basis for the project's final presentation and demonstration, as well as a vital source for future developments.

3.1. Technologies

Mininet - A network emulator used to create a virtual network environment for testing SDN applications.

GNS3 - A network simulation tool used to create and test complex network topologies.

OpenDaylight - A modular SDN controller providing a flexible platform for creating network applications and policies.

TensorFlow - An open-source library for building and training machine learning models, useful for detecting anomalies and intrusions.

NetFlow/SFlow - Protocols for collecting and analyzing network traffic data, providing insights into network performance and anomalies.

Wireshark - Packet Capture Tools for capturing and analyzing network packets and traffic.

MySQL - Relational databases for storing structured data, such as network logs and IDS alerts

Jupyter Notebooks: A web application for creating and sharing documents with live code, visualizations, and narrative text, useful for documenting data analysis and results.

Programming languages – Python, SQL and Java

4. Requirements

4.1. Functional

Requirements

1. Flow Table Overflow Detection

The system must detect Flow Table Overflow attacks accurately in real time in the SDN environment.

The IDS must monitor flow table parameters to identify potential overflow conditions, such as the number of flow entries and flow table usage

2. Integrating Machine Learning

The system should integrate machine learning models trained to identify patterns indicative of Flow Table Overflow attacks.

The system must process incoming network traffic data and use machine learning models to determine if an attack is occurring.

3. Proactive Incident Response

When a Flow Table Overflow attack is detected, the system should initiate customized automatic response actions, such as blocking malicious traffic or reallocating flow table resources

The system should support dynamic configuration changes based on the severity and nature of the detected attack.

4. Insights and Reports:

If a Flow Table Overflow attack is detected, the system should generate alerts and notifications.

Alerts should be sent to network administrators with detailed information about the attack, including the switch involved and the nature of the overflow.

5. System management and logging:

The system should provide real-time analysis of flow table status and network traffic.

All detected attacks, responses, and related network data should be recorded for later analysis and audit.

4.2. Non-Functional Requirements

1. Performance

The system should detect Flow Table Overflow attacks with minimal latency, ensuring real-time response capability.

The system must handle high network traffic volumes without significant performance degradation.

2. Scalability

The system must be scalable to increase network sizes and traffic volumes. And the architecture must support the addition of more SDN switches and controllers as the network expands.

3. Reliability

The system must be reliable, with low downtime and robust error handling mechanisms to ensure continued operation. It can provide precise visual results with high accuracy and recall.

4. Security

The system itself must be secure, including access controls to prevent unauthorized changes to detection codes or response procedures.

Communication between system components (e.g., IDS, SDN controller, and switches) must be encrypted to prevent tampering.

5. Usability

The system interface should be user-friendly, allowing network administrators to set up diagnostic rules, view alerts, and create access profiles with ease.

Provide documentation to guide users in system installation, operation, and troubleshooting.

6. Maintainability

The system should be designed for easy maintenance, with modular components that can be upgraded or replaced without affecting overall performance.

The codebase should be well documented to facilitate future updates and debugging.

7. Interoperability

The system must be compatible with different SDN controllers and networking devices, allowing for integration across SDN environments.

It should support standard communication protocols to interface with other security tools and network management systems.

4.3. System Diagram

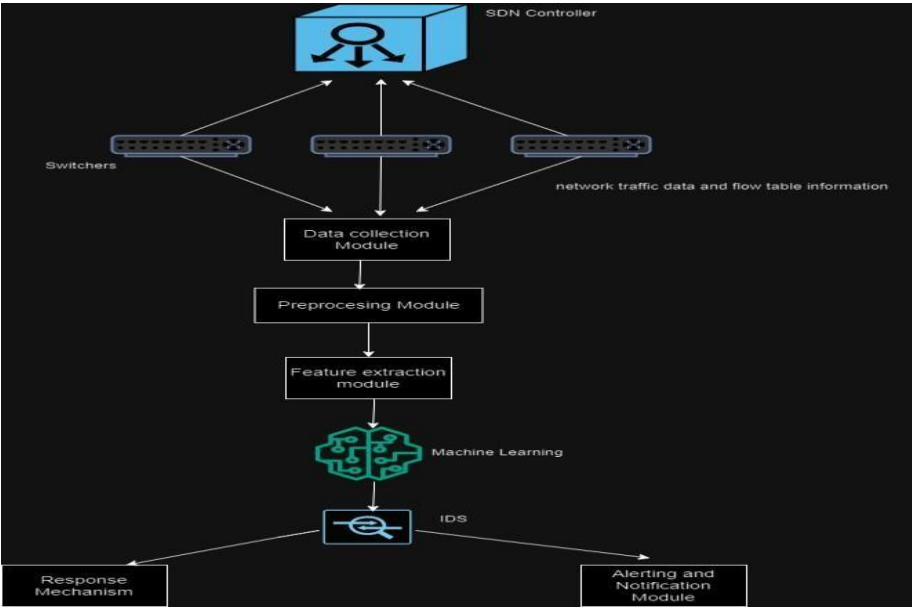


Figure 2 Individual system diagram

4.4. Timeline

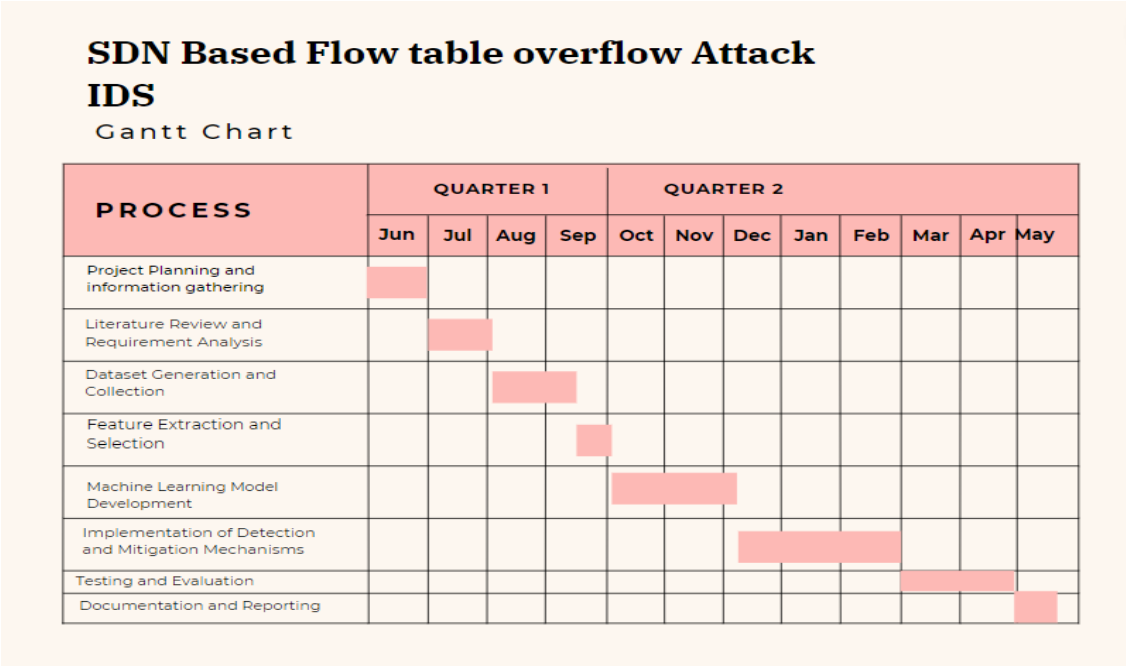


Table 1Gantt chart

5. Conclusion

In conclusion, the goal of this research is to create an Intrusion Detection System (IDS) that is especially made to recognize and stop Flow Table Overflow attacks in order to improve the security of Software-Defined Networking (SDN) settings. Through the establishment of a regulated SDN environment, the acquisition and preprocessing of extensive network traffic data, and the utilization of cutting-edge machine learning algorithms, the intrusion detection system will be capable of precisely identifying attack patterns. By putting in place a real-time detection framework with automated reaction capabilities, the system can respond quickly to overflow situations and preserve the integrity and stability of the network. This project will demonstrate the efficacy and efficiency of the IDS through thorough testing and assessment, offering insightful analysis and significant advancements to the field of network security. In addition to increasing defenses against particular SDN attacks, the project's successful completion will offer a scalable architecture for future security solutions in dynamic networking settings.

6. Commercialization

Our SDN-based Intrusion Detection System (IDS) will be positioned strategically to meet the increasing market need for cutting-edge network security solutions when it comes to commercialization. Initially, the IDS will be made available to all enterprises aiming to improve their cybersecurity posture as a feature-rich, adaptable solution that includes all the necessary tools to identify and stop Flow Table Overflow attacks. We will offer premium modules and advanced features, such extended attack pattern libraries, automatic response settings, and enhanced analytics, as part of a subscription-based approach in order to make more money. A one-month free trial that grants access to all premium functionalities will provide new customers the chance to see the IDS's full potential. This strategy strikes a balance between accessibility and the potential for recurring income by allowing companies to assess the entire range of advantages prior to committing to a subscription. Our IDS will serve both small and large businesses by providing a scalable and feature-rich solution that will meet a variety of needs and capitalize on the expanding market for sophisticated network protection.

7. Approximate Budget Analysis

Component	Amount (USD)	Amount (LKR)
Data Collection and Storage	25	7508.40
Testing and Evaluation Tools	30	9010.07
Miscellaneous Expenses	20	6006.72
Total	75	22525.19

Table 2 budget

8. References

- I. Noh, S.K Park, M. HSDT, "Table-Overflow Attack Defender with Historical Statistics Based Dynamic Timeout in Software Defined Networks". [Online], Nov 10 2023, Available: <https://doi.org/10.3390/app132212232>
- II. Changqing Zhao, Ling Xia Liao, Han-Chieh Chao, Roy Xiaorong Lai, Miao Zhang, "Flow Table Overflow Attacks in Software Defined Networks: A Survey", Journal of Internet Technology Vol.24, pp.1391- 1401, December 2023
- III. D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," [Online] *Proc. IEEE*, vol. 103, no. 1, pp. 14-76, Jan. 2015. Available: <https://ieeexplore.ieee.org/document/6994333>
- IV. B. A. A. Nunes, M. Mendonca, X. N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," [Online] *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014. Available: <https://ieeexplore.ieee.org/document/6739370>
- V. F. Hu, Q. Hao, and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," [Online] *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 1-21, Third Quarter 2018. Available: <https://ieeexplore.ieee.org/document/8382293>
- VI. H. Zhang, X. Liu, Y. Liu, and J. Zhou, "A Survey on Traditional and SDN-Based IDS Approaches: Adaptation and Challenges," [Online] *IEEE Access*, vol. 5, pp. 21273-21281, 2017. Available: <https://ieeexplore.ieee.org/document/7964336>
- VII. P. Wang, X. Zhu, and L. Zhou, "Machine Learning-Based Security Approaches in SDN," [Online] *J. Commun. Netw.*, vol. 21, no. 4, pp. 317-331, Aug. 2019. Available: <https://ieeexplore.ieee.org/document/8847565>

- VIII. J. Chen, X. Huang, and Y. Li, "Anomaly Detection and Prediction Using Machine Learning in SDN: Challenges and Solutions,"[Online] *IEEE Commun. Surv. Tutorials*, vol. 22, no. 4, pp. 2739-2761, Fourth Quarter 2020. Available: <https://ieeexplore.ieee.org/document/9145013>
- IX. Mustafa SOYLU," A Study on Flow Table Overflow Attack Mitigation in SDN using Network Functions Virtualization.", Master'Thesis, Department of Applied Information Science Graduate School of Information Science, Tohoku University, 2022