A Major Project Proposal Report on

Praharak - An Enhanced threat detection and protection

Submitted in Partial Fulfillment of the Requirements for

The Degree of **Bachelor of Engineering in Computer Engineering**

Under Pokhara University

Submitted by:

Aishu Gyawali, 191306

Bishal Poudel, 191318

Date

27 Apr, 2024

Department of Computer Engineering

NEPAL COLLEGE OF INFORMATION TECHNOLOGY

Balkumari, Lalitpur, Nepal

ABSTRACT

Cyberattacks are becoming increasingly frequent and complicated, posing a substantial danger to individuals and businesses throughout the world. Traditional cybersecurity solutions frequently fall short of the adaptive techniques used by hackers, leaving networks open to attack. In response, this project "Praharak - An Enhanced Threat Detection and Protection" provides a complete security system for detecting and preventing unauthorized access, malicious actions, and other network security risks. Praharak integrates IDS, IPS, and SIEM features to provide a more comprehensive approach to network security. Praharak uses deep learning algorithms to analyze network traffic patterns, detect irregularities that indicate threatening activities, and take required steps in real time. This project intends to create an open-source, user-friendly interface for system configuration, monitoring, and reporting that will be accessible to a wide variety of users. Praharak aims to improve cybersecurity measures and guard against emerging threats by offering a low-cost, AI-powered alternative to standard network security solutions.

Keywords: Network security, Intrusion Detection and prevention, Intrusion Prevention System, Security Information and Event Management, Deep learning

Table of Content

1. Introduction

Praharak - An Enhanced threat detection and protection is a security solution which is designed to detect and prevent unauthorized access, malicious activities, and other security threats within a network with the integration of IPS, IDS and SEIM.

IDS stands for Intrusion Detection System, which is a security system designed to monitor network or system activities for malicious activities or policy violations. IPS stands for Intrusion Prevention System, which is a security tool that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. SIEM stands for Security Information and Event Management, which is a software solution that aggregates and analyzes activity from many different resources across an entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more, and analyzes that data to identify and respond to security threats.

Integrating SEIM, IDS and IPS capabilities enables a more comprehensive approach to security. IDS can detect suspicious behavior, but IPS can take proactive steps to prevent such risks and SIEM enables centralized logging, analysis, and correlation of security events across several network devices. Praharak uses deep learning models to evaluate network traffic patterns, detect abnormalities indicating hostile behavior, and initiate necessary actions since Deep learning algorithms have shown promising results for anomaly detection and threat categorization.

2. Problem Statement

Hackers target computers connected to the internet every 39 seconds increasing the frequency and complexity of cyberattacks that impact one in three people daily [1]. These assaults, which mostly target network endpoints, present a serious problem for people and enterprises everywhere. Even with advancements in cybersecurity, traditional measures typically fall short against adaptive strategies used by hackers, leaving the network vulnerable to exploit.

3. Project objective

The primary objective of the 'Praharak' project is

- To develop an open-source network security system by using deep learning algorithms, which is capable of detecting and preventing a wide range of security threats in real-time.
- To create a user-friendly interface for a system configuration, monitoring and reporting by integrating IDS, IPS and SEIM functionalities.

4. Scope and Limitation

4.1 Scope

The system's scope includes real-time analysis of network activity, which allows for continuous monitoring to detect and respond to any threats. Furthermore, its use spans other sectors, including companies, banking institutions, workplace and industries providing a powerful security solution.

4.2 Limitation

As we are limited to resources like representative datasets, that might encounter false positives and false negatives which result in false alerts.

5. Literature review

5.1 Snort

Snort, a free and open-source NIDS/IPS, has gained significant recognition for its effectiveness and flexibility.Developed by Martin Roesch in 1998,Snort has evolved as a versatile significant tool in network security for two years.It is rule based detection mechanism.

Snort is based on the packet capture library (libpcap), a system-independent interface for capturing traffic that is widely used in network analyzers [2]. Snort monitors network traffic and compares it against a Snort rule set defined by users in a config file. It applies these rules to packets in network traffic and issues alerts when it detects any anomalous activity.

Snort finds widespread application across diverse sectors of cybersecurity. It is extensively deployed in enterprise networks, where it acts as a vigilant guardian, detecting and thwarting unauthorized access attempts, malware intrusions, and other cyber threats in real-time. Government agencies and defense organizations rely on Snort to safeguard critical infrastructure and national security interests, detecting espionage activities and defending against cyber attacks.Snort serves as a valuable tool for cybersecurity research and development, enabling researchers and developers to analyze network traffic, devise new detection techniques, and evaluate the effectiveness of security solutions.Beyond its core functionality, researchers have sought to expand Snort's capabilities through the integration of plugins and preprocessors. These extensions enable Snort to handle a wider range of network protocols and data formats, thereby increasing its versatility and applicability in diverse network environments [3].

Snort doesn’t offer advanced machine learning capabilities,relying only on old tools like signature whereas ‘Praharak’ is an all-in-one approach that makes it easier to manage your network security and fight off new attacks, unlike older tools that rely on signatures. Praharak uses advanced machine learning to catch tricky attacks that other systems might miss.

5.2 Suricata

Suricata is also an open-source detection engine that can act as an intrusion detection system (IDS) and an intrusion prevention system (IPS). It was developed by the Open Information Security Foundation (OSIF) and is a free tool used by enterprises.multi-threaded. Meaning that the tool can use multiple cores at once, allowing for greater load balancing. This allows us to process more data without dialing back on the number of rules we implement.

Suricata distinguishes itself by its ability to perform both intrusion detection and prevention functions effectively . Suricata not only merely detects and alerts threats but also actively blocks malicious traffic. Furthermore, Suricata's proficiency in deep packet inspection enhances its efficacy in identifying and mitigating diverse cyber threats, making it well-suited for a wide range of security monitoring initiatives .

Several studies have explored techniques for optimizing Suricata rule sets to improve detection accuracy and performance. This includes research on rule prioritization, rule chaining, and reducing rule redundancy [4].

Suricata, a popular NIDS, relies on static rules and manual management, limiting its ability to adapt to new threats. Praharak, on the other hand, leverages AI for advanced threat detection and automated rule management. Additionally, Praharak is designed for effortless cloud deployment, unlike Suricata. This makes Praharak a superior choice for organizations seeking a future-proof and AI-powered intrusion detection solution.

5.3 Palo Alto

Palo Alto Networks, is a well-known cybersecurity company headquartered in Santa Clara, California,which they focus on providing next-generation firewalls that go beyond traditional firewalls by inspecting traffic based on application, user, and content. .

This enables more precise management and improved security against cyber attacks. Their solution contributes to network security by offering visibility and control over network activity for more than 60,000 business clients globally [5].

They are regarded as a prominent cybersecurity firm, providing a range of solutions to defend organizations from cyberattacks [5].Their main products are sophisticated firewalls that examine application traffic in addition to IP addresses.

Although, Palo Alto Networks' provide a full security suite, they may not be appropriate for many enterprises owing to cost and complexity . Praharak seeks to provide a possibly more cost-effective and configurable alternative, with an emphasis on deep learning-based threat detection and mitigation.

5.4 Splunk

Splunk is the world's leading operational data intelligence platform [6]. This platform is used to search, analyze and visualize the machine-generated data gathered from the websites, applications, sensors, devices etc. which make up IT infrastructure and business. Providing real time processing stands it out from other platforms. Splunk comes in different variants, and which is proprietary software. It is one example of a SEIM solution.

Throughout the course of time, there have been many tries for the development of integrated tools having capability of IDS, IPS and SEIM. One of the important attempts can be considered by Muhammad et al. [7]. They integrated IDS and SEIM for live analysis using machine learning techniques. In this project they have used ELK stack for SEIM functionality, Zeek for IDS and Slip for machine learning analysis. The proposed system by them was tested using Denial of Service (DoS) test with 344.1/sec packet.

ELK is the stack that comprises three popular projects: Elasticsearch, Logstash, and Kibana. It provides the search and analytics engine, data ingestion, visualization and thus SEIM capabilities. It can be considered as an open source alternative for SEIM [8].

Zeek on the other hand works as IDS, It can create different log files based on the flow of traffic such as conn.log, dns.log, http.log etc. Which helps for data feeding to the next stage, Slips. Which is used for real time packet analysis using machine learning algorithm Support Vector Machine and some behavioral techniques.

Beside these, Praharak provides deep learning techniques for the attack detection, provides a more flexible environment and also integrates IPS capabilities. Which itself can be considered an ideal project for security solution.

6. Methodology

Software Development Life Cycle(SDLC) provides a method for building and delivering software projects. There are various stages of SDLC such as communication, planning, design, implementation, and deployment. There are various software development models like waterfall, incremental, spiral, and prototyping, which are based on the framework provided by SDLC. Each model has their usage and criteria. We found an Incremental model also known as Rapid Application Development(RAD) is best suited for our project. This model combines elements of the waterfall model applied in an iterative fashion [9].

In our project there will be two increments, each increment will traverse through the stages of SDLC. Our end product is somehow clear but there are many requirements/features that we have to add or modify over time. In each increment, we will develop a working product and add new features to it.

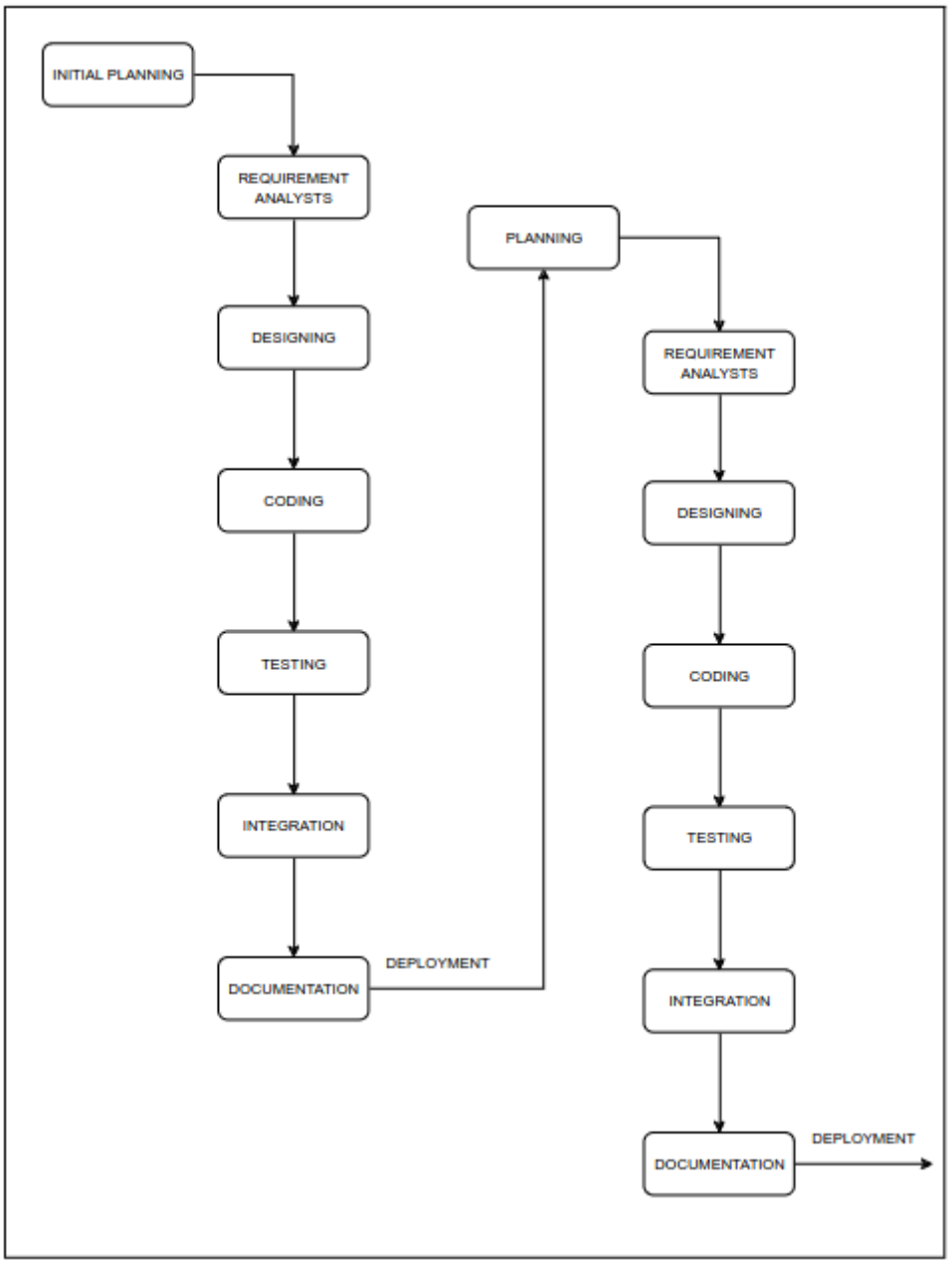

Figure 1. Methodology of Praharak

7. System Architecture

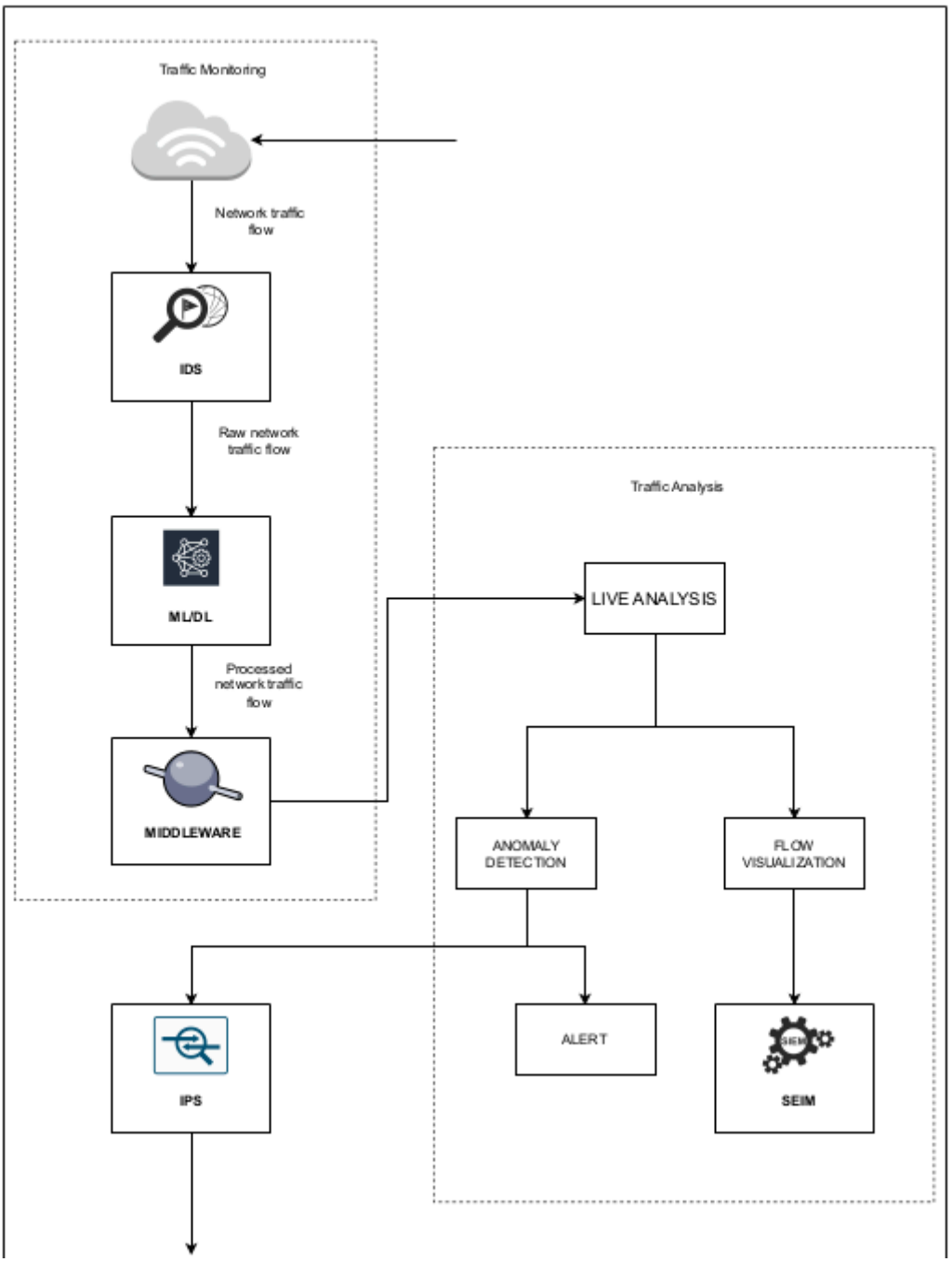

Figure 2. Generalized System Architecture

8. Use case diagram

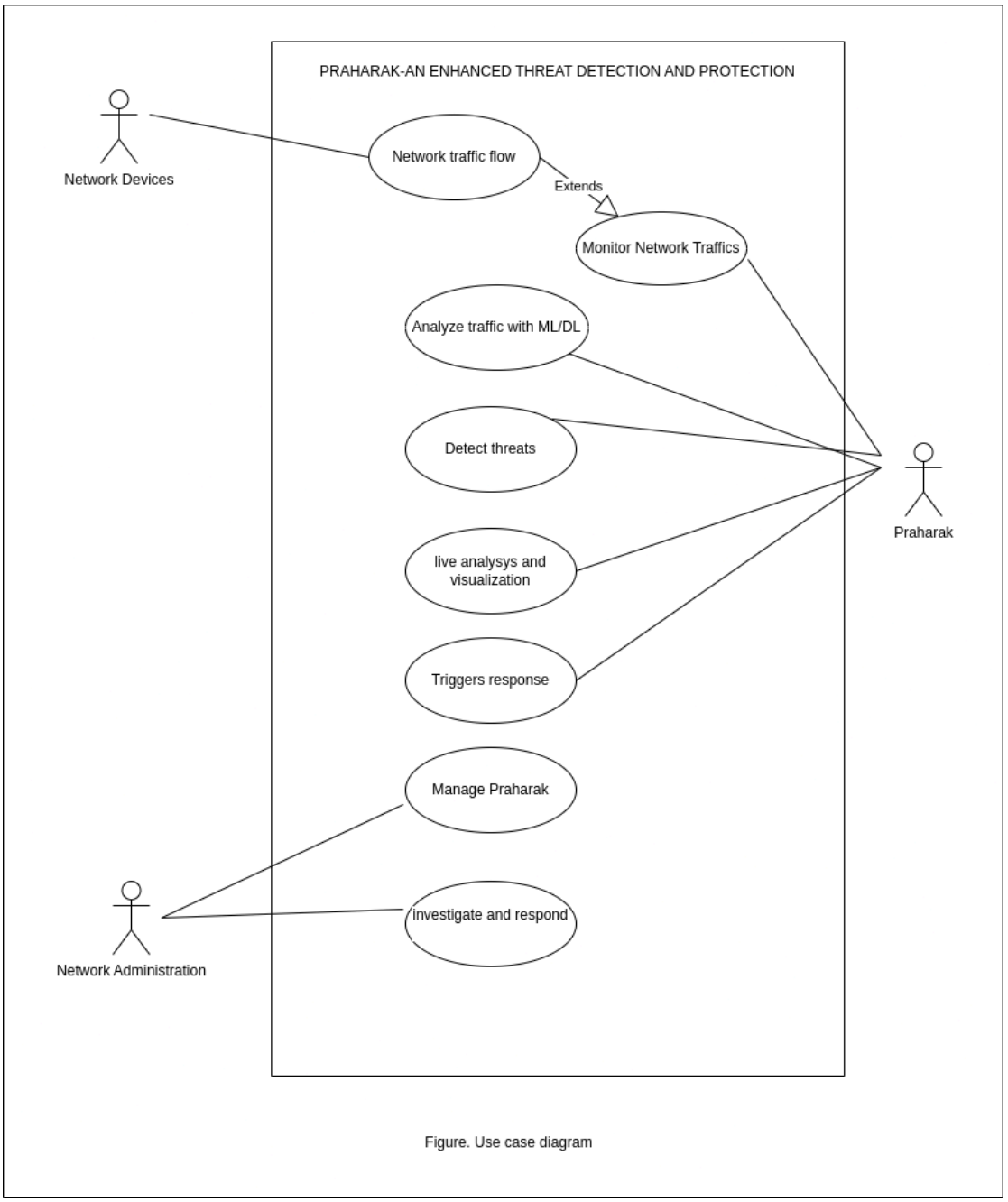

Figure 3. Use Case diagram

9. Expected outcomes

The Praharak system is expected to produce a real-time network security system capable of detecting and preventing a variety of security threats through deep learning algorithms. It will integrate IDS, IPS, and SIEM features to create a user-friendly interface for configuration, monitoring, and reporting. Overall, Praharak intends to provide an open-source, low-cost, AI-powered alternative to traditional network security solutions.

10. Time schedule

Figure 4. Gantt chart for increment 1

Figure 5. Gantt chart for increment 2

References

[1] University of North Georgia. "Cyber Operations." [Online]. Available: https://ung.edu/cyber-operations/index.php [Accessed: April 19, 2024].

[2] "How Snort Works," CrowdStrike, Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/ ,[Accessed :14 Apr, 2024].

[3] Teng, L., et al. (2017). Enhancing Snort with a Protocol Parsing Plugin for SCADA Protocol Detection. Journal of Network and Computer Applications, 89, 40-49.

[4] A. Dulac, X. Levillain, and I. E. Magedanz, "Optimizing Snort and Suricata Rule Sets for Fast and Accurate Intrusion Detection," in 2014 International Conference on Computing, Networking and Security (CNS), pp. 152-157, 2014.

[5] Palo Alto Network [online] .Available:https://www.paloaltonetworks.com/ [Accessed:April 21,2024].

[6] Subramanian, Karun, and Karun Subramanian. "Introducing the Splunk Platform." *Practical Splunk Search Processing Language: A Guide for Mastering SPL Commands for Maximum Efficiency and Outcome* (2020): 1-38.

[7] Muhammad, Adabi & Sukarno, Parman & Wardana, Aulia. (2023). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. Procedia Computer Science. 217. 1406-1415. 10.1016/j.procs.2022.12.339.

[8] Vazão, Ana, et al. "SIEM open source solutions: a comparative study." *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2019.

[9] Salve SM, Samreen SN, Khatri-Valmik N. A Comparative Study on Software

Development Life Cycle Models. International Research Journal of Engineering and

Technology (IRJET). 2018 Feb;5(2):696-700.