International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 11, Issue 7, July-2026, http://ijmec.com/, ISSN: 2456-4265

Network Traffic Monitoring and Intrusion Detection System for Digital Forensics

Ms C Bhargavi[1], A. Sai Srija[2], G. Sindhutulani[3], Ch. Sujatha[4]

[1]Assistant Professor: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

[2,3,4]B. Tech Students: Department of Electronics and Communication Engineering, Bhoj Reddy Engineering College for Women Hyderabad, India

Mail Id: saisrija.01@gmail.com[2], gurramsindhutulani@gmail.com[3], chavalasujatha1234@gmail.com[4]

Accepted 4 July 2026

ABSTRACT

A Network Traffic Monitoring and Intrusion Detection System (IDS) plays a vital role in identifying malicious activities, strengthening network security, and supporting digital forensic investigations. This project focuses on the design and implementation of a system that captures, analyzes, and records network traffic in real time while detecting suspicious activities such as unauthorized access, malware attacks, and data breaches.

With the rapid expansion of networked environments, cybersecurity threats have become increasingly sophisticated and frequent. The proposed Network Traffic Monitoring and Intrusion Detection System for Digital Forensics continuously monitors network traffic, captures packets, analyzes communication patterns, and detects potential intrusions using both signature-based and anomaly-based detection techniques. These methods enable the system to identify known attacks as well as unusual network behaviors that may indicate emerging threats.

The system employs packet sniffing, traffic analysis, anomaly detection, and signature-based mechanisms to recognize malicious activities. All captured network data and security events are securely stored to facilitate forensic investigations. The proposed approach enhances intrusion detection accuracy, strengthens network monitoring, and assists investigators in tracing cyber-attacks and identifying their origin. Additionally, the system maintains comprehensive logs of network activities, which are essential for reconstructing attack scenarios, tracing malicious actions, and providing reliable digital evidence during forensic analysis. Real-time alerts are also generated to notify network administrators of potential threats, enabling prompt response and effective mitigation.

Experimental results demonstrate that the proposed system provides efficient real-time network monitoring, accurate intrusion detection, and reliable data logging for forensic purposes. Owing to its capability to improve network security and support digital investigations, the system is well suited for applications in enterprise networks, cybersecurity operations, and digital crime investigations. Furthermore, the proposed system can be enhanced by integrating advanced machine learning techniques to improve detection accuracy, minimize false positives, and adapt to evolving cyber threats.

Keywords— *Network Traffic Monitoring, Intrusion Detection System (IDS), Digital Forensics, Packet Sniffing, Signature-Based Detection, Anomaly Detection, Cybersecurity, Network Security, Traffic Analysis, Real-Time Monitoring.*

Introduction

In today's interconnected digital environment, computer networks have become an essential part of communication, business operations, cloud computing, and information sharing. Organizations, educational institutions, government agencies, and individuals rely heavily on network infrastructure for the secure transmission and storage of data. As the number of connected devices and internet-based services continues to grow, networks are increasingly exposed to various cybersecurity threats, including unauthorized access, malware infections, phishing attacks, ransomware, denial-of-service (DoS) attacks, and data breaches. These threats can compromise the confidentiality, integrity, and availability of critical information, resulting in significant financial losses, operational disruptions, and reputational damage.

To address these security challenges, continuous monitoring of network traffic has become a fundamental requirement for modern cybersecurity. A Network Traffic Monitoring and Intrusion Detection System (IDS) is designed to capture, inspect, analyze, and interpret network packets in real time to identify malicious activities and abnormal behavior. By monitoring incoming and outgoing traffic, the system can detect known attack signatures as well as unusual network patterns that may indicate emerging or previously unknown threats. Early detection enables

network administrators to respond promptly, minimize damage, and maintain the overall security of the network infrastructure.

In addition to enhancing cybersecurity, network traffic monitoring plays a significant role in digital forensics. The system captures and securely stores detailed records of network activities, including packet information, communication logs, timestamps, and intrusion events. These records serve as valuable digital evidence for forensic investigations, enabling investigators to reconstruct attack sequences, identify the origin of cyber-attacks, analyze attacker behavior, and support legal proceedings. By preserving accurate and reliable network evidence, the system contributes to effective incident response and cybercrime investigation.

The proposed Network Traffic Monitoring and Intrusion Detection System integrates packet sniffing, traffic analysis, signature-based detection, and anomaly-based detection techniques to provide comprehensive network monitoring and threat detection. It generates real-time alerts whenever suspicious activities are detected and maintains detailed logs for future forensic analysis. The system aims to improve network visibility, enhance intrusion detection accuracy, strengthen cybersecurity, and support digital forensic investigations, making it a valuable solution for enterprise networks, educational institutions, government organizations, and other environments where secure network operations are essential.

Literature Survey

Network fundamentals provide the foundation for understanding how computer networks communicate and exchange information. In modern computer networks, devices communicate by transmitting data in the form of packets through standardized communication protocols and layered network architectures. A thorough understanding of these concepts is essential for developing a Network Traffic Monitoring and Intrusion Detection System (IDS), as the system relies on capturing, analyzing, and interpreting network traffic to identify malicious activities. In the field of digital forensics, knowledge of network fundamentals also enables investigators to examine communication patterns, reconstruct cyber incidents, and preserve digital evidence. This chapter discusses the core networking concepts, including the OSI model, the TCP/IP model, data packet structure, communication protocols, and their significance in intrusion detection systems.

OSI Model (Open Systems Interconnection Model)

The Open Systems Interconnection (OSI) model is a conceptual framework developed to standardize communication between different networking systems. It consists of seven layers, each responsible for a specific function in the process of data transmission. The **Physical Layer** forms the lowest layer of the model and is responsible for transmitting raw binary data through physical media such as cables, switches, and wireless signals. Above it, the **Data Link Layer** provides node-to-node communication by using Media Access Control (MAC) addresses while also performing error detection and correction to ensure reliable transmission over the physical medium.

The **Network Layer** manages logical addressing and routing by using Internet Protocol (IP) addresses to determine the most efficient path for data packets across interconnected networks. The **Transport Layer** ensures reliable communication between sender and receiver by segmenting data, controlling data flow, detecting transmission errors, and reassembling packets at the destination. It primarily utilizes the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

The **Session Layer** establishes, manages, and terminates communication sessions between applications, ensuring synchronized communication throughout data exchange. The **Presentation Layer** is responsible for data formatting, encryption, decryption, and compression, allowing information to be represented in a format understandable by both communicating systems. Finally, the **Application Layer** serves as the interface between network services and end users by supporting applications such as web browsers, email clients, file transfer services, and other internet-based applications. Understanding the functions of each OSI layer enables intrusion detection systems to inspect network traffic at multiple levels and accurately identify suspicious activities.

Cyber Attacks

Cyber Attacks are deliberate attempts by malicious individuals or organizations to gain unauthorized access to computer systems, disrupt network services, steal sensitive information, or compromise the confidentiality, integrity, and availability of digital resources. With the rapid growth of internet-based technologies, cloud computing, and interconnected devices, cyber threats have become increasingly sophisticated and difficult to detect. Attackers employ various techniques to exploit vulnerabilities in network infrastructure, operating systems, applications, and communication protocols. Therefore, understanding the nature and working mechanisms of these attacks is essential for designing an effective Network Traffic Monitoring and Intrusion Detection System (IDS). By continuously monitoring

network traffic and identifying suspicious activities, an IDS helps organizations detect threats at an early stage and respond before significant damage occurs.

Types of Cyber Attacks

Port Scanning

Port scanning is one of the most commonly used reconnaissance techniques employed by attackers to identify potential vulnerabilities within a target system. Every computer system contains multiple communication ports that provide access to various network services such as web servers, secure shell (SSH), file transfer, and email services. Common examples include Port 80 for HTTP web services, Port 22 for SSH remote access, and Port 21 for FTP file transfer. During a port scanning attack, the attacker systematically sends connection requests, typically TCP SYN packets, to a range of ports in order to determine whether they are open, closed, or filtered.

If an open port receives a SYN packet, it responds with a SYN-ACK packet, indicating that the service is available for communication. Conversely, closed ports respond with a Reset (RST) packet, while filtered ports may not respond at all due to firewall restrictions. Attackers use this information to identify accessible services and discover potential entry points for future attacks. Since port scanning is often the first stage of a cyber Attack intrusion detection systems monitor repeated connection attempts, sequential access to multiple ports, and abnormal scanning behavior to detect reconnaissance activities before exploitation occurs.

Denial of Service (DoS) Attack

A Denial of Service (DoS) attack is intended to make a network service, application, or server unavailable to legitimate users by overwhelming it with an excessive volume of requests or network traffic. The attacker continuously sends large numbers of packets that consume critical system resources such as processor time, memory, storage, and network bandwidth. As a result, the target system becomes overloaded and is unable to process legitimate user requests efficiently.

A more advanced variation, known as a Distributed Denial of Service (DDoS) attack, utilizes multiple compromised computers or botnets to launch simultaneous attacks from different locations. These coordinated attacks generate significantly higher traffic volumes, making mitigation more challenging. The primary consequences of DoS and DDoS attacks include website downtime, service interruptions, reduced system performance, and financial losses. Intrusion Detection Systems detect these attacks by monitoring unusually high traffic volumes, repeated requests from the same IP address, abnormal packet rates, and sudden spikes in network activity.

Tools Used – Wireshark

Wireshark is one of the most widely used open-source network protocol analyzers for capturing, inspecting, and analyzing network traffic in real time. It enables network administrators, cybersecurity professionals, and forensic investigators to examine every packet transmitted across a network and understand communication between devices. Wireshark captures packets directly from the selected network interface and presents detailed packet information in a structured and user-friendly format.

Each captured packet contains valuable information such as source and destination IP addresses, communication protocols, port numbers, packet size, timestamps, payload content, and various protocol-specific details. Wireshark also provides advanced filtering and search capabilities that allow users to isolate specific traffic for detailed investigation.

In this project, Wireshark is used to capture live network traffic, inspect packet structures, analyze communication patterns, detect suspicious packets, and identify cyber attacks such as port scanning, abnormal traffic behavior, and denial of service attacks. For example, repeated TCP SYN packets directed toward multiple ports may indicate port scanning activity, unusually high traffic volumes may suggest a DoS attack, while communication with unknown or malicious IP addresses may reveal unauthorized or suspicious network activity.

IDS Architecture

An Intrusion Detection System (IDS) is a cybersecurity solution designed to monitor network traffic and system activities to identify unauthorized access, malicious behavior, policy violations, and potential cyber attacks. As modern organizations increasingly depend on computer networks for communication and data exchange, the frequency and complexity of cyber threats have also increased significantly. Intrusion Detection Systems play a crucial role in strengthening network security by continuously analyzing network traffic and identifying suspicious activities before they cause severe damage. Although an IDS does not directly prevent attacks, it serves as an early warning system by detecting intrusions, generating alerts, and recording security events for further investigation. IDS solutions are widely deployed in enterprise networks, educational institutions, financial organizations, government agencies, cloud infrastructures, and cybersecurity operation centers to improve network visibility and support digital forensic investigations.

Based on Detection Method

Signature-Based IDS

Signature-Based Intrusion Detection Systems identify attacks by comparing captured network traffic against

a database containing signatures of previously known attacks. Each signature represents a unique pattern associated with specific malware, exploits, or intrusion techniques. When incoming packets match an existing signature, the IDS immediately classifies the activity as malicious and generates an alert.

This detection method provides high accuracy and low false-positive rates when identifying known threats. It is widely used for detecting malware, viruses, worms, and established attack techniques. However, because it depends on predefined signatures, it cannot detect newly emerging threats or zero-day attacks until new signatures are added to the database.

Hybrid IDS

A Hybrid Intrusion Detection System combines the capabilities of both signature-based and anomaly-based detection methods to improve overall security performance. By simultaneously comparing network traffic against known attack signatures and monitoring behavioral anomalies, hybrid IDS solutions achieve higher detection accuracy while reducing false alarms. This combined approach enables the detection of both known cyber attacks and previously unseen threats, making hybrid IDS one of the most effective intrusion detection solutions for modern network environments.

IDS Architecture

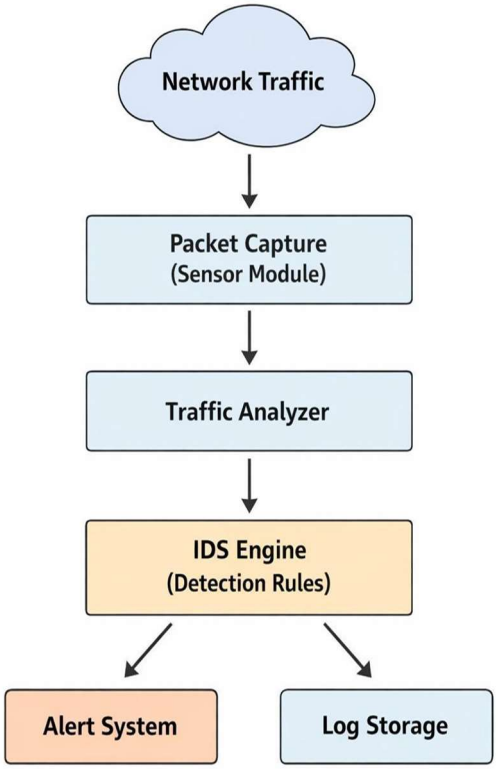

Fig 1 Basic Architecture of Intrusion Detection System

Basic Architecture of an Intrusion Detection System

The architecture of an Intrusion Detection System consists of several interconnected components that work together to monitor network traffic, analyze packets, detect malicious activities, generate alerts, and store security events for future forensic investigations. The primary components include the Packet Capture Module, Traffic Analyzer, IDS Detection Engine, Alert Generation Module, and Log Storage System. Together, these components provide continuous real-time monitoring and effective intrusion detection across the network.

Explanation of Components

Packet Capture (Sensor Module)

The Packet Capture Module, also known as the Sensor Module, serves as the entry point of the Intrusion Detection System. It continuously captures network packets directly from the network interface using packet sniffing techniques. Tools and libraries such as Scapy, Wireshark, libpcap, or WinPcap are commonly employed for packet acquisition. The captured packets contain valuable information including source and destination IP addresses, communication protocols, port numbers, packet length, timestamps, and payload data. This module supplies the raw network traffic required for subsequent analysis.

Traffic Analyzer

The Traffic Analyzer processes the captured packets by extracting relevant networking information required for intrusion detection. It identifies packet attributes such as IP addresses, transport protocols, port numbers, packet size, TCP flags, communication sessions, and packet payload characteristics. The analyzer organizes this information into structured formats suitable for the IDS detection engine while filtering unnecessary or duplicate traffic. Accurate traffic analysis enables the system to distinguish between normal network communication and suspicious behavior.

IDS Detection Engine

The IDS Detection Engine is the central component of the Intrusion Detection System. It analyzes processed network traffic using multiple detection techniques, including signature-based detection, anomaly-based detection, and threshold-based detection. The engine compares network packets with known attack signatures while simultaneously identifying deviations from normal traffic behavior. It detects various cyber threats such as port scanning, denial-of-service attacks, malware communication, brute-force login attempts, and unauthorized access. Upon identifying suspicious activities, the detection engine classifies the threat and forwards the information to the alert generation module.

Alert System

The Alert System is responsible for notifying network administrators whenever malicious activity is detected. Based on the severity of the detected threat, the system generates real-time notifications through warning messages, log entries, email alerts, or dashboard notifications. Immediate alert generation enables administrators to investigate security incidents promptly and take appropriate mitigation measures before attacks can cause significant damage.

Log Storage

The Log Storage component securely records all detected security events and network activities for future reference. Each log entry typically contains information such as timestamps, source and destination IP addresses, communication protocols, attack categories, severity levels, packet details, and detection results. These logs provide valuable evidence during digital forensic investigations, allowing investigators to reconstruct attack sequences, analyze attacker behavior, identify compromised systems, and support legal proceedings.

Working of Intrusion Detection System

The Intrusion Detection System operates by continuously monitoring network traffic and analyzing captured packets in real time. Initially, the Packet Capture Module intercepts all incoming and outgoing network packets from the network interface using packet sniffing techniques. Each packet contains essential information, including source IP address, destination IP address, protocol type, port numbers, timestamps, and payload data.

The captured packets are then forwarded to the Traffic Analyzer, where relevant packet information is extracted and organized for further processing. During this stage, the analyzer examines communication protocols such as TCP, UDP, ICMP, HTTP, and FTP while evaluating packet headers, payload contents, and communication sessions. The processed information is subsequently transferred to the IDS Detection Engine for security analysis.

Within the Detection Engine, the system applies multiple detection mechanisms to identify malicious activities. Signature-based detection compares captured packets against a database of known attack patterns to identify previously documented cyber threats. Simultaneously, anomaly-based detection evaluates network behavior against established baseline traffic patterns to recognize abnormal communication that may indicate emerging or unknown attacks. Threshold-based detection further identifies excessive traffic volumes, repeated connection attempts, and unusual network behavior by comparing network statistics against predefined limits.

Whenever suspicious activity is detected, the Alert System immediately generates warning notifications for network administrators, enabling rapid incident response and threat mitigation. Simultaneously, detailed information about the detected intrusion—including timestamps, IP addresses, attack type, protocol information, and detection results—is securely stored in the Log Storage module. These records provide comprehensive evidence for cybersecurity audits, incident response, and digital forensic investigations.

The entire monitoring and detection process operates continuously without interrupting normal network communication. By integrating packet capture, traffic analysis, intelligent detection techniques, real-time alert generation, and comprehensive event logging, the Intrusion Detection System provides an effective solution for identifying cyber threats, strengthening network security, and supporting digital forensic analysis.

System Design

The proposed Network Traffic Monitoring and Intrusion Detection System (IDS) is designed to monitor network traffic continuously, analyze captured packets, detect suspicious activities, generate security alerts, and maintain detailed logs for digital forensic investigations. The overall system architecture integrates packet capture, traffic analysis, intrusion detection, alert generation, and data storage into a unified framework that enables real-time monitoring of network activities. The system combines both a block diagram and a flowchart to illustrate the complete workflow, beginning with packet acquisition from the network and ending with threat detection, alert notification, and secure log storage. Each module performs a specific function while working together to provide effective intrusion detection and network security.

Network Input

The Network Input forms the initial stage of the proposed system. It represents all network-connected devices such as desktop computers, laptops, servers, routers, switches, mobile devices, and Internet of Things (IoT) devices that continuously communicate over the network. These devices exchange information in the form of data packets through various communication protocols, including TCP, UDP, HTTP, FTP, and ICMP. The entire network traffic generated by these devices serves as the input to the Intrusion Detection System.

The proposed system continuously monitors both incoming and outgoing network traffic in real time. Every packet transmitted through the network interface is captured and analyzed to determine

whether it represents normal communication or suspicious behavior. Continuous traffic monitoring enables the system to detect cyber threats at an early stage before they can compromise network security.

Traffic Analyzer

After packet acquisition, the captured network traffic is transferred to the Traffic Analyzer module. This component processes raw packet data and extracts meaningful networking information required for intrusion detection. During this stage, the analyzer identifies packet attributes such as source IP address, destination IP address, transport protocol (TCP or UDP), port numbers, packet length, protocol flags, and communication sessions.

The Traffic Analyzer converts the captured packet information into a structured format that can be efficiently processed by the IDS Engine. It also filters duplicate or unnecessary packets and organizes network communication into meaningful sessions. By transforming raw packet data into interpretable information, the Traffic Analyzer prepares the network traffic for accurate threat detection.

Flowchart Explanation

The flowchart illustrates the operational workflow of the proposed Intrusion Detection System from the initial packet capture stage to the final logging process. The execution begins when live network traffic is received from the connected network devices. The Packet Capture Module continuously captures incoming and outgoing packets and forwards them to the Traffic Analyzer.

The Traffic Analyzer extracts relevant information from each packet, including IP addresses, protocol types, port numbers, timestamps, and communication details. The processed information is then transferred to the IDS Engine, where the system applies signature-based, anomaly-based, and threshold-based detection techniques to determine whether the observed network behavior is normal or suspicious.

If no malicious activity is detected, the system continues monitoring network traffic without interruption. However, if suspicious behavior or an intrusion is identified, the IDS Engine immediately activates the Alert System, which generates warning notifications for the network administrator. Simultaneously, detailed information about the detected intrusion is stored in the Storage Module for future analysis and digital forensic investigations.

The entire process operates continuously in real time, ensuring uninterrupted network monitoring, timely intrusion detection, rapid alert generation, and comprehensive event logging. This integrated architecture enables the proposed Network Traffic Monitoring and Intrusion Detection System to provide effective cybersecurity protection while supporting digital forensic analysis.

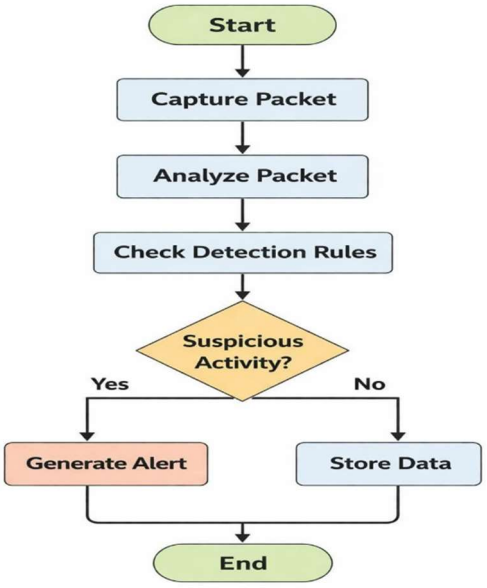

Figure 2 : Flowchart of the Proposed Intrusion Detection System (IDS)

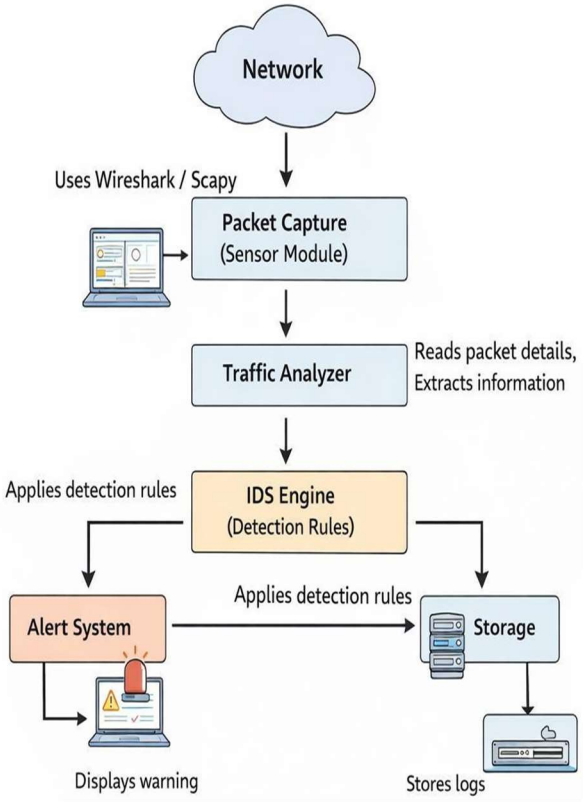

Figure 3 : Overall System Design of the Network Traffic Monitoring and Intrusion Detection System (IDS)

6.2 Software Requirements

Python

Python serves as the primary programming language for developing the Intrusion Detection System due to its simplicity, flexibility, and extensive support for networking and cybersecurity applications. Python offers numerous libraries that simplify packet processing, protocol analysis, real-time monitoring, and data manipulation. Its object-oriented programming capabilities and cross-platform compatibility make it an ideal choice for implementing network security applications. In the proposed system, Python is responsible for coordinating packet capture, processing network traffic, applying detection rules, generating alerts, and maintaining event logs.

Scapy

Scapy is a powerful Python-based packet manipulation library that plays a central role in the proposed IDS. It provides advanced packet sniffing capabilities, allowing the system to capture live network traffic directly from the network interface. Scapy extracts detailed packet information, including source and destination IP addresses, port numbers, transport protocols, packet headers, timestamps, and payload data. It also supports packet inspection, protocol analysis, packet modification, and custom packet generation, making it highly suitable for network traffic monitoring and intrusion detection. The captured packet information is forwarded to the IDS engine for security analysis.

Wireshark

Wireshark is an open-source network protocol analyzer used for monitoring, capturing, and analyzing network traffic in real time. It provides a graphical interface that displays detailed packet-level information, allowing users to inspect communication between network devices. Wireshark assists in validating the operation of the proposed IDS by enabling visualization of captured packets and verification of intrusion detection results. It supports hundreds of communication protocols and offers advanced filtering capabilities that simplify network troubleshooting, protocol analysis, and digital forensic investigations.

Operating System

The proposed Intrusion Detection System can be implemented on commonly used operating systems such as Microsoft Windows or Linux. These operating systems provide stable networking environments, support packet capture drivers, and allow the installation of Python, Scapy, Wireshark, and other required software components. The operating system also provides access to network interfaces required for packet sniffing and real-time traffic monitoring.

Python Package Manager (pip)

Python Package Manager (pip) is used to install and manage the external libraries required for the project. It enables easy installation of Scapy and other Python packages necessary for packet processing and network analysis. Proper installation and configuration of these packages ensure that the IDS functions correctly during execution.

Together, Python, Scapy, Wireshark, the operating system, and supporting software packages provide a complete software environment for implementing the proposed Network Traffic Monitoring and Intrusion Detection System.

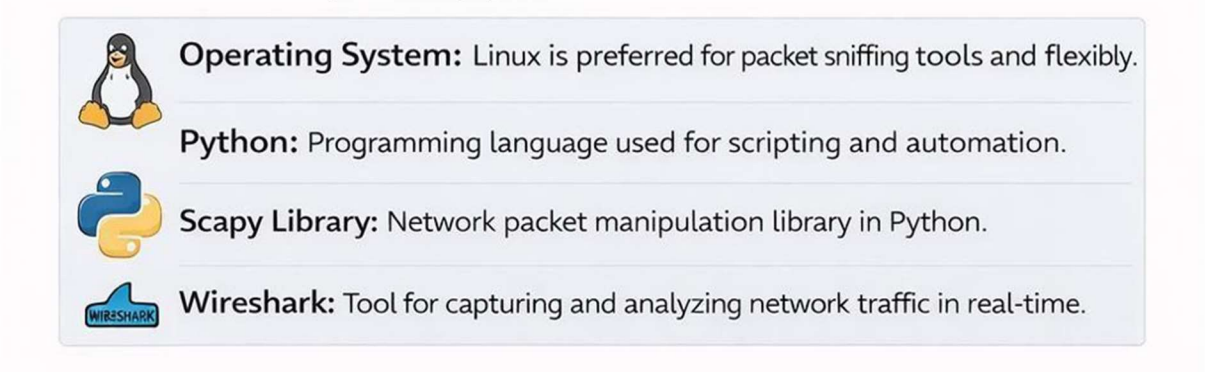

Figure 4: Software Requirements for the Proposed IDS (Python, Scapy, and Wireshark)

Conclusion

In this project, a **Network Traffic Monitoring and Intrusion Detection System for Digital Forensics** was successfully designed and implemented to enhance network security and support digital forensic investigations. The proposed system integrates real-time network traffic monitoring, packet analysis, intrusion detection techniques, alert generation, and secure log storage to identify and analyze cyber threats effectively. By combining signature-based and anomaly-based detection methods, the system is capable of detecting both known attack patterns and

previously unknown network anomalies, thereby improving the overall accuracy and reliability of intrusion detection.

The implementation demonstrates how network packets can be captured, processed, and analyzed in real time to identify suspicious activities such as port scanning, denial-of-service attacks, unauthorized access attempts, and abnormal communication patterns.

Although the proposed system provides significant improvements over conventional network monitoring approaches, certain challenges remain. Handling large-scale network traffic, minimizing false-positive detections, analyzing encrypted communications, and adapting to sophisticated cyber threats continue to be important research areas. Despite these limitations, the proposed Network Traffic Monitoring and Intrusion Detection System establishes a strong foundation for developing advanced intrusion detection and digital forensic solutions. Overall, the project demonstrates the importance of integrating continuous network monitoring, intelligent intrusion detection, real-time alert generation, and forensic evidence collection to create a secure, reliable, and efficient cybersecurity environment.

Future Scope

The future scope of the proposed **Network Traffic Monitoring and Intrusion Detection System** involves incorporating advanced technologies to improve detection performance, scalability, and forensic capabilities. Machine learning and artificial intelligence algorithms can be integrated to automatically learn network behavior, detect sophisticated cyber attacks, reduce false-positive alerts, and improve the identification of previously unknown threats. These intelligent techniques can significantly enhance the adaptability and accuracy of intrusion detection systems in dynamic network environments.

Future enhancements may also include implementing the system on hardware platforms such as **Field Programmable Gate Arrays (FPGAs)** and **Application-Specific Integrated Circuits (ASICs)** to achieve faster packet processing, lower latency, and real-time intrusion detection for high-speed networks. Additional improvements may focus on analyzing encrypted network traffic without compromising user privacy, integrating advanced threat intelligence, implementing secure cloud-based log storage, and employing blockchain technology to ensure the integrity and authenticity of forensic evidence. The system can also be enhanced with automated incident response mechanisms, predictive threat analysis, and centralized security management to provide comprehensive protection against evolving cyber threats. Overall, the proposed system has significant potential to evolve into a scalable, intelligent, and highly efficient solution for modern network security, cybersecurity operations, and digital forensic investigations.

References

[1] R. Zhang, “A Hybrid Intrusion Detection System Based on Machine Learning Techniques for Network Security,” *IEEE Access*, vol. 11, pp. 45231–45245, May 2023.

[2] H. Zhao, “Graph Neural Network-Based Intrusion Detection for Internet of Things Networks,” *IEEE Access*, vol. 11, pp. 67890–67905, Aug. 2023.

[3] Y. Zhou, “Deep Learning-Based Network Intrusion Detection Using CNN-LSTM Model,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1345–1358, Jun. 2023.

[4] A. Kumar, “Real-Time Network Traffic Monitoring and Intrusion Detection Using Machine Learning,” *International Journal of Network Security*, vol. 25, no. 4, pp. 512–520, Jul. 2023.

[5] S. Chen, “An Efficient FPGA-Based Intrusion Detection System for High-Speed Networks,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 32, no. 1, pp. 85–97, Jan. 2024.

[6] P. Singh, “Digital Forensics Framework for Network Traffic Analysis and Cybercrime Investigation,” *IEEE Access*, vol. 12, pp. 10234–10250, Feb. 2024.

[7] M. Ali, “Anomaly-Based Intrusion Detection System Using Artificial Intelligence Techniques,” *IEEE Access*, vol. 12, pp. 22345–22360, Mar. 2024.

[8] T. Nguyen, “Cloud-Based Intrusion Detection System for Scalable Network Security,” *IEEE Transactions on Cloud Computing*, vol. 12, no. 2, pp. 456–468, Apr. 2024.

[9] K. Patel, “ASIC Implementation of High-Speed Pattern Matching for Intrusion Detection Systems,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 3, pp. 765–770, Mar. 2025.

[10] L. Wang, “AI-Driven Network Intrusion Detection for Next-Generation Communication Systems,” *IEEE Access*, vol. 13, pp. 55678–55692, Jan. 2025.