Chapter 1 Introduction The rapid expansion of the Internet has resulted in the widespread use of computer networks for various daily activities.Additionally, IDS lacks the capability to execute essential actions upon detecting an attack, exhibits inefficiency in processing encrypted packets, tends to generate elevated false positives, and remains vulnerable to protocol-based attacks.Network sensors further enhance the efficiency of IDS by analyzing audit trails from multiple hosts, ensuring thorough examination of each event for intrusion detection purposes [5].1.4 Significance Machine learning-based Network Intrusion Detection Systems (NIDS) provide improved detection accuracy, adaptability, reduced false positives, efficient resource utilization, automation, and scalability.Additionally, ML-based NIDS prioritize alerts based on severity levels, automate threat detection and response processes, and are well-suited for organizations of varying sizes.Nonetheless, it is constrained by certain limitations, including the inability to instantaneously prevent or thwart attacks, necessitating integration with complementary security mechanisms such as Intrusion Prevention Systems.Signature-based IDS identify known attack patterns by matching against predefined signatures, while anomaly-based systems, also referred to as heuristic systems, construct models of normal behavior and flag deviations from this baseline.Attackers often aim to identify loopholes and gather information for successful attacks, while defenders monitor network activities to reduce abnormal behaviors, often concealing their identities during observation [1].Figure 1.2 Classification of IDS [3] 1.2 Statement of the problem Network Intrusion Detection Systems (NIDS) play a vital role in addressing computer and network security threats, as traditional intrusion prevention systems such as encryption and firewalls may not provide sufficient protection.This growth has also led to an increase in network attacks that exploit vulnerabilities to disrupt legitimate operations, such as device malfunctions, overloading, and malicious scanning.Network security is a critical research area that utilizes tools like firewalls, antivirus software, and intrusion detection systems (IDS) to protect networks and their assets.ML algorithms can improve detection accuracy by analyzing large amounts of network data and identifying complex patterns.1.6 Scope The Network Intrusion Detection System (NIDS) is a network security mechanism that leverages machine learning algorithms for the detection and mitigation of network intrusions.The NIDS operates in a continuous monitoring mode, promptly notifying security personnel upon detecting anomalies in network traffic.The first path involves an anomaly-based detector that creates activity profiles, detects anomalies, and subsequently generates a report.With the evolution of switching technologies, vendors have introduced port-mirroring techniques to replicate all network traffic to the NIDS.Figure 1.1 NIDS [3] Figure 1.2 illustrates the classification of Intrusion Detection Systems (IDSs) based on various criteria.Given the inherent vulnerabilities in computer networks, the implementation of a NIDS is crucial for mitigating potential attacks.These systems analyze extensive amounts of network data, enabling the identification of malicious activity patterns with greater precision compared to traditional rule-based systems.It gathers network traffic data, processes it iteratively, and employs machine learning methodologies to pinpoint pertinent features.Furthermore, it offers logging and reporting functionalities to adhere to regulatory mandates and industry standards.An Intrusion Detection System (IDS) serves as a tool for scrutinizing network packets to identify and assess attacks.These systems learn to recognize anomalies or aberrant behavior, enabling administrators to classify previously unidentified behavior as

acceptable [7].This project focuses on developing a NIDS based on machine learning (ML) techniques to prevent and mitigate network attacks.1.1 Background As illustrated in Figure 1.1, Network Intrusion Detection Systems (NIDS) are intelligent devices that passively examine network traffic.They can be implemented as hardware or software-based solutions and can be deployed across various network mediums.Positioned strategically within networks, NIDS monitor and analyze network traffic, comparing it against known attack patterns.1.3 Justification Network Intrusion Detection Systems (NIDS) are crucial for protecting computer networks from cyber threats.ML-based NIDS can reduce false alarms, anomalies, and the workload on security staff.They are effective in managing large networks, continuously updating their knowledge, and speeding up response times by automating the detection process.These models are trained utilizing labelled data and assessed based on metrics such as accuracy, precision, recall, and F1-score.Network security tools play a crucial role in identifying vulnerabilities and collecting statistics to prevent such attacks.Cisco, for example, utilizes Switched Port Analyzer functionality to enable this capability.NIDS can operate using signature-based or anomaly-based detection systems, distinguishing between benign and malicious traffic.A network-based IDS monitors the entire network environment, scrutinizing all incoming and outgoing packets.Machine learning (ML) offers a promising solution to enhance NIDS capabilities.Raw events enter the E section, which forwards them to the three components: A, S, and C. Analysis performs analysis on events, producing high level events, which go to the countermeasure section.The second path entails a signature-based detector that matches patterns based on security rules and generates alerts accordingly.Network IDS (NIDS) continuously monitors network traffic for malicious behavior [2].For example, deploying a NIDS on firewall subnets can help identify potential firewall breaches [3].With respect to the analysis strategy, IDSs can be classified as anomaly-based or misuse-based.Regarding the response mechanism, IDSs can be characterized as either active or passive.In terms of architecture, IDSs can be classified as centralized or distributed.Lastly, in terms of decision-making processes, IDSs can be categorized as collaborative or independent.Key design concepts, including machine learning, are essential in enhancing the effectiveness of NIDS [4].This comprehensive data analysis enables the detection of potential network vulnerabilities.This project is dedicated to developing a network IDS utilizing machine learning techniques.It dynamically adjusts to changing threats and network conditions, ensuring scalability and optimal performance.Consequently, the integration of IDS with other security mechanisms is imperative [6].1.8 Definition of terms Figure 1.3 shows IDS four components: Events (E), Analysis(A), Storage(S), and Countermeasures (C).Figure 1.3 Model of Intrusion Detection System [7] Intrusion Detection Systems (IDS) can be categorized as either Signature-based or anomaly-based systems.As illustrated in Figure 1.4, incoming network traffic can undergo two distinct paths.It will then outline the objectives, limitations, and definitions of the project.Upon detecting an attack, the NIDS generates an alert that is sent to the network administrator.Traditional methods, such as rule-based or signature-based approaches, struggle to keep up with evolving attack techniques.1.7 Limitations and delimitations This project encounters several constraints.They can also adapt to new threats by learning from different attack patterns and behaviors.1.5 Objectives The main objectives of this project can be listed as follows.Survey previous work on NIDS.Measuring the performance and accuracy of NIDS.This

chapter will provide background information on the project, followed by a discussion of the problem statement and its significance and justification. In terms of the information source, IDSs can be categorized as either host-based or network-based. Building an ML-based NIDS. Understanding how NIDS work. Actions are performed from C section. 1.2.3.4. a report.