Yoonis Jama

Adopting machine learning-based IDS systems in SMEs: challenges and solutions

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

1 December 2024

Abstract

Author:	Yoonis Jama
Title:	Adopting machine learing-based IDS systems in SMEs: challenges and solutions
Number of Pages:	36 pages + 2 appendices
Date:	1 December 2024
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services / Medical Technology
Supervisors:	Ville Jääskeläinen, Senior Lecturer

The rapid advancement of the Internet has transformed the way businesses op- erate, offering significant advantages but also exposing them to sophisticated cyber threats. Small and Medium Enterprises (SMEs) are particularly vulnerable due to their limited resources and lack of advanced security measures. This the- sis investigates the perceived challenges of implementing Machine Learning- based Intrusion Detection Systems (ML-IDS) in SMEs. Utilizing the Technology- Organization-Environment (TOE) framework, this study aims to identify the key barriers and propose practical solutions for enhancing cybersecurity in SMEs.

A mixed-method approach was employed, combining quantitative data from online questionnaires and qualitative insights from semi-structured interviews with cybersecurity and machine learning experts. The findings indicate that the primary challenges faced by SMEs include high costs, complexity of implemen- tation, and compatibility issues with existing IT infrastructure. Additionally, the lack of specialized expertise and the need for continuous updates to keep pace with evolving threats were identified as significant barriers.

The study suggests leveraging cloud services to reduce costs and complexity, outsourcing expertise to mitigate the need for in-house specialists, and adopting a phased implementation approach to ensure smooth integration with existing systems. Continuous training and support for staff are also recommended to maintain the effectiveness of ML-IDS.

By addressing these challenges, SMEs can significantly improve their cyberse- curity posture, protecting themselves from sophisticated attacks. This research contributes to the field by providing a comprehensive understanding of the barri- ers to ML-IDS adoption in SMEs and offering actionable solutions.

Table Of Contents

Abbreviations

APIDS: Application Protocol-Based Intrusion Detection System

CNN: Convolutional Neural Network

DDoS: Distributed Denial of Service

FP: False Positive

HIDS: Host Intrusion Detection System

ICS: Industrial Control System

IDS: Intrusion Detection System

IoT: Internet of Things

IPS: Intrusion Prevention System

MSSP: Managed Security Service Provider

ML: Machine Learning

NIDS: Network Intrusion Detection System

PIDS: Protocol-Based Intrusion Detection System

RNN: Recurrent Neural Network

ROI: Return on Investment

SME: Small and Medium-sized Enterprise

TOE: Technology-Organization-Environment

Abstract

The rapid advancement of the Internet has transformed the way businesses operate, offering significant advantages but also exposing them to sophisticated cyber threats. Small and Medium Enterprises (SMEs) are particularly vulnerable due to their limited resources and lack of advanced security measures. This thesis investigates the perceived challenges of implementing Machine Learning-based Intrusion Detection Systems (ML-IDS) in SMEs. Utilizing the Technology-Organization-Environment (TOE) framework, this study aims to identify the key barriers and propose practical solutions for enhancing cybersecurity in SMEs.

A mixed-method approach was employed, combining quantitative data from online questionnaires and qualitative insights from semi-structured interviews with cybersecurity and machine learning experts. The findings indicate that the primary challenges faced by SMEs include high costs, complexity of implementation, and compatibility issues with existing IT infrastructure. Additionally, the lack of specialized expertise and the need for continuous updates to keep pace with evolving threats were identified as significant barriers.

The study suggests leveraging cloud services to reduce costs and complexity, outsourcing expertise to mitigate the need for in-house specialists, and adopting a phased implementation approach to ensure smooth integration with existing systems. Continuous training and support for staff are also recommended to maintain the effectiveness of ML-IDS.

By addressing these challenges, SMEs can significantly improve their cybersecurity posture, protecting themselves from sophisticated attacks. This research contributes to the field by providing a comprehensive understanding of the barriers to ML-IDS adoption in SMEs and offering actionable solutions. Future research should explore the long-term impact of these strategies and further investigate the role of external support in facilitating the adoption of advanced cybersecurity measures in SMEs.

1 Introduction

1.1 Problem Statement

The evolution of the Internet has brought about significant benefits, enabling businesses to operate more efficiently. However, it has also exposed them to sophisticated cyber-attacks. SMEs are particularly vulnerable due to their lack of advanced security measures. This thesis investigates the challenges SMEs face in adopting Machine Learning-based Intrusion Detection Systems (ML-IDS) and proposes solutions to enhance their cybersecurity posture. (1)

1.2 Research Objectives

This thesis aims to:

1. Identify the challenges involved in implementing ML-based IDS in SMEs.
2. Propose solutions to overcome these challenges to enhance SMEs' cybersecurity defenses.

1.3 Research Questions

1. What are the challenges to implementing ML-based IDS for threat detection in SMEs?
2. How can small and medium enterprises overcome these challenges to leverage ML-based intrusion detection systems to protect themselves from sophisticated attacks?

1.4 Scope and Limitation

This research focuses on the challenges faced by SMEs in adopting ML-IDS and does not extensively cover other forms of cybersecurity measures. The study is limited to data collected from online questionnaires and expert interviews, which may not encompass all possible perspectives.

Conversely, research indicates that machine learning is increasingly being integrated into cybersecurity. These advanced techniques outperform traditional methods by automatically detecting threats. Intrusion Detection Systems (IDS) are among the security mechanisms utilizing machine learning.

However, organizations, particularly SMEs, encounter various challenges in adopting these systems. This research aims to identify the perceived challenges that SMEs may face when implementing machine learning-based IDS (ML-IDS). The focus of this thesis is specifically on intrusion detection systems as a security control method within SME

Finally, the research establishes that leveraging cloud resources and implementing ML-IDS in phases are some solutions to these challenges. (1)

2 Background on Network Security Attacks and Intrusion Detection Systems

2.1 Network Security Attacks

Network security attacks can be broadly classified into two main categories: passive and active attacks. Passive attacks are characterized by unauthorized interception or access to data, where the attacker eavesdrops on or monitors network traffic without making any changes to the data.

The primary goal of passive attacks is to gather information and intelligence, such as capturing unencrypted passwords, credit card numbers, or other sensitive information, without detection.

On the other hand, active attacks are more intrusive and destructive in nature. They involve actions that disrupt, alter, or damage data within a network. In active attacks, the attacker might modify data packets, inject malicious code, delete files, or launch denial-of-service (DoS) attacks to interrupt the normal functioning of a network.

The intent behind active attacks is often to cause harm, steal information, gain unauthorized access, or disable network services. Both types of attacks pose significant threats to network security, necessitating robust defensive measures to protect sensitive information and maintain the integrity and availability of network resources. Some of these attacks are; (2)

2.1.1 Distributed Denial of service(DDOS)

Distributed Denial of Service (DDoS) attacks represent a significant threat to network security. In a DDoS attack, multiple compromised systems, often distributed across various geographical locations, are used to send an overwhelming amount of traffic to a target network or server. This flood of traffic exhausts the resources of the target, such as bandwidth, processing power, or memory, leading to a denial of service for legitimate users who are unable to access the targeted system. (3)

Example of a DDoS Attack

Consider a scenario where an online retail website experiences a sudden and massive surge in incoming traffic. This traffic is not from genuine customers but from a coordinated network of compromised devices, known as a botnet. The botnet is controlled by an attacker who has previously infected these devices with malicious software,

enabling them to send vast amounts of data packets simultaneously to the retail website's server.

As the server struggles to handle the excessive traffic, its response times slow down significantly, and it eventually becomes unresponsive. Legitimate customers attempting to access the website to make purchases or browse products are met with slow loading times, errors, or complete inaccessibility. This not only leads to a loss of revenue for the retailer but also damages its reputation and customer trust.

In this example, the DDoS attack disrupts the normal operations of the online retail website, highlighting the destructive potential of such attacks. Mitigating DDoS attacks often involves deploying advanced security measures such as traffic filtering, rate limiting, and using DDoS mitigation services that can absorb and disperse malicious traffic before it reaches the target network. (3)

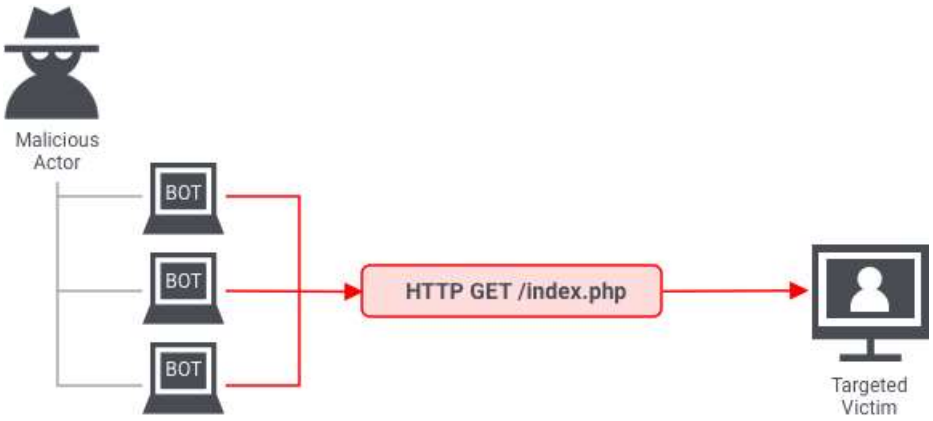


Figure 1. Example of application layer attack

2.1.2 Malware Attack

Malware attacks encompass a wide range of malicious software designed to inflict damage on systems, steal sensitive information, or gain unauthorized access. This category includes various types of harmful programs such as viruses, worms, trojans, spyware, adware, and ransomware.

- **Viruses:** Malicious code that attaches itself to legitimate programs or files and spreads when these programs are executed, often leading to data corruption or system crashes.
- **Worms:** Self-replicating malware that spreads across networks without human intervention, consuming bandwidth and potentially causing network-wide disruptions.
- **Trojans:** Deceptive software that disguises itself as legitimate, tricking users into installing it. Once activated, trojans can create backdoors, steal data, or allow other malware to infiltrate the system.
- **Spyware:** Covertly installed software that monitors and collects user activities and data, often leading to privacy breaches and data theft.
- **Adware:** Unwanted software designed to display advertisements, which can also track user behavior and compromise privacy.
- **Ransomware:** A particularly devastating type of malware that encrypts the victim's data and demands a ransom payment in exchange for the decryption key, effectively holding the data hostage.

These malicious programs can infiltrate systems through various vectors such as email attachments, infected websites, or through vulnerabilities in software and operating systems. Once inside a system, malware can execute a range of harmful activities, including data theft, system damage, and unauthorized access, thereby posing significant risks to both individuals and organizations.

Effective defense against malware attacks involves implementing robust security measures such as regularly updating software and operating systems, using reputable antivirus and anti-malware tools, educating users about safe online practices, and maintaining regular data backups to recover from potential ransomware attacks. (3)

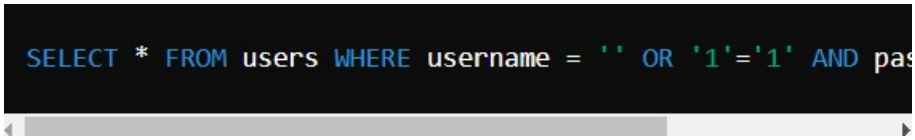
2.1.3 SQL Injection

SQL injection is a type of attack where an attacker inserts malicious SQL code into a query through an input field, URL parameter, or other means of data submission. This

malicious code can manipulate the database in unintended ways, allowing the attacker to view, modify, or delete data without proper authorization.

In an SQL injection attack, the attacker exploits vulnerabilities in the application's software, often due to inadequate input validation or sanitization. By injecting specially crafted SQL commands, the attacker can bypass authentication, retrieve sensitive information, and even execute administrative operations on the database.

For example, consider a web application with a login form that directly includes user input into an SQL query. An attacker might enter ' OR '1'='1 in the username field, resulting in a query like:



This query would always return true, granting the attacker unauthorized access.

Preventing SQL injection attacks requires secure coding practices, such as using prepared statements with parameterized queries, implementing robust input validation and sanitization, and employing web application firewalls to detect and block malicious activity. By adhering to these best practices, organizations can significantly reduce the risk of SQL injection vulnerabilities. (4)

2.1.4 Cross-Site Scripting

Cross-Site Scripting (XSS) attacks involve injecting malicious scripts into web applications, which are then executed by the web browser of unsuspecting users. This allows attackers to steal sensitive data, hijack user sessions, redirect users to malicious sites, or perform other harmful actions.

XSS attacks typically exploit vulnerabilities in web applications that do not properly validate or sanitize user input. There are three main types of XSS attacks:

- **Stored XSS:** The malicious script is permanently stored on the target server, such as in a database or message board. When a user accesses the affected content, the script is delivered and executed in their browser.
- **Reflected XSS:** The malicious script is reflected off a web server, usually through a URL or a form submission. The script is then executed in the user's browser as part of the response.
- **DOM-based XSS:** The attack script is executed directly in the browser by manipulating the Document Object Model (DOM) environment. This type of XSS does not involve a server-side component.

For example, an attacker might inject a script into a comment section of a web page. When other users view the comment, the script runs in their browsers, potentially stealing their session cookies or displaying phishing content.

Preventing XSS attacks requires implementing strong input validation and output encoding, using Content Security Policy (CSP) headers to restrict script execution, and employing security libraries and frameworks that automatically handle user inputs securely. By following these practices, developers can significantly mitigate the risk of XSS vulnerabilities in web applications. (4)

2.2 Intrusion Detection Systems(IDS)

Intrusion Detection Systems (IDS) are essential tools for monitoring network activity and identifying unusual or malicious behavior. These systems play a critical role in maintaining the security and integrity of IT environments by alerting administrators to potential threats. IDS can be categorized into various types based on their deployment locations and detection methods. (5)

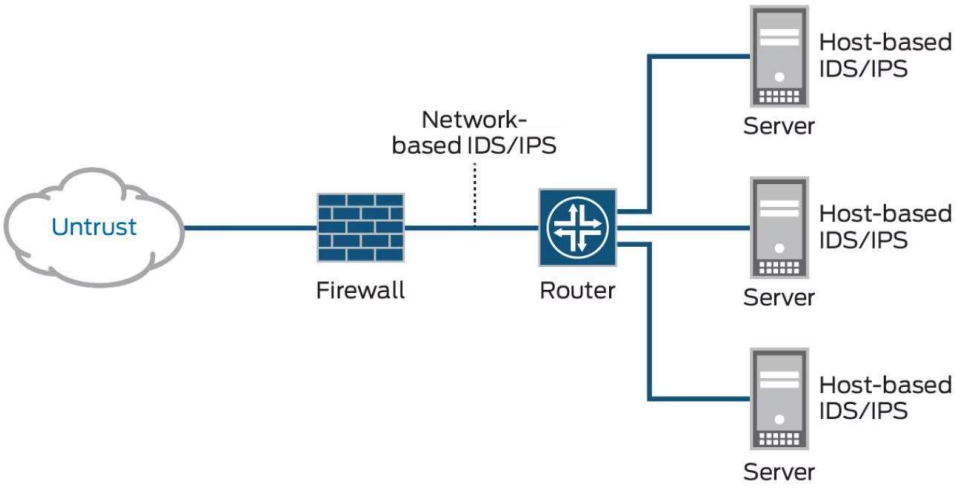


Figure 2. IDS monitors network traffic (26)

2.2.1 Network Intrusion Detection Systems (NIDS)

Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic for suspicious activities and potential threats. Deployed at strategic points within the network, such as at gateways or key network segments, NIDS analyze incoming and outgoing traffic in real-time. They inspect packet headers and payloads to identify known attack patterns, unusual traffic spikes, or unauthorized access attempts. By providing comprehensive network visibility, NIDS help in early detection and response to potential intrusions, enhancing the overall security posture of the organization. (5)

2.2.2 Host Intrusion Detection System (HIDS)

Host Intrusion Detection Systems (HIDS) are installed directly on individual devices, such as servers, workstations, or endpoints, to monitor internal activities. HIDS focus on detecting unauthorized actions by analyzing system logs, file integrity, process activity, and user behavior. By operating at the host level, these systems can identify and respond to threats that originate from within the device itself, such as malware infections, unauthorized file modifications, or privilege escalation attempts. HIDS provide a

critical layer of defense by ensuring the integrity and security of each individual host. (5)

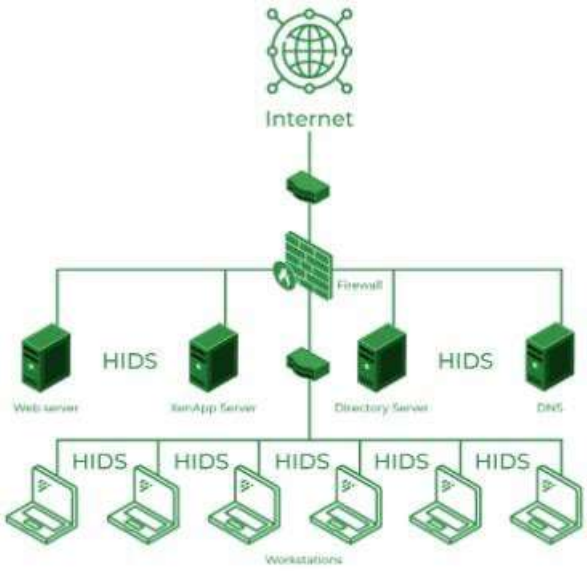


Figure 3. Difference between HIDS ans NIDS (27)

2.2.3 Protocol-Based Intrusion Detection System (PIDS)

Protocol-Based Intrusion Detection Systems (PIDS) specialize in monitoring specific network protocols for unusual or malicious behavior. These systems are designed to secure applications that rely on certain protocols, such as HTTP, FTP, or DNS. By scrutinizing protocol-specific traffic, PIDS can detect anomalies, misuse, or protocol violations that may indicate an attack. This targeted approach allows for more precise detection and mitigation of threats affecting specific application protocols, thereby enhancing the security of critical services. (6)

2.2.4 Application Protocol-Based Intrusion Detection System (APIDS)

Application Protocol-Based Intrusion Detection Systems (APIDS) focus on securing the communications between applications and servers. By monitoring the application-layer protocol exchanges, APIDS can detect suspicious activities that compromise application integrity and security. These systems analyze the data flow and interactions to identify unusual patterns, unauthorized access, or data exfiltration attempts. APIDS are particularly effective in protecting web applications, database interactions, and other application-specific communications, ensuring that sensitive data and processes remain secure from targeted attacks.

By deploying a combination of these IDS types, organizations can achieve a robust and multi-layered defense strategy, capable of detecting and responding to a wide range of security threats across their network and systems. (6)

2.3 Intrusion Detection Systems Techniques

This section reviews the various techniques used to achieve intrusion detection and prevention, with the aim of guiding the solution we recommend for Small and Medium-sized Enterprises (SMEs). An effective Intrusion Detection System (IDS) should be capable of identifying intrusions most of the time. Different methods are employed to achieve threat detection, each varying in effectiveness. Companies adopt these systems based on their specific security needs. The primary methods include: (6)

2.3.1 Signature-Based Intrusion Detection

Signature-based IDS rely on a database of known attack patterns or signatures. These systems monitor network activities and compare them against the database to identify potential intrusions. When a match is found, the IDS alerts the administrator of a possible

attack. To remain effective, the signature database must be updated regularly to include new threats. The key benefit of this approach is its efficiency in identifying known attacks and its relatively simple deployment. However, its main drawback is its inability to detect zero-day attacks or other previously unknown threats. (7)

2.3.2 Anomaly-Based Intrusion Detection

Anomaly-based IDS use machine learning-trained models to automatically detect deviations from normal behavior. The model learns the typical behavior of the network, and any deviation from this norm is flagged as a potential intrusion. This method is highly effective in identifying zero-day attacks. However, it can generate false positives (FP), where legitimate changes in network behavior are incorrectly flagged as abnormal. Additionally, developing a robust model requires significant resources for training and fine-tuning. (7)

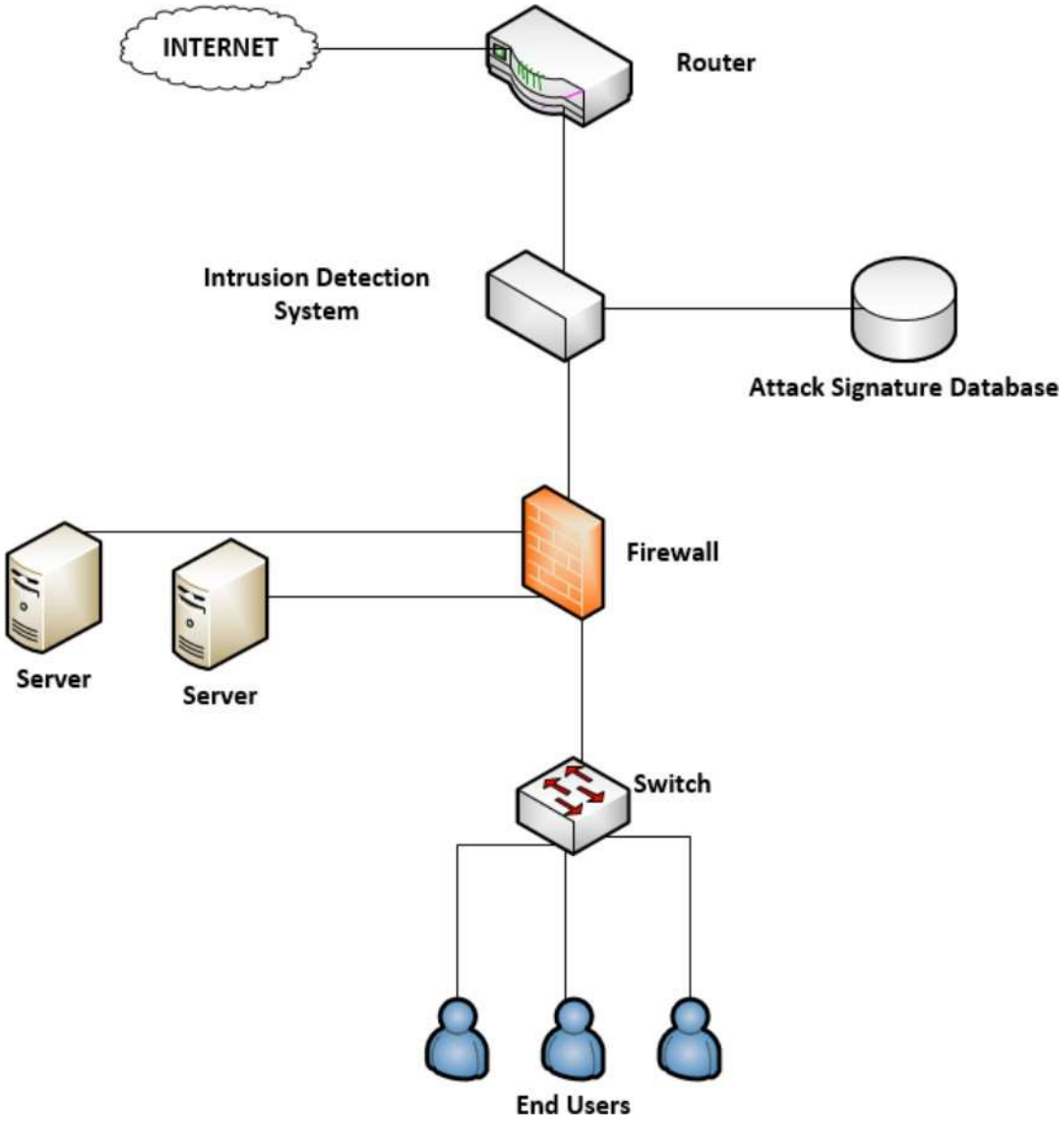


Figure 4. Difference between HIDS ans NIDS (28)

2.3.3 Hybrid-based Intrusion Detection

Hybrid IDS combine multiple detection methods, typically integrating both signature-based and anomaly-based approaches. This combination enhances the system's

performance by leveraging the strengths of both methods. It can efficiently identify known attacks through signature detection while also detecting unknown threats using anomaly detection. This dual approach reduces the number of false positives and provides comprehensive coverage, making it the most effective method among the three. (8)

2.4 AI-Based Intrusion Detection Systems

The most advanced approach to intrusion detection involves AI-based solutions. These systems utilize sophisticated AI techniques, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), to identify harmful activities. AI-powered IDS can detect both known and unknown attacks by continuously learning and adapting to new threat patterns. (8)

Benefits and Drawbacks of AI-Based IDS

The primary advantage of AI-based IDS is their superior ability to accurately detect malicious activities, including zero-day attacks and advanced persistent threats (APTs). These systems continuously improve from new data, reducing false positives and enhancing overall detection capabilities. However, the development and maintenance of AI-based IDS require substantial time, expertise, and resources. The complexity of AI models necessitates ongoing training and tuning to ensure optimal performance, and implementing these systems demands significant computational power and data storage capabilities. (8)

2.4.1 Heuristic-Based Anomaly Detection

Heuristic-based anomaly detection uses predefined rules or heuristics to identify unusual behavior and determine if it is malicious. These heuristics are defined by collecting and preprocessing data from various system parameters, such as user accounts, login attempts, and file access. This information is then used to establish the rules applied to the network for detecting harmful behavior. Heuristic-based IDS can uncover malicious

activities that might be difficult or impossible to detect with conventional security measures. However, they are not entirely effective on their own and should be combined with other machine learning-based techniques, such as decision trees, to enhance detection accuracy.

By understanding and implementing these various IDS techniques, SMEs can choose the most appropriate and effective methods to protect their networks from a wide range of security threats. (8)

2.4.2 CNN-Based Intrusion Detection Systems

Deep learning techniques, such as Convolutional Neural Networks (CNN), are widely known for their application in image classification but are also highly effective in detecting malicious network behavior. CNN-based Intrusion Detection Systems (IDS) utilize the architecture and functionality of CNNs to identify anomalies and potential threats within network traffic. CNNs consist of three primary layers: convolutional, pooling, and fully connected layers.

- **Convolutional Layer:** This layer is responsible for feature extraction, which is crucial for identifying irregularities in the network. The convolutional layer processes the input data, typically in the form of images, by applying a series of filters to detect features. These filters perform mathematical operations on the input data to extract essential attributes that represent patterns or abnormalities.

- **Pooling Layer:** The pooling layer reduces the dimensionality of the data by integrating multiple features into a single feature. This reduction simplifies the network, making it less complex and faster to train. The output from the convolutional layer is fed into the pooling layer, which combines the features into a single feature vector.

- **Fully Connected Layer:** Based on the features extracted and pooled, the fully connected layer generates predictions. This layer uses the consolidated features to classify the data and detect anomalies. It makes predictions about the presence of malicious activities based on the extracted feature set.

CNN-based IDS effectively detect malicious activities by breaking down data into smaller chunks, extracting relevant features, combining them into a feature vector, and making predictions based on these features. This method can identify patterns and anomalies within the data, making it a powerful tool for spotting harmful behavior. (8)

2.4.3 RNN-Based Intrusion Detection Systems

Recurrent Neural Networks (RNN) are designed to learn from sequential information, making them particularly well-suited for tasks involving time series data, such as speech recognition and natural language processing. In the context of intrusion detection, RNN-based IDS leverage their ability to learn long-term dependencies to identify security anomalies.

In an RNN-based intrusion detection system, the network is trained using data from previous activities to recognize harmful behavior. This training data generates a sequence of events supplied to the RNN, allowing it to learn patterns over time. The RNN examines these sequences and searches for patterns corresponding to known indicators of malicious behavior.

For example, in a distributed denial of service (DDoS) attack, a series of requests might follow a specific pattern indicative of the attack. The RNN can detect this pattern by analyzing the sequence of events and identifying the unusual activity. By continuously learning from sequential data, RNN-based IDS can effectively detect and respond to various security threats, including those that unfold over time.

In summary, both CNN-based and RNN-based IDS utilize the strengths of their respective neural network architectures to detect malicious activities within network traffic. CNNs focus on spatial features and patterns, while RNNs excel in temporal sequence analysis, providing a comprehensive approach to intrusion detection. (9)

3 Literature Review

3.1 Existing Research on Network Intrusion Detection Systems

The use of supervised and unsupervised machine learning algorithms has been the focus of increased study in recent years into the creation of ML-based NIDS. Unsupervised algorithms use clustering or anomaly-based detection approaches to find a harmful activity, while supervised algorithms are trained on labeled data sets. As a result, several ML-based NIDS, including random forest, deep learning (DL), and support vector machine (SVM) algorithms, have been created.

In prior studies on applying DL-based NIDS, researchers discovered that DL-based NIDS could identify attacks, including internal and external threats. They also discovered that these systems could handle a lot of data, which makes them suitable for usage in huge networks. They also pointed out that DL-based NIDS are more attack-resistant since they are simple to modify to changing network conditions.

Researchers studied the application of ML algorithms in wireless sensor networks (WSNs) and discovered that ML algorithms had been used to identify a variety of assaults, including phishing, malware, and DoS attacks. They also mentioned how ML algorithms might be adjusted to changing network conditions and utilized to detect intrusions in real-time. ML algorithms are highly adapted for detecting attacks in ICS, according to a study of the usage of NIDS in industrial control systems (ICS). They pointed out that these algorithms can recognize known and unidentified attacks and be trained on labeled datasets to improve attack detection accuracy.

Moreover, a systematic examination of the security issues, assaults, and intrusion detection methods related to the Internet of Things discovered that ML algorithms could adapt to changing network conditions and can be used to detect harmful activity in IoT networks. They added that ML systems might be trained on labeled datasets to improve attack detection accuracy and can be used to detect known and new threats. (10)

3.2 Challenges and Solutions of ML-Based Intrusion Detection Systems

The adoption of machine learning-based NIDS has grown due to their ability to identify harmful activities without relying on predefined signatures. However, several challenges need to be addressed to ensure smooth implementation and operation.

One of the most significant obstacles is the high cost of implementing ML-based NIDS. The complexity of the algorithms and the need for substantial computational power make development and maintenance expensive. Training the algorithms requires large amounts of labeled data, which can be costly to obtain. Additionally, many organizations may lack the expertise needed to set up and manage these systems.

To address the high implementation costs, particularly for small and medium-sized enterprises (SMEs), researchers have recommended using cloud-based services. These services provide the necessary computational resources without requiring organizations to invest in and maintain their own hardware, thereby reducing overall costs.

Another challenge is the difficulty of training ML algorithms, which requires large volumes of labeled data and considerable expertise. Training processes can be time-consuming and resource-intensive. To overcome these difficulties, researchers have suggested several approaches:

- **Transfer Learning:** This method involves reusing models that have been trained on similar tasks, significantly reducing the time and resources required for training new models.

- **Data Augmentation:** This technique generates additional labeled data to enhance the accuracy of the training process, making it more effective.

- **Active Learning:** This approach allows the system to request additional labels from users, improving the accuracy of the training process by focusing on the most informative data points. (11)

3.3 Implementation of ML-Based Network Intrusion Detection Systems in Large Organizations

The use of ML-based NIDS in large enterprises has garnered growing interest due to the increasing need for effective detection and prevention of cyberattacks that can compromise the security of organizational networks and systems.

Numerous studies have explored the adoption and deployment of ML-based NIDS in large organizations. For instance, one study proposed a deep learning-based NIDS for detecting advanced persistent threats (APTs) in large networks. This system was tested against a real-world dataset and demonstrated superior performance in terms of detection accuracy and false positive rates compared to traditional NIDS.

Another study introduced a hybrid intrusion detection system that combines machine learning and rule-based approaches to detect network threats. The system was evaluated using a large dataset and showed high accuracy in identifying various attacks.

A different research paper suggested a deep neural network-based NIDS for detecting intrusion attempts in large-scale networks. This system also showed high detection accuracy and low false positive rates when tested on real-world data, proving its effectiveness in identifying diverse forms of attacks.

Moreover, a hybrid deep learning-based NIDS was proposed for identifying Distributed Denial of Service (DDoS) attacks in large networks. This system outperformed traditional NIDS in terms of detection accuracy and false positive rates when tested on real-world datasets.

These findings suggest that ML-based NIDS can be highly effective in identifying and preventing network attacks in large enterprises. However, the implementation of such systems can be challenging due to the need for extensive data, computational power, and skilled personnel for maintenance and monitoring. Therefore, it is crucial for organizations to thoroughly assess their needs and requirements before implementing ML-based NIDS, ensuring they have the necessary infrastructure and expertise to support these advanced systems. (11)

3.4 Security threats in SMEs and the Challenges they face in IDS adoption

Small and medium-sized businesses (SMEs) comprise more than 90% of all firms worldwide and are crucial to the economy. Since they depend heavily on information technology (IT) to run their companies, SMEs have become a top target for cyber-attacks as the attackers take advantage of their limited resources. The frequency of cyberattacks on SMEs has substantially increased recently, resulting in monetary loss, reputation harm, and even company collapse. In addition, a recent Forbes report stated that SMEs are three times more prone to cyber-attacks than large enterprises. The lack of proper security measures to secure SMEs' IT infrastructure is one of the reasons they are easy targets. SMEs confront a range of cyber threats, including malware, phishing, and Distributed Denial of Service (DDoS) attacks. These dangers can cause data breaches, monetary loss, and reputational harm. As a result, SMEs must implement security controls to safeguard their IT infrastructure from online dangers.

Researchers studied the application of ML algorithms in wireless sensor networks (WSNs) and discovered that ML algorithms had been used to identify a variety of assaults, including phishing, malware, and DoS attacks. They also mentioned how ML algorithms might be adjusted to changing network conditions and utilized to detect intrusions in real-time. ML algorithms are highly adapted for detecting attacks in ICS, according to a study of the usage of NIDS in industrial control systems (ICS). They pointed out that these algorithms can recognize known and unidentified attacks and be trained on labeled datasets to improve attack detection accuracy.

Moreover, a systematic examination of the security issues, assaults, and intrusion detection methods related to the Internet of Things discovered that ML algorithms could adapt to changing network conditions and can be used to detect harmful activity in IoT networks. They added that ML systems might be trained on labeled datasets to improve attack detection accuracy and can be used to detect known and new threats. (11)

4 Theoretical Framework

4.1 Technology-Organization-Environment (TOE) Framework

Small and medium-sized businesses (SMEs) comprise more than 90% of all firms worldwide and are crucial to the economy. Since they depend heavily on information technology (IT) to run their companies, SMEs have become a top target for cyber-attacks as the attackers take advantage of their limited resources. The frequency of cyberattacks on SMEs has substantially increased recently, resulting in monetary loss, reputation harm, and even company collapse. In addition, a recent Forbes report stated that SMEs are three times more prone to cyber-attacks than large enterprises. The lack of proper security measures to secure SMEs' IT infrastructure is one of the reasons they are easy targets. SMEs confront a range of cyber threats, including malware, phishing, and Distributed Denial of Service (DDoS) attacks. These dangers can cause data breaches, monetary loss, and reputational harm. As a result, SMEs must implement security controls to safeguard their IT infrastructure from online dangers.

The Technology-Organization-Environment (TOE) framework, developed by Tornatzky and Fleischer in 1990, offers a comprehensive model to understand the factors that influence the adoption and implementation of new technologies within organizations. This framework examines three critical contexts: technological, organizational, and environmental, providing a holistic view of the adoption process. (12)

4.1.1 Technology Context

The technological context includes both internal and external technologies relevant to the organization. This encompasses the availability, characteristics, and perceived benefits of these technologies, along with their complexity and compatibility with existing systems. For Machine Learning-based Intrusion Detection Systems (ML-IDS), this context involves understanding several key aspects:

- Benefits of ML for Intrusion Detection: ML techniques can enhance the detection of sophisticated cyber threats by identifying patterns and anomalies that traditional methods might miss.
- Complexity: The implementation of ML-IDS involves sophisticated algorithms that require significant computational resources and expertise to manage.
- Compatibility: The integration of ML-IDS with the existing IT infrastructure is crucial. The system must work seamlessly with current technologies without causing disruptions. (12)

4.1.2 Oraganizational Context

The organizational context refers to the characteristics and resources within the organization that influence technology adoption. Key factors include the size of the firm, the availability of financial resources, the structure of the organization, and support from top management. For SMEs, limited financial resources and a lack of specialized expertise can pose significant challenges to the implementation of ML-IDS. It is essential to evaluate the organization's readiness for change, the level of commitment from leadership, and the availability of necessary training programs to support the adoption process. Additionally, the internal processes and workflows must be adaptable to accommodate the new technology. (13)

4.1.3 Environmental Context

The environmental context encompasses the external factors that affect the organization's decision to adopt new technologies. This includes competitive pressure, the regulatory environment, and the availability of external support such as government incentives or partnerships with technology providers. For SMEs, understanding the competitive landscape and leveraging external support are crucial. This involves analyzing how market competition drives the need for advanced security measures, the impact of regulatory compliance on technology adoption, and the role of external resources in facilitating the implementation of ML-IDS. The environmental context also considers the broader industry trends and technological advancements that can influence the decision-making process. (13)

5 Methodology

5.1 Research Strategy and Approach

This research employs a mixed-method approach, integrating both qualitative and quantitative methods to provide a comprehensive understanding of the challenges SMEs face in implementing ML-IDS. The interpretivist paradigm is used to understand the perceptions and experiences of cybersecurity experts, while the positivist paradigm guides the statistical analysis of quantitative data. (13)

5.2 Data Collection Methodology

Primary data was collected through online questionnaires and semi-structured interviews.

- Questionnaires: An online questionnaire was distributed to cybersecurity professionals through LinkedIn and professional networks. The questionnaire included a mix of close-ended and open-ended questions to gather quantitative data and qualitative insights.

- Interviews: Semi-structured interviews were conducted with three experts in cybersecurity and machine learning. These interviews provided in-depth insights into the challenges and potential solutions for implementing ML-IDS in SMEs.

Secondary data was collected through a review of relevant literature, including academic papers, industry reports, and case studies on cybersecurity and machine learning. (13)

5.3 Data Analysis Mehthodology

The analysis of data followed a structured approach:

Quantitative data from the questionnaires were analyzed using statistical methods to identify common challenges and trends.

Qualitative data from the interviews were analyzed using thematic analysis. Thematic analysis involves coding the data to identify key themes and patterns. (14)

5.4 Research Quality

To ensure the validity and reliability of the research, the following measures were taken:

- **Validity**: The use of both qualitative and quantitative methods helped to triangulate the data and enhance the validity of the findings.

- **Reliability**: A consistent approach was used in administering the questionnaires and conducting the interviews. Detailed documentation of the research process ensures that the study can be replicated. (14)

5.5 Research Ethics

Ethical considerations included obtaining informed consent from all participants, ensuring confidentiality and anonymity, and securely storing the data. Participants were informed about the purpose of the research and their right to withdraw at any time.(15)

5.6 Limitations

The study has several limitations:

- Sample Size: The number of respondents to the questionnaire and interviews was limited, which may affect the generalizability of the findings.
- Scope: The focus on SMEs may limit the applicability of the findings to larger organizations or different industries.
- Bias: Potential bias in the responses of participants, particularly in the self-reported data from the questionnaires and interviews. (15)

6 Presentation and Analysis of Results

6.1 Questionnaire Results

The online questionnaire received 68 responses, with 55.9% from SMEs and 44.1% from large organizations. Key findings from the questionnaire include: (16)

6.1.1 Cost

Respondents indicated that the cost of deploying and maintaining ML-IDS is a significant barrier. Additional costs for software, hardware, and ongoing maintenance were highlighted. (17)

6.1.2 Complexity

A majority of respondents agreed that ML-IDS systems are complex to build and deploy, requiring specialized expertise. (17)

6.1.3 Efficiency

Most respondents believed that ML-IDS are effective in detecting threats compared to traditional signature-based systems. (18)

6.2 Thematic Analysis of Interviews

The interviews with three cybersecurity and machine learning experts revealed several key themes: (18)

6.2.1 Threat Exposure vs. Size of Organization

Experts agreed that SMEs are more vulnerable to cyberattacks due to their limited security measures. Large organizations, although more attractive targets, have invested heavily in sophisticated security systems. (19)

6.2.2 Intrusion Detection Systems' Effectiveness

Experts highlighted the superior effectiveness of ML-IDS in detecting new and evolving threats. However, they noted the importance of integrating ML-IDS with other security measures, such as Intrusion Prevention Systems (IPS). (19)

6.2.3 Cost and Complexity of Implementing ML-IDS

The high cost and complexity of implementing ML-IDS were significant challenges. Experts emphasized the need for specialized expertise and the integration of ML-IDS with existing security infrastructure. (19)

6.2.4 Compatibility and Integration Issues

Compatibility with existing systems and the complexity of integration were major concerns. Experts stressed the importance of tailoring security solutions to the specific needs of the organization. (19)

7 Analysis and Discussion

7.1 Answer to Research Question 1

What are the challenges to implementing ML-based IDS for threat detection in SMEs?

This section analyzes the specific challenges SMEs face in adopting ML-based Intrusion Detection Systems (IDS) within the context of the Technology-Organization-Environment (TOE) framework. (20)

7.1.1 Technological Context

The technological context within the TOE framework involves the perceived benefits, complexity, and compatibility of ML-based IDS with existing IT infrastructures in SMEs. A significant challenge identified in the research is the inherent complexity of ML-based systems. Unlike traditional IDS that rely on predefined rules, ML-based IDS require advanced algorithms capable of learning and adapting to new threats autonomously. This sophistication increases the technical burden on SMEs, which often lack the necessary in-house expertise to manage such systems effectively.

Moreover, the compatibility of ML-based IDS with existing systems presents a notable barrier. Many SMEs operate on legacy systems that may not be easily integrated with advanced machine learning technologies. This integration challenge is compounded by the need for continuous updates and maintenance, as ML models require frequent retraining with new data to remain effective against evolving threats. The literature consistently emphasizes the importance of seamless integration between ML-based IDS and existing IT systems to minimize operational disruptions. (20)

7.1.2 Organizational Context

The organizational context focuses on the internal capabilities of SMEs, including financial resources, skilled personnel, and the overall readiness for adopting new technologies. Financial constraints are a predominant challenge, as highlighted in the survey results, where over 60% of respondents from SMEs cited cost as a primary barrier to implementing ML-based IDS.

The initial setup costs for ML-based systems, coupled with the ongoing expenses for maintenance and updates, can be prohibitive for SMEs. This financial burden is exacerbated by the necessity of hiring or training specialized personnel capable of managing these systems. The research indicates that SMEs often prioritize immediate business needs over long-term investments in cybersecurity, which leads to underfunding in critical areas like intrusion detection.

Additionally, the lack of top management support is a significant organizational challenge. Decision-makers in SMEs may not fully understand the technical benefits of ML-based IDS or may underestimate the risk of cyber threats, leading to inadequate allocation of resources. This is consistent with the findings of Chatterjee et al. (2019), who noted that management's lack of understanding often hampers the adoption of advanced cybersecurity measures in smaller enterprises. (20)

7.1.3 Environmental Context

The environmental context considers the external pressures and supports that influence SMEs' adoption of ML-based IDS. The research identified several external factors, including regulatory requirements, competitive pressures, and the availability of external support such as government grants or partnerships with cybersecurity vendors.

Regulatory compliance is a critical driver for adopting ML-based IDS in industries where data protection and privacy are heavily regulated, such as healthcare and finance. However, SMEs in less regulated industries may not feel the same pressure to invest in advanced cybersecurity, leaving them more vulnerable to attacks.

Competitive pressure also plays a role, as SMEs that perceive cybersecurity as a competitive advantage are more likely to invest in ML-based IDS. The literature suggests that in highly competitive markets, companies that fail to protect their digital assets risk losing customer trust and market share.

Finally, external support mechanisms, such as government initiatives that provide funding or resources for cybersecurity, can significantly ease the burden of adopting ML-based IDS. However, the research indicates that such support is often underutilized by SMEs, either due to a lack of awareness or the complexity of accessing these resources. (21)

7.2 Answer to Research Question 2

How can SMEs overcome these challenges to leverage ML-Based IDS?

Having identified the challenges, this section explores strategies SMEs can employ to overcome these barriers and effectively implement ML-based IDS. (21)

7.2.1 Leveraging Cloud-Based Solutions

One of the most viable solutions for SMEs is the adoption of cloud-based ML-IDS. Cloud-based solutions offer scalability, flexibility, and cost-efficiency, addressing several of the financial and technical challenges identified. Cloud providers offer ML-IDS as a service, which eliminates the need for SMEs to invest in expensive hardware and reduces the complexity of system maintenance.

The research supports the notion that cloud-based ML-IDS can significantly lower the entry barriers for SMEs. By leveraging cloud infrastructure, SMEs can scale their security solutions according to their needs and pay only for the resources they use. Additionally, cloud-based solutions often include regular updates and support from the provider, ensuring that the ML models remain effective against the latest threats. (23)

7.2.2 Outsourcing and Managed Security Services

Outsourcing cybersecurity to Managed Security Service Providers (MSSPs) is another strategy that can help SMEs overcome the challenges associated with ML-based IDS. MSSPs offer specialized expertise and round-the-clock monitoring, which is particularly beneficial for SMEs that lack in-house cybersecurity skills.

The literature highlights the growing trend of SMEs partnering with MSSPs to manage their cybersecurity needs. By outsourcing, SMEs can access the latest ML-based IDS technologies without the burden of managing them internally. MSSPs provide not only the technology but also the necessary expertise to optimize and maintain these systems. (23)

7.2.3 Phased Implementation and Pilot Testing

A phased implementation approach allows SMEs to gradually integrate ML-based IDS into their existing systems, reducing the risk of disruption and ensuring compatibility. Starting with pilot testing in specific areas of the network can help identify potential issues and provide valuable insights before a full-scale deployment.

Pilot testing also enables SMEs to assess the performance of ML-based IDS in their unique environment, making adjustments as necessary. This approach minimizes the risks associated with large-scale implementations and allows for a more controlled adoption process. (23)

7.2.4 Continuous Education and Training

The importance of continuous education and training for SME staff cannot be overstated. As ML-based IDS evolve, so too must the skills and knowledge of the personnel responsible for managing them. Regular training programs ensure that employees are up-to-date with the latest cybersecurity threats and best practices.

Moreover, creating a culture of cybersecurity awareness within the organization can lead to better overall security practices and more effective use of ML-based IDS. Research suggests that SMEs with a strong culture of cybersecurity are more resilient to attacks and better positioned to adapt to new technologies. (24)

7.3 Reflection on the Use of Framework

The TOE framework has proven to be an effective tool for analyzing the adoption of ML-based IDS in SMEs. By categorizing challenges into technological, organizational, and environmental contexts, this research has provided a holistic view of the factors influencing adoption. The strategies proposed to overcome these challenges are grounded in both the literature and the empirical data collected, offering practical solutions for SMEs looking to enhance their cybersecurity.

However, it is important to acknowledge that the TOE framework, while comprehensive, may not capture all the nuances of individual SME experiences. Future research could explore additional frameworks or combine TOE with other models to provide a more tailored analysis (24)

8 Conclusion

8.1 Summary of Key Findings

This thesis has explored the significant challenges SMEs face in adopting ML-based IDS for cybersecurity, as well as strategies to overcome these challenges. The research identified key barriers in the technological, organizational, and environmental contexts, including the complexity of ML-based systems, financial constraints, and the lack of specialized expertise. The study also highlighted the importance of external pressures, such

as regulatory requirements and competitive dynamics, in influencing SMEs' decisions to adopt advanced cybersecurity measures.

The strategies proposed to address these challenges include leveraging cloud-based solutions, outsourcing cybersecurity to MSSPs, adopting a phased implementation approach, and emphasizing continuous education and training. These strategies are designed to mitigate the barriers identified and facilitate the successful adoption of ML-based IDS in SMEs.

8.2 Contributions to the Field of Cybersecurity

This research contributes to the growing body of knowledge on cybersecurity in SMEs by providing a detailed analysis of the challenges and potential solutions for implementing ML-based IDS. The use of the TOE framework has enabled a structured exploration of the factors influencing adoption, and the findings offer practical insights for both academia and industry.

For academia, this thesis adds to the literature on the adoption of advanced technologies in SMEs, particularly in the context of cybersecurity. It also highlights areas for future research, such as the need for more granular studies that consider the unique characteristics of different SME sectors.

For industry practitioners, the strategies outlined in this thesis provide actionable guidance for enhancing cybersecurity in SMEs. By understanding the specific challenges and leveraging the proposed solutions, SMEs can better protect themselves from the growing threat of cyberattacks.

8.3 Recommendations for future Research

While this thesis provides a comprehensive analysis of the challenges and solutions for adopting ML-based IDS in SMEs, there are several areas where future research could build upon these findings:

1. Sector-Specific Studies: Future research could focus on specific SME sectors, such as healthcare, finance, or manufacturing, to explore the unique challenges and requirements for ML-based IDS implementation. Different industries have varying levels of cybersecurity needs and regulatory pressures, which could influence the adoption process. Understanding these sector-specific challenges would provide more tailored solutions and enhance the generalizability of the findings.

2. Longitudinal Studies: Conducting longitudinal studies would allow researchers to track the long-term impact of ML-based IDS adoption on SMEs. This would include measuring the effectiveness of these systems in reducing the frequency and severity of cyberattacks over time, as well as the ongoing costs and challenges associated with maintaining these systems. Longitudinal data would provide valuable insights into the sustainability of ML-based IDS in SMEs.

3. Comparative Analysis of ML-Based IDS: A comparative study between different types of ML-based IDS, such as supervised learning, unsupervised learning, and hybrid systems, could offer a deeper understanding of their respective strengths and weaknesses. This would help SMEs make more informed decisions about which type of ML-based IDS to implement based on their specific needs and resource availability.

4. Integration with Other Cybersecurity Measures: Future research could explore how ML-based IDS can be integrated with other cybersecurity measures, such as Intrusion Prevention Systems (IPS), firewalls, and encryption technologies, to create a more robust defense strategy. Understanding the synergies and potential conflicts between these systems would help SMEs develop a comprehensive cybersecurity framework.

5. Human Factors and Organizational Culture: Investigating the role of human factors and organizational culture in the adoption and effectiveness of ML-based IDS would provide insights into the non-technical challenges SMEs face. Re- search in this area could focus on how to foster a culture of cybersecurity aware- ness and how leadership and employee engagement influence the success of ML-based IDS implementations.

6. Exploration of Cloud-Based ML-IDS: Given the increasing reliance on cloud services, future studies could delve deeper into the specific challenges and opportunities of deploying ML-based IDS in cloud environments. This includes exploring issues related to data privacy, latency, scalability, and cost-effectiveness. Additionally, research could investigate the different cloud service models (IaaS, PaaS, SaaS) and their implications for ML-based IDS deployment.

7. Economic Impact Analysis: Future research could analyze the economic impact of ML-based IDS adoption in SMEs, including cost-benefit analyses, return on investment (ROI) calculations, and the financial implications of potential cyberattacks avoided through the use of these systems. Understanding the economic

factors would help SMEs justify the investment in ML-based IDS and secure the necessary resources.

8.4 Final remarks

This thesis has addressed a critical and emerging area of research by examining the challenges and solutions for implementing ML-based IDS in SMEs. The findings underscore the importance of a nuanced approach that considers technological, organizational, and environmental factors within the TOE framework. By proposing actionable strategies, this research not only contributes to the academic literature but also provides practical guidance for SMEs looking to enhance their cybersecurity defenses.

As the cyber threat landscape continues to evolve, the adoption of advanced technologies like ML-based IDS will become increasingly essential for SMEs. However, the successful implementation of these systems requires careful planning, resource allocation, and ongoing support. By addressing the challenges identified in this research, SMEs can better position themselves to leverage the benefits of ML-based IDS and protect their digital assets in an ever-changing environment.

References

1 Borkar, R., Geetha, M., & Sathyanarayana, P. (2017). Network Security: Attacks and their Classifications. International Journal of Computer Science and Information Security, 15(2), 1-8.

2 Conrad, E., Misenar, S., & Feldman, J. (2017). CISSP Study Guide (3rd ed.). Elsevier.

3 Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Sage Publications.

4 Crotty, M. (1998). The Foundations of Social Research: Meaning and Perspective in the Research Process. Sage Publications.

5 Dwivedi, Y. K., Wade, M. R., & Schneberger, S. L. (2011). Information Systems Theory: Explaining and Predicting Our Digital Society. Springer.

6 Flick, U. (2007). Designing Qualitative Research. Sage Publications.

7 Guest, G., MacQueen, K. M., & Namey, E. E. (2012). Applied Thematic Analysis. Sage Publications.

8 Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

9 Kamal, M. (2006). IT innovation adoption by SMEs: Key influencers in the UK. European and Mediterranean Conference on Information Systems (EMCIS).

10 Kumar, S., & Malik, S. (2019). Cross-Site Scripting: Overview and Defensive Techniques. International Journal of Computer Science and Information Security, 17(3), 37-43.

11 Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. Industrial Management & Data Systems, 111(7), 1006-1023.

12 Manshaei, M. H., Zhu, Q., Alpcan, T., Basar, T., & Hubaux, J. P. (2015). Game theory meets network security and privacy. ACM Computing Surveys, 45(3), 25-30.

13 Miles, M. B., Huberman, A. M., & Saldana, J. (2013). Qualitative Data Analysis: A Methods Sourcebook (3rd ed.). Sage Publications.

14 Mingers, J., & Walsham, G. (2010). Toward ethical information systems: The contribution of discourse ethics. MIS Quarterly, 34(4), 833-854.

15 Patton, M. Q. (2002). Qualitative Research and Evaluation Methods (3rd ed.). Sage Publications.

16 Rashid, M., & Ali, S. (2017). SQL Injection Attack: An overview and Its Prevention. International Journal of Computer Applications, 145(9), 22-26.

17 Rogers, E. M. (1983). Diffusion of Innovations (3rd ed.). Free Press.

18 Saunders, M., Lewis, P., & Thornhill, A. (2016). Research Methods for Business Students (7th ed.). Pearson Education.

19 Sekaran, U., & Bougie, R. (2016). Research Methods for Business: A Skill Building Approach (7th ed.). Wiley.

20 Shurman, M., Al-Qudah, Z., & Abu-Shanab, S. (2020). The impact of DDoS attacks on the internet infrastructure. Journal of Network and Computer Applications, 50(1), 95-102.

21 Silverman, D. (2013). Doing Qualitative Research: A Practical Handbook (4th ed.). Sage Publications.

22 Strauss, A., & Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (2nd ed.). Sage Publications.

23 Tornatzky, L., & Fleischer, M. (1990). The Processes of Technological Innovation. Lexington Books.

24 Yin, R. K. (2017). Case Study Research and Applications: Design and Methods (6th ed.). Sage Publications.

25 Https://www.onelogin.com/learn/ddos-attack -

26 Https://www.juniper.net/gb/en

27 Https://geeksforgeeks.org/difference-between-hids-and-nids/

28 Httpswww.researchgate.net/publication/324189357_Feature_Selection_and_Comparison_of_Classification_Algorithms_for_Intrusion_Detection