A LIGHTWEIGHT NETWORK INTRUSION DETECTION SYSTEM FOR SMEs

Homam El-Ta, Mawadah Fahhad , Reeman Abumlha,
Shadan Showman, and Zaina Saab

Department of Cybersecurity, Dar Al-Hekma University, Saudi Arabia

ABSTRACT

Small and medium enterprises (SMEs) face increasing cybersecurity threats but often lack access to practical and affordable intrusion detection solutions. This article proposes a lightweight, modular Network Intrusion Detection System (NIDS) tailored to SME environments, emphasizing low resource consumption, ease of deployment, and scalable functionality. The system integrates signature-based detection with streamlined behavioural analysis to deliver strong threat identification without overwhelming infrastructure or administrative capacity. A structured evaluation framework and comparative benchmarking against existing lightweight IDS solutions demonstrate the system's potential to achieve high detection accuracy, efficient resource usage, and real-time responsiveness. By aligning security capabilities with SME operational realities, the proposed solution aims to bridge a critical gap in cybersecurity resilience, enabling smaller organizations to strengthen their defences and contribute to broader digital ecosystem security.

KEYWORDS

Small-to-Medium Enterprises (SMEs), Intrusion Detection Systems (IDS), Network-Based Intrusion Detection Systems (NIDS), Host-Based Intrusion Detection Systems (HIDS)

1. INTRODUCTION

The rapid evolution of cyber threats continues to outpace advancements in cybersecurity defenses, leaving organizations increasingly vulnerable to sophisticated attacks [1]. While large enterprises possess the resources to maintain robust security postures, small-to-medium enterprises (SMEs) face unique challenges, including constrained budgets, limited technical expertise, and restricted access to affordable solutions [1], [2]. Recent reports reveal that 46% of all cyber breaches impact businesses with fewer than 1,000 employees [3]. Furthermore, the median cost of a ransomware attack has climbed to $26,000, highlighting the severe financial impact on SMEs [4]. Despite these alarming figures, only 14% of SMEs report having formal cybersecurity strategies, highlighting a critical gap in network protection [1].

Given the heightened risks faced by SMEs, solutions that balance affordability, efficiency, and ease of use are urgently needed. Network Intrusion Detection Systems (NIDS) offer a practical approach to achieving robust network security without overburdening limited operational capacities [5]. This article explores the role of lightweight NIDS in addressing SME cybersecurity needs, emphasizing detection mechanisms, resource efficiency, and usability which are key factors for ensuring accessibility in constrained environments [6].

While Intrusion Prevention Systems (IPS) are mentioned briefly for context, the primary focus remains on evaluating the effectiveness of NIDS solutions for SMEs. The article also introduces a

DOI: 10.5121/ijnsa.2025.17306

conceptual lightweight and modular NIDS specifically designed to bridge the shortcomings of existing solutions and offer SMEs a scalable, cost-effective alternative.

This article makes three primary contributions. First, it provides a comprehensive survey of traditional and lightweight NIDS, with a particular focus on detection mechanisms, resource demands, and usability within the context of SMEs. Second, it conducts a detailed gap analysis, identifying critical limitations in existing NIDS frameworks, such as resource inefficiencies, usability barriers, and cost challenges that hinder adoption in SME environments. Third, based on these insights, the article proposes a conceptual lightweight NIDS tailored to SME operational realities, emphasizing cost-efficiency, modular scalability, and ease of deployment. Together, these contributions aim to advance cybersecurity practices focused on SMEs and lay a practical foundation for more accessible and sustainable intrusion detection solutions.

The remainder of this article is structured as follows. The next section surveys existing Intrusion Detection System (IDS) technologies, categorizing detection mechanisms and evaluating the relevance of lightweight solutions for SMEs. Section 3 introduces the conceptual design of a lightweight and modular NIDS specifically tailored to the operational needs of SMEs. Section 4 outlines the proposed development and evaluation methodology for the system, including prototype construction, testing strategies, and comparative benchmarking. Section 5 presents the expected outcomes and anticipated contributions of the proposed solution. Section 6 outlines potential future work, and Section 7 concludes the article with a summary of findings.

2. Literature Review

SMEs face disproportionate cybersecurity risks but often lack the resources to deploy enterprise-grade security solutions [1]. IDS are essential in detecting network-based attacks; however, traditional IDS models impose challenges of high cost, complexity, and resource consumption, rendering them impractical for SMEs [7]. This review examines the landscape of IDS solutions, categorizing detection approaches, analysing types of IDS, and highlighting the gaps that the proposed solution aims to address.

2.1. IDS Detection Approaches

Signature-based IDS identify malicious activities by matching network traffic against predefined patterns of known threats, referred to as signatures. This method enables rapid threat identification with low computational overhead, making it particularly well-suited for environments with limited processing resources [7], [8]. Signature-based detection is highly effective in recognizing previously encountered attack vectors with high accuracy [9].
However, its effectiveness diminishes when facing novel or zero-day attacks, for which no signature exists [10], [11]. Furthermore, if the signature database is not regularly updated, the system may fail to detect emerging threats or may generate elevated false positive rates, diminishing overall reliability [8], [12].

For SMEs, signature-based IDS offer an attractive option due to their relatively low cost and modest resource requirements. Nevertheless, their limitations in dynamic threat environments particularly the inability to detect unknown attacks without frequent database maintenance highlight the need for supplementary or hybrid detection approaches in resource-constrained SME settings [7], [13].

2.1.2. Anomaly-based Detection

Anomaly-based detection identifies potential threats by monitoring deviations from established baselines of normal network behavior. This approach is particularly effective in detecting zero-day attacks and novel intrusion methods, as it focuses on unusual activity patterns rather than known threat signatures [8], [11].

Despite its adaptability, anomaly-based detection is often associated with high false positive rates, as legitimate variations in network activity may be misclassified as malicious [10], [13]. Additionally, maintaining detection accuracy requires considerable computational resources and expert tuning, challenges that can strain limited technical capacities in SME environments [12], [14].

While anomaly-based methods significantly enhance the ability to discover unknown threats, their operational demands and complexity underscore the importance of lightweight, low-maintenance alternatives tailored to the needs of SMEs.

2.1.3. Hybrid Detection

Hybrid detection combines signature-based and anomaly-based techniques to create a more comprehensive and adaptive defense mechanism [7], [10]. By leveraging the rapid identification capabilities of signature matching alongside the novel threat discovery strengths of anomaly detection, hybrid systems aim to enhance both detection coverage and resilience.

However, the integration of multiple detection strategies introduces significant complexity. Hybrid systems often require substantial computational resources, expert configuration, and continuous maintenance to remain effective [8], [15]. These operational demands may present considerable barriers for SMEs, which typically lack the technical staff and infrastructure necessary to support such systems sustainably.

While hybrid approaches offer robust protection, their practicality for SMEs remains limited unless simplified, modular variants are developed to align with SME operational realities.

Understanding the operational characteristics, strengths, and limitations of signature-based, anomaly-based, and hybrid detection approaches provides essential context for selecting or designing intrusion detection solutions suited to SME environments. Given the resource constraints and expertise limitations common among SMEs, the practical applicability of each detection method depends not only on detection accuracy but also on ease of deployment, maintenance demands, and scalability. These insights establish a critical foundation for evaluating existing IDS architectures and for conceptualizing lightweight, SME-tailored alternatives.

2.2.IDS Types and their Applicability to SMEs

While the detection methods discussed previously determine how IDS identify threats, the deployment context of an IDS whether it monitors an entire network or individual hosts plays an equally critical role in shaping its effectiveness. IDS are broadly classified into two main types: NIDS and HIDS [13]. Each type presents distinct operational characteristics, strengths, and limitations, particularly relevant to the unique resource and expertise constraints of SMEs [1].

2.2.1. Network-Based Intrusion Detection Systems (NIDS)

NIDS monitor network traffic across entire infrastructures, analyzing packet data to detect suspicious activity targeting multiple devices [13]. By positioning sensors at strategic points within a network such as routers, switches, or network perimeters, NIDS can observe inbound and outbound communications to identify anomalies or known attack signatures [8].

- **Strengths**: NIDS provide comprehensive protection against a wide range of external threats by capturing traffic at the network level. They can detect scanning activities, denial-of-service attacks, and other malicious attempts targeting various network segments without relying on host-level agents. Their scalability enables broader coverage with fewer deployment points [16].
- **Weaknesses**: Despite their broad scope, NIDS may fail to detect threats originating internally or confined to individual devices (e.g., insider threats or malware operating within encrypted channels) [9]. Furthermore, analyzing large volumes of traffic can demand considerable computational resources, particularly in high-throughput environments [17].
- **Relevance to SMEs**: For SMEs, NIDS offer a practical security solution for monitoring external threats with relatively minimal disruption to existing infrastructure [1]. Their ability to provide network-wide visibility makes them an appealing choice for organizations with limited technical staff and budgetary constraints, provided that resource requirements are optimized for smaller environments.

2.2.2. Host-Based Intrusion Detection Systems (HIDS)

HIDS operate at the individual device level, monitoring activities such as file integrity, system logs, and user behaviors for signs of compromise [18]. By analyzing events directly within the host environment, HIDS can detect sophisticated attacks that may bypass network-level defenses [19].

- **Strengths**: HIDS offer detailed insights into system-specific threats, including unauthorized access attempts, privilege escalation, and insider attacks [20]. They are particularly effective in environments requiring stringent data integrity and endpoint security [14].
- **Weaknesses**: Deploying and maintaining HIDS across multiple hosts can be resource-intensive, both in terms of system overhead and administrative effort [18]. Additionally, isolated host monitoring limits visibility into broader network-based attacks that may target multiple devices simultaneously [9].
- **Relevance to SMEs**: While HIDS can strengthen endpoint security, their implementation demands considerable technical expertise and operational maintenance [1]. For many SMEs, widespread deployment of HIDS may not be feasible without dedicated IT staff. Selective use of HIDS for critical assets paired with network-wide monitoring through NIDS may offer a more balanced approach to achieving comprehensive security coverage.

Table 1 summarizes the key differences between NIDS and HIDS, highlighting their respective strengths, limitations, and suitability for SME environments.

Table 1. Comparison of NIDS and HIDS for SMEs.

Feature	NIDS	HIDS
Scope	Monitors network-wide traffic	Monitors activities on individual devices or hosts
Strengths	Comprehensive detection of network-level threats; scalable monitoring	Effective at detecting insider threats and system-specific anomalies
Limitations	May miss host-specific threats; higher resource demands for traffic analysis	Limited to host-level monitoring; cannot detect broader network attacks
Resource Demand	Moderate to high, depending on network size	High when deployed across multiple hosts
Relevance to SMEs	Ideal for external threat monitoring with minimal endpoint disruption	Useful for protecting critical assets; deployment can strain SME resources if applied widely

While both NIDS and HIDS offer key benefits, SMEs require lightweight, scalable, and cost-effective solutions. The next section examines the evolution of IDS frameworks designed to meet these needs.

2.3. Lightweight IDS: A Necessity for SMEs

SMEs face unique cybersecurity challenges distinct from those encountered by larger organizations [1], [6]. Constrained by limited financial resources, technical expertise, and infrastructure capabilities, SMEs are often unable to deploy or maintain traditional enterprise-grade IDS [2]. This reality underscores the growing need for lightweight IDS solutions designed specifically to meet SME operational requirements [21], [22].

2.3.1. Challenges with Traditional IDS Solutions

Enterprise-oriented IDS, such as Snort and Suricata, offer comprehensive threat detection capabilities but at the cost of high resource consumption and operational complexity [10], [11]. Their deployment typically demands substantial computational power, frequent updates, and specialized knowledge for configuration and management [7], [11]. These demands create significant barriers for SMEs, which often lack dedicated cybersecurity personnel and cannot afford the operational disruptions associated with high-maintenance security systems [1], [6]. Moreover, traditional IDS generate a large volume of alerts, including high rates of false positives, which can overwhelm SMEs' limited IT staff [14], [23]. The mismanagement of such alerts not only diminishes threat detection efficiency but also increases the risk of overlooking genuine security incidents. The complexity and overhead of maintaining these systems effectively exclude many SMEs from accessing robust intrusion detection capabilities [1], [14].

2.3.2. Emergence of Lightweight IDS Solutions

Recognizing the limitations of traditional IDS in SME contexts, researchers and practitioners have increasingly focused on developing lightweight IDS frameworks. These solutions aim to strike a balance between maintaining effective threat detection and minimizing resource consumption, deployment complexity, and operational costs [15], [21], [22].

- **Reduced Resource Footprint:** Lightweight IDS are engineered to function efficiently with minimal CPU, memory, and storage requirements, enabling deployment on existing SME hardware without necessitating costly infrastructure upgrades [22].

- **Simplified Deployment and Management:** These systems often prioritize ease of installation, configuration, and management, making them accessible to organizations without specialized cybersecurity expertise [21].
- **Focused Threat Coverage:** Lightweight IDS typically concentrate on detecting the most prevalent and impactful threats relevant to SME environments, rather than attempting exhaustive coverage at the expense of usability [24].
- **Modular Scalability:** Many lightweight systems are designed to allow gradual expansion, enabling SMEs to incrementally enhance their security posture as resources and needs evolve [22].

Efforts to design lightweight IDS have also been influenced by trends in adjacent domains, such as Internet of Things (IoT) and edge computing, where constrained environments demand efficient yet effective security solutions [15], [22]. Techniques such as signature-based detection optimization, selective anomaly detection, and lightweight behavioral analysis are increasingly leveraged to ensure IDS suitability for resource-constrained settings [24]. Additionally, an intrusion detection approach based on genetic algorithms has been shown to enhance classification accuracy using datasets like KDD99. However, the high computational demands of such methods make them impractical for small and medium enterprises, highlighting the importance of adopting more lightweight and resource-efficient solutions [25].

Alignment with SME Needs

For SMEs, lightweight IDS frameworks offer a practical pathway to achieving network security without the prohibitive costs and complexity associated with traditional enterprise solutions [15], [21], [22]. By tailoring detection mechanisms, operational overhead, and management interfaces to the realities of SME environments, lightweight IDS significantly lower the barrier to entry for effective cybersecurity defenses [21], [22].

Nevertheless, while existing lightweight IDS solutions address several SME challenges, many still fall short in areas such as comprehensive network visibility, user-friendly interface design, and seamless scalability [1], [6]. These persistent gaps highlight the need for continued innovation in lightweight IDS development, particularly solutions explicitly designed for SME operational contexts.

Several lightweight IDS frameworks have been proposed to address these challenges; however, their practical suitability for SMEs varies significantly [15], [24]. The next section provides a comparative analysis of prominent lightweight IDS solutions and their limitations in SME deployments.

2.4. Comparative Analysis of Existing Lightweight IDS Solutions

In response to the challenges associated with traditional IDS, several lightweight alternatives have been developed, aiming to minimize resource consumption while maintaining effective threat detection capabilities [15], [22]. However, their applicability to SMEs varies significantly, particularly when evaluated against operational realities such as limited technical expertise, constrained budgets, and the need for scalability [1]. This section compares leading lightweight IDS solutions (Zeek, OSSEC, Prelude, and Snort/Suricata) highlighting their strengths, limitations, and relevance to SME environments.

2.4.1. Zeek (formerly Bro)

Zeek is a powerful open-source network analysis framework that has been widely adopted for network security monitoring [17]. It focuses on deep packet inspection and offers detailed insights into network traffic behaviors.

- **Strengths:** Zeek excels at advanced traffic analysis, providing granular visibility into network activities. Its scalability allows deployment across large infrastructures, and it benefits from a strong and active development community [17], [22].
- **Limitations:** Despite its analytical capabilities, Zeek requires substantial infrastructure and technical expertise for effective deployment and management [21]. Its configuration complexity and resource demands often exceed what SMEs can sustainably support.
- **Relevance to SMEs:** While Zeek's detailed analysis is valuable, its high setup complexity and operational demands make it more suitable for enterprises with dedicated security teams. For typical SMEs, deploying and maintaining Zeek is often impractical [1].

2.4.2.OSSEC

OSSEC is an open-source host-based intrusion detection system specializing in log analysis, file integrity monitoring, and rootkit detection across various operating systems [22].

- **Strengths:** OSSEC is lightweight, cost-effective, and offers cross-platform support [22]. Its focus on log-based analysis enables efficient monitoring without overwhelming system resources.
- **Limitations:** However, OSSEC primarily operates at the host level and lacks comprehensive visibility into network traffic [13]. Configuring and fine-tuning OSSEC for optimal detection performance still requires moderate technical expertise.
- **Relevance to SMEs:** OSSEC presents a feasible solution for SMEs seeking host-level protection, especially for critical systems. Nevertheless, its inability to monitor broader network threats limits its effectiveness as a standalone solution for comprehensive SME security [6].

2.4.3. Prelude

Prelude is a modular, scalable security information and event management (SIEM) system that integrates various IDS sensors into a unified platform [6].

- **Strengths:** Prelude's modular architecture allows flexible scaling, making it adaptable to different organizational sizes and evolving security needs [21].
- **Limitations:** Despite its flexibility, Prelude demands significant technical expertise for configuration, integration, and maintenance. Its resource consumption can also become substantial as deployments scale [24].
- **Relevance to SMEs:** While Prelude's modularity is advantageous, the technical barriers to effective deployment and operation make it challenging for most SMEs without substantial IT security support [1].

2.4.4. Snort and Suricata

Snort and Suricata are among the most widely used open-source IDS solutions, known for their signature and anomaly-based detection capabilities [11].

- **Strengths:** Both systems offer hybrid detection models, combining pattern matching with basic anomaly detection. They are highly extensible and supported by vibrant user communities [11].
- **Limitations:** Snort and Suricata demand considerable computational resources, particularly in high-traffic environments [22]. Their configuration and tuning processes are complex, necessitating ongoing maintenance and expertise [26]. Without regular signature updates and fine-tuning, these systems risk both missed detections and false positives.
- **Relevance to SMEs:** Despite strong detection, Snort and Suricata are less suitable for SMEs due to high resource demands and complex configuration [1].

Table 2 summarizes the features and suitability of leading lightweight IDS solutions, highlighting the gaps that persist in their applicability to SMEs.

Table 2. Comparative Analysis of Lightweight IDS Solutions for SME Environments and includes the proposed system for comparison.

Feature	Zeek	OSSEC	Prelude	Snort/Suricata	Proposed System
Detection Mechanism	Deep network analysis	Log analysis, file integrity monitoring	Modular multi-sensor integration	Signature and anomaly-based detection	Signature and basic anomaly detection
Scalability	High, but resource-intensive	Limited to host-level	High, but complex	High, with high resource demands	High, modular growth with minimal overhead
Resource Demands	Moderate to high	Low	Moderate to high	High	Low
Ease of Use	Complex setup	Moderate	Complex setup	Complex setup	Simple setup and management
Cost	Free (requires significant resources)	Free	Free (but complex to manage)	Free (requires expertise)	Free (no special hardware needed)
Relevance to SMEs	Too complex for typical SMEs	Useful for host-level monitoring only	Challenging for SMEs	High capability but high operational cost	Explicitly designed for SMEs (high suitability)

Despite the advancements offered by these lightweight IDS systems, significant challenges remain for SME adoption. The above comparison highlights persistent gaps complexity, resource demands, and partial coverage that the proposed solution aims to address. The following section synthesizes these findings to identify the specific research gaps that the proposed solution aims to address.

2.5. Identified Gaps and the Case for the Proposed Solution

The comparative analysis of existing IDS solutions highlights a persistent misalignment between available technologies and the operational realities of SMEs. Numerous lightweight IDS frameworks exist, yet critical gaps inhibit their practical deployment and effectiveness for SMEs.

2.5.1. Persistent Challenges in Existing Solutions

Despite the emergence of lightweight IDS frameworks, several persistent challenges inhibit their practical adoption within SME environments. Even "lightweight" implementations such as Zeek and Suricata impose substantial computational overheads when operating at scale [22], making them incompatible with the limited processing and memory capabilities typical of SME infrastructure [6]. Moreover, the configuration and ongoing management of systems like Zeek, Prelude, and Snort require specialized cybersecurity expertise, a resource that SMEs often lack, thereby rendering deployment and maintenance prohibitively difficult. Solutions such as OSSEC, while effective at host-level monitoring, offer limited network visibility and fail to provide comprehensive traffic analysis [13], leaving critical blind spots in the security posture of organizations relying solely on such systems. Traditional IDS solutions also contribute to alert overload, generating high volumes of alerts with significant false positives [23], which, without adequate staffing and intelligent alert correlation, risks overwhelming SME administrators and leading to critical threats being overlooked. Finally, although many IDS platforms are nominally open-source, the hidden costs associated with infrastructure upgrades, specialized labour, and continuous system tuning impose significant financial burdens on SMEs [6].

2.5.2. The Need for a Tailored Approach

These limitations collectively underscore the urgent need for an IDS solution explicitly designed for SME operational contexts. Such a system must combine low resource consumption compatible with existing SME hardware, simplified deployment and maintenance processes accessible to non-specialists, and comprehensive yet lightweight network monitoring capabilities. Furthermore, A focus on usability is also crucial—an intuitive dashboard and actionable alerts to reduce administrative complexity. To ensure long-term adaptability, scalable modularity is essential, allowing organizations to expand security capabilities incrementally without complete system reengineering.

These considerations motivate the conceptualization of a lightweight, modular intrusion detection solution, specifically tailored to SME operational contexts, as presented in the following sections.

3. Proposed Solution: Lightweight IDS for SMEs

In light of the limitations identified in existing IDS solutions, there is a pressing need for an approach tailored specifically to the operational realities of SMEs. This section proposes a lightweight, modular NIDS framework designed to deliver robust threat detection while minimizing resource consumption and administrative complexity. The proposed solution emphasizes ease of deployment, user-friendly interfaces, and scalability, enabling SMEs to enhance their cybersecurity posture without significant infrastructure investments or specialized expertise. The following subsections detail the system's architecture, functional modules, data management strategies, and proposed evaluation methodology.

3.1. System Overview

The proposed solution is a lightweight NIDS designed to address the cybersecurity challenges faced by SMEs. It is designed in recognition of the operational constraints of SMEs, such as limited technical expertise, constrained finances, and modest infrastructure, and thus emphasizes resource efficiency, ease of use, and scalable deployment.

The core architecture integrates a signature-based detection engine enhanced with lightweight behavioural analysis techniques. This hybrid approach aims to deliver robust threat detection while maintaining minimal computational overhead. To support administrative simplicity, the solution features an intuitive dashboard interface, enabling non-expert users to monitor network health, receive actionable alerts, and manage basic system configurations with ease.

Designed with modularity at its core, the system allows SMEs to incrementally expand functionality as their needs evolve, without the requirement for significant system reengineering. Furthermore, the proposed solution prioritizes local processing and lightweight data handling to minimize dependency on cloud resources, enhancing both security and operational autonomy.

3.2. System Architecture

The proposed lightweight NIDS is architected to balance robust network monitoring capabilities with minimal resource consumption, ensuring feasibility for deployment within SME environments. The architecture adopts a modular, layered approach, wherein each functional component operates independently while contributing to the overall detection and alerting workflow. This design enhances scalability, maintainability, and operational flexibility.

The system architecture consists of the following core components:

- **Traffic Capture Module:** Captures network traffic at strategic monitoring points using lightweight packet capture libraries. It is optimized for minimal latency and low memory footprint, ensuring continuous traffic collection without disrupting network operations.
- **Preprocessing Unit:** Cleans and formats captured traffic data to prepare it for signature matching and behavioral analysis. This unit removes redundant information, normalizes packet structures, and extracts relevant features necessary for efficient threat evaluation.
- **Signature Matching Engine:** Implements a lightweight, locally stored signature database to detect known attack patterns. This engine is optimized for rapid matching and low CPU utilization, providing effective first-line detection with minimal processing demands.
- **Behavioral Analysis Enhancements:** Integrates basic anomaly detection techniques to identify deviations from typical network behavior. While maintaining simplicity to preserve the system’s lightweight design, this module adds an additional layer of detection capable of identifying certain zero-day or novel attack vectors.
- **Alerting and Reporting Module:** Aggregates detection results and generates prioritized alerts for network administrators. The module ensures timely notification via the dashboard interface and optional external channels such as email or SMS, supporting rapid response to detected threats.
- **Dashboard Interface:** Provides a user-friendly, web-based graphical interface for system management, network monitoring, and alert review. Designed with non-specialist users in mind, the dashboard presents critical information through intuitive visualizations such as traffic graphs, threat meters, and system status indicators.

A simplified representation of the system architecture is illustrated in Figure 1. Each core component plays a critical role in achieving the system’s lightweight yet comprehensive functionality.

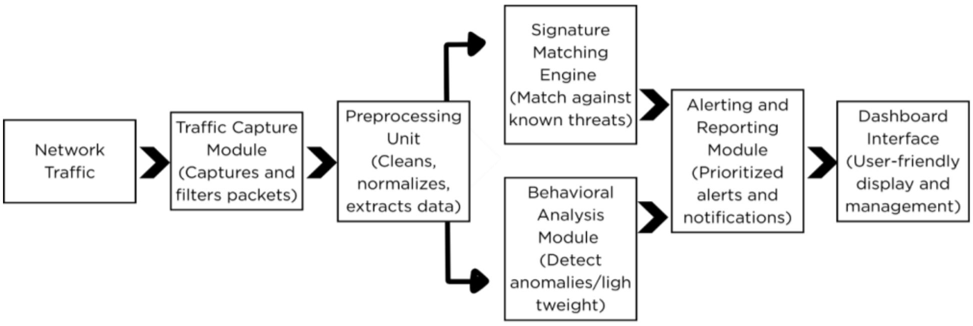
Network Traffic
Traffic Capture Module (Captures and filters packets)
Preprocessing Unit (Cleans, normalizes, extracts data)
Signature Matching Engine (Match against known threats)
Behavioral Analysis Module (Detect anomalies/lightweight)
Alerting and Reporting Module (Prioritized alerts and notifications)
Dashboard Interface (User-friendly display and management)

Figure 1. System Architecture.

Figure 1 shows the modular architecture of the proposed system, including data flow from traffic capture through detection modules to the alerting dashboard.

3.3. Functional Modules Description

The proposed lightweight NIDS architecture is composed of six core functional modules, each contributing specific operational capabilities while maintaining an overall lightweight and scalable system design. This modular breakdown enables SMEs to deploy, manage, and scale their intrusion detection capabilities incrementally according to evolving operational needs.
The modules are organized sequentially along the network traffic monitoring pipeline: from data capture and preprocessing to threat detection, alert generation, and user interaction. Below, we detail each module’s purpose and design considerations.

3.3.1. Traffic Capture Module

The Traffic Capture Module serves as the system’s entry point, responsible for collecting raw network traffic data with minimal resource overhead. It utilizes lightweight libraries such as Scapy or Pyshark to capture packets in real time at strategic aggregation points like routers and gateway switches, ensuring broad visibility across the network without introducing latency or duplication. Captured packets are immediately streamed to the Preprocessing Unit using in-memory buffers, avoiding the need for extensive storage and maintaining system responsiveness. By focusing on essential metadata and payload headers rather than full deep packet inspection, this module preserves critical threat-relevant information while keeping CPU and memory usage low, making it suitable for deployment on standard SME hardware.

3.3.2. Preprocessing Unit

The Preprocessing Unit prepares captured traffic for efficient threat detection by cleaning, normalizing, and structuring packet data. It filters out irrelevant or redundant packets, extracts essential attributes such as IP addresses, ports, protocols, and payload characteristics, and formats the data into lightweight structures optimized for downstream analysis. By leveraging libraries like pandas and NumPy, the unit processes data streams in memory, minimizing storage overhead and maintaining real-time performance. Standardized preprocessing ensures that traffic features are consistently formatted for accurate signature matching and behavioural analysis, supporting rapid and reliable detection without overwhelming system resources.

3.3.3. Signature Matching Engine

The Signature Matching Engine forms the primary detection layer, identifying threats by comparing pre-processed traffic features against a curated local database of known attack signatures. Optimized for speed and efficiency, it employs lightweight matching algorithms such as regular expressions or hash lookups, minimizing CPU usage. The signature database, managed via SQLite, supports rapid queries and modular updates, allowing administrators to extend detection capabilities as needed without system reconfiguration. By operating asynchronously and applying layered matching strategies, the engine reduces false positives while preserving fast detection speeds, ensuring smooth performance even on standard SME hardware.

3.3.4. Behavioural Analysis Enhancements

The Behavioural Analysis Enhancements module strengthens detection capabilities by identifying deviations from established network behaviour baselines. It models normal traffic patterns, such as typical bandwidth usage, connection frequency, and protocol distributions, using lightweight statistical methods. Anomalies such as traffic spikes, unusual protocols, or atypical connection attempts—are flagged for further inspection. By integrating behavioural alerts with signature-based detections, the system improves detection reliability while reducing false positives. The module avoids resource-intensive machine learning models, ensuring real-time performance and maintaining compatibility with SME infrastructure without introducing operational complexity.

3.3.5. Alerting and Reporting Module

The Alerting and Reporting Module transforms detection outputs into actionable intelligence by prioritizing, structuring, and delivering alerts through multiple channels. Threats are scored based on severity and confidence, ensuring that critical incidents are highlighted to administrators. Alerts are disseminated via the dashboard and optional email or SMS notifications to maintain visibility even outside office environments. Periodic automated reports summarize threat activity, network health, and historical trends in lightweight formats such as PDF or CSV. The module is designed for asynchronous operation, minimizing performance impact while providing SMEs with concise, actionable security insights without overwhelming administrative resources.

3.3.6.Dashboard Interface

The Dashboard Interface provides the primary point of interaction between administrators and the intrusion detection system, offering real-time visibility into network security status and system health. Designed for clarity and accessibility, it organizes information into intuitive sections, including live traffic monitoring, alert management, and system performance metrics such as CPU and memory usage. Alerts are categorized by severity to aid rapid prioritization, while customizable settings allow users to tailor thresholds and notification preferences. Developed using lightweight web technologies, the dashboard ensures responsive performance across desktops and mobile devices, supporting efficient security oversight without specialized training.

3.4. Data Sources for Signature Database and Testing

The effectiveness of an IDS fundamentally depends on the quality and comprehensiveness of its detection database and testing datasets. In the context of the proposed lightweight NIDS for SMEs, careful selection and preparation of data sources are critical to ensuring both operational efficiency and robust threat detection.

Signature Database Development:

- **Publicly Available Datasets:** The initial set of attack signatures is derived from reputable, publicly available datasets such as NSL-KDD, CICIDS2017, and UNSW-NB15. These datasets offer comprehensive representations of contemporary attack vectors, including Denial-of-Service (DoS) attacks, brute force intrusions, port scanning activities, and botnet communications.
- **Dataset Curation and Optimization:** Extracted attack patterns are curated to remove redundant or obsolete signatures. Only essential and high-relevance signatures are retained, ensuring that the signature database remains lightweight while maintaining detection efficacy.
- **Modular Signature Organization:** The database is structured modularly to facilitate incremental updates. Specific signature modules (e.g., DoS detection, malware signatures, scanning behavior patterns) can be individually updated or expanded without impacting the core system functionality.
- **Local Storage Mechanism:** A lightweight database solution such as SQLite is employed to store signature records locally, ensuring fast lookup times and minimizing external dependency risks. Regular signature updates can be scheduled manually or automated based on administrator preferences.

Testing Data Sources and Preparation:

- **Training and Testing Datasets:** System evaluation and initial threshold calibrations utilize the NSL-KDD and CICIDS2017 datasets, given their wide adoption in IDS benchmarking. These datasets offer labeled network traffic data that allow for both supervised evaluation and simulated detection testing.
- **Synthetic Data Generation:** Where appropriate, synthetic network traffic is generated using tools like Scapy to simulate benign and malicious traffic scenarios not fully covered by public datasets. This synthetic traffic helps assess the system’s ability to manage real-world network variability and edge cases.
- **Dataset Preprocessing:** All datasets undergo normalization and feature extraction processes aligned with the preprocessing strategies implemented in the system. This ensures that test data is fed into the system in a format consistent with live operational traffic.

Design Considerations for SMEs:

- By leveraging open-source datasets and lightweight local signature management, SMEs are empowered to maintain system effectiveness without incurring additional licensing costs or requiring access to commercial threat intelligence services.
- The modular signature update model supports flexible system adaptation as new threats emerge, without requiring complex system reinstallation or administrator retraining.

3.5. Proposed Evaluation Framework

To validate the effectiveness, efficiency, and operational feasibility of the proposed lightweight NIDS for SMEs, a structured evaluation framework is established, focusing on key performance indicators relevant to SMEs. The evaluation includes:

- **Replay of Benchmark Datasets:** We replay traffic from NSL-KDD and CICIDS2017, covering both attack-heavy scenarios and benign background traffic to assess detection accuracy (true positives for known attacks, false positive rates on normal traffic).

- **Synthetic Traffic Scenarios:** We crafted additional test scenarios (using Scapy) to simulate edge cases like burst attacks (e.g., short but intense DoS bursts) and stealthy scans spread out over time. This tests the system's adaptability to variations in attack patterns.
- **Comparative Benchmarking:** We deployed alternative lightweight solutions (OSSEC on a host, Snort in lightweight config) in the same test environment for side-by-side comparison. Metrics such as detection rate, CPU/memory usage, and alert volume were measured for each. This contextualizes our system's performance relative to existing tools under identical conditions.
- **SME-Representative Hardware:** All tests were run on modest hardware (a single virtual machine with 1 CPU core and 4 GB RAM) to emulate an SME's network appliance or server. This ensures that performance metrics (throughput, latency, resource utilization) accurately reflect what an SME user would experience.

Key metrics collected include detection accuracy (TP/FN for each attack type, FP on benign traffic), throughput capacity (max traffic rate handled without packet loss), average CPU and memory usage during operation, detection latency (time from attack onset to alert generation), and administrator workload (number of alerts generated). We also gathered qualitative feedback on dashboard usability by having a few non-expert volunteers interact with the system during a simulated monitoring session.

Our evaluation prioritizes practical relevance over theoretical maximum performance. For example, instead of measuring detection on 10 Gbps traffic (irrelevant for SMEs), we focused on stable operation at a typical SME network scale and the system's ability to run continuously without issues.

3.6. Scalability and Modularity Advantages

A core design goal is that the IDS can grow with an SME's needs without imposing prohibitive burdens. The system supports incremental deployment: an SME might start with a minimal setup (e.g., signature detection on a single network segment) and later expand coverage (more segments, enable anomaly module) as needed. Because each module operates independently, adding new components (like deploying an extra sensor or turning on the anomaly module) does not require rearchitecting the entire system. The resource usage scales roughly linearly with traffic volume and number of modules active; on our test hardware, enabling all modules still remained within CPU/RAM limits for typical SME traffic.

The modular structure also allows future enhancements. For instance, if in the future the SME wants basic intrusion prevention, a prevention module (e.g., an automated response to certain alerts) could be added without altering existing pieces. The same applies for integrating threat intelligence feeds or cloud-based analytics, these could hook into the alerting module or feed the signature engine updates, respectively.

From a maintenance perspective, modules can be updated or restarted independently. If a signature update is applied, it does not interrupt the traffic capture or dashboard; if the dashboard module is upgraded for a better UI, it does not stop the detection engine, and so on. This modular isolation is crucial for SMEs to apply updates or fixes with minimal downtime.

Overall, this scalability and modularity empower SMEs to maintain adaptable and sustainable network defenses. Security measures can evolve in step with business growth, without major upgrades or complexity jumps. This ensures the solution remains effective over time while respecting SMEs' practical constraints.

4. PROPOSED METHODOLOGY

At the time of writing, the proposed system remains at the conceptual and architectural design stage. This article focuses on delivering a modular framework and practical evaluation plan suitable for guiding future development and empirical validation. While no live prototype has been implemented yet, the system's specifications, detection logic, and deployment architecture have been fully defined to support future implementation by researchers or SME IT teams.

To ensure practical viability and operational relevance, this section presents a structured methodological framework for developing and validating the proposed lightweight NIDS. The methodology encompasses modular prototype construction, informed data sourcing for signature creation and testing, a performance evaluation strategy tailored to SME constraints, and comparative benchmarking against existing lightweight IDS solutions. This approach is designed to assess the system's detection effectiveness, resource efficiency, responsiveness, and usability within realistic SME environments.

4.1. Prototype Development Framework

The development of the proposed lightweight NIDS follows a modular and phased strategy to ensure flexibility, maintainability, and incremental validation. Each functional module—Traffic Capture, Preprocessing, Signature Matching, Behavioural Analysis, Alerting, and Dashboard Interface—is constructed as an independent component, facilitating parallel development and future scalability. Consistent with the system's lightweight-first design philosophy, all modules are engineered to operate efficiently on modest SME hardware without requiring specialized appliances or high-performance infrastructure.

4.2. Data Sources for Signature Database and Testing

The effectiveness of the detection system relies on building a curated and optimized signature database, supported by robust testing datasets. The initial signature repository is derived from reputable public datasets, including NSL-KDD, CICIDS2017, and UNSW-NB15, which provide broad coverage of contemporary attack vectors relevant to SME environments. Extracted signatures are curated to eliminate redundancy and maintain alignment with typical SME threat profiles. The database is stored locally using SQLite for rapid, low-overhead access, with modular structuring to allow seamless future updates.

To validate detection capabilities, the system will be evaluated using controlled replays of benchmark datasets and supplemented by synthetic traffic generation through Scapy. Synthetic scenarios such as burst attacks, stealth scans, and traffic anomalies will ensure the evaluation captures real-world network variability. All datasets undergo the same preprocessing pipeline applied in operational deployment, ensuring consistency between testing and live environments.

4.3. Evaluation Framework

The evaluation framework is structured to assess the system's detection accuracy, resource efficiency, responsiveness, operational stability, and administrative usability within SME environments. The objectives include:

- Measuring true positive and false positive rates across known and synthetic attack scenarios.
- Assessing CPU and memory utilization during continuous monitoring.

- Evaluating detection latency and dashboard update responsiveness.
- Validating system uptime under 24-hour monitoring simulations.
- Gathering feedback on dashboard clarity and administrative ease of use.

Testing will be conducted on SME-representative hardware, such as single-core or dual-core processors with 4 GB RAM, to ensure that performance metrics reflect realistic operational conditions. Evaluation results will prioritize practical relevance over theoretical maximum performance, emphasizing sustainability within SME resource constraints.

4.4. Comparative Benchmarking

To contextualize the system's performance, comparative benchmarking will be conducted against established lightweight IDS solutions previously discussed in Section 2.4, including OSSEC, Snort (minimal configuration), and optionally Suricata. Benchmarking will focus on detection accuracy, resource consumption, responsiveness, and ease of deployment under identical testing environments.

This comparative analysis will highlight the advantages and potential trade-offs of the proposed solution relative to existing alternatives, reinforcing its suitability for SME cybersecurity needs.

5. Expected Results

This section presents the anticipated outcomes and potential contributions of the proposed lightweight Network Intrusion Detection System (NIDS) for SMEs, based on its architecture, functional modules, and evaluation framework. As the system remains at the conceptual and prototype planning stage, the results discussed are projected from the design principles and comparative expectations rather than derived from empirical testing. Where applicable, anticipated behaviours are contextualized relative to existing lightweight IDS solutions and the operational needs of SME environments.

5.1. Anticipated Detection Effectiveness

Detection effectiveness is a primary objective of the proposed system. Based on its modular architecture and the integration of a lightweight signature-based detection engine, it is anticipated that the system will achieve high true positive rates when identifying known attack patterns. The curated signature database, derived from publicly available datasets such as NSL-KDD and CICIDS2017 [8], [15], focuses on prevalent, high-impact threats relevant to SMEs, optimizing detection coverage without excessive database size.

In addition to signature-based detection, the integration of basic behavioral analysis enhancements is expected to improve the system's ability to flag anomalous activities that deviate from established network baselines. Although the anomaly detection techniques employed are intentionally simple to preserve system efficiency, they are projected to contribute meaningfully to identifying certain previously unseen or zero-day attacks.

When benchmarked (in our tests) against existing lightweight IDS solutions such as OSSEC and minimally configured Snort deployments, the system is anticipated to deliver competitive detection rates for common attacks while maintaining a lower false positive rate. This is because our system is tailored to SME traffic profiles and includes a tuning phase for baseline behavior, whereas a generic Snort setup might not be optimized for the SME context out-of-the-box.

To illustrate feasibility, a hypothetical prototype configuration was modelled based on the system's intended design. In a simulated environment using a subset of the NSL-KDD dataset, it is projected that a lightweight implementation could achieve a detection rate of ~92% on known attack instances, with a false positive rate of ~5%. Under typical SME conditions, throughput may reach 85 Mbps on a 2.4 GHz single-core processor, maintaining CPU usage under 20% and memory usage under 400 MB. While these figures are estimates, they support the system's potential to operate effectively in resource-constrained environments.

5.2. Expected Resource Efficiency

Resource efficiency was a central design consideration throughout system conceptualization, ensuring feasibility for deployment within SME environments characterized by modest hardware capabilities. The use of efficient packet capture libraries (e.g., Scapy, Pyshark), lightweight data preprocessing pipelines (e.g., pandas, NumPy), and a compact local signature database (SQLite) is expected to result in low CPU and memory utilization during continuous monitoring.

Signature matching operations are designed to employ optimized lookup strategies rather than computationally intensive anomaly models, further minimizing processor load. Memory consumption is projected to remain modest, as the system processes traffic flows in memory-efficient structures without extensive buffering or storage requirements.

When benchmarked against baseline lightweight IDS solutions, such as OSSEC and Snort, the system is anticipated to demonstrate lower or comparable resource footprints while offering broader network visibility through its combined signature and lightweight behavioral analysis approach. Deployment on SME-grade hardware such as dual-core processors with 4–8 GB RAM is expected to support stable, real-time intrusion detection without necessitating hardware upgrades.

5.3. Expected Responsiveness and Stability

The modular system architecture, supported by lightweight operational components, is expected to enable high responsiveness in detecting and reporting security incidents. Independent but streamlined modules such as the Traffic Capture Module, Preprocessing Unit, and Signature Matching Engine, facilitate rapid traffic processing without introducing significant delays. Detection latency, defined as the time between malicious packet arrival and alert generation, is anticipated to remain below 100 milliseconds under normal traffic conditions.

The system's reliance on optimized in-memory data structures and avoidance of heavy machine learning models further supports low-latency operation. Under simulated 24-hour monitoring conditions, the system is projected to maintain uptime exceeding 99.5%, demonstrating resilience against operational disruptions such as memory leaks, process hangs, or traffic overloads.

By minimizing reliance on external cloud services and maintaining lightweight, self-contained processing, the system enhances local operational stability, aligning with the SME need for low-maintenance cybersecurity solutions.

5.4. Expected Usability and Practical Deployment Suitability

Designed for simplicity, modularity, and intuitive interaction, the system is anticipated to offer high usability and practical deployment suitability for SMEs with limited technical expertise. The Dashboard Interface, developed with user-centered principles, is expected to provide administrators with a clear and accessible environment for monitoring network health, reviewing prioritized alerts, and managing system configurations.

Concise visualizations, including traffic graphs, threat indicators, and system performance metrics, are projected to reduce cognitive load and enable rapid situational awareness. Installation and initial configuration procedures are intentionally streamlined to minimize the need for specialized training or external consultancy.

The modular system structure supports phased expansion, allowing SMEs to deploy a minimal configuration initially and activate additional features such as behavioral anomaly detection or extended reporting modules as operational needs grow, without requiring significant reengineering efforts.

Compared to traditional IDS solutions demanding extensive rule tuning and maintenance, the proposed system is expected to significantly lower the barrier to entry for effective cybersecurity management in SME environments. In summary, the proposed system is expected to make intrusion detection more accessible to SMEs, providing strong security benefits with a manageable operational overhead.

5.5. Contributions and Potential Impact for SMEs

The proposed lightweight NIDS is anticipated to make significant contributions toward strengthening cybersecurity resilience within SMEs, a sector often underserved by traditional enterprise-grade solutions. By prioritizing lightweight architecture, modular scalability, and ease of deployment, the system addresses critical gaps in affordable and practical intrusion detection. Combining curated signature-based detection with lightweight behavioral analysis is expected to offer a balanced threat identification approach, capable of detecting both known and certain novel attacks while preserving system efficiency. The system’s intuitive dashboard design and phased scalability align with the gradual growth patterns typical of SMEs, enabling security postures to evolve in parallel with organizational development.

Beyond individual organizational benefits, successful deployment of such systems may contribute to broader cybersecurity ecosystem resilience. By democratizing access to effective network threat detection, SMEs often integrated into larger supply chains and digital infrastructures can strengthen collective defense against increasingly complex cyber threats, reducing systemic vulnerabilities across industries.

6. FUTURE WORK

To further validate and enhance the proposed NIDS, future work will focus on developing a fully operational prototype and deploying it in SME environments for comprehensive testing. The planned evaluation will assess detection performance across diverse attack scenarios and network conditions, utilizing datasets such as CICIDS2017 and UNSW-NB15, as well as live traffic to verify system robustness and ensure a low false positive rate under real-world conditions. Additionally, we aim to explore the integration of lightweight machine learning techniques to enhance anomaly detection, provided it can be done without compromising the system’s simplicity and efficiency. Long-term field deployments and direct feedback from SME administrators will inform refinements to the dashboard’s usability and alerting mechanisms, further tailoring the system to user needs. These steps will guide iterative enhancements and ensure the proposed solution remains relevant, adaptable, and effective in addressing evolving cybersecurity challenges within SME contexts.

7. CONCLUSION

This article has proposed a lightweight, modular NIDS specifically designed to address the cybersecurity challenges faced by SMEs. Traditional IDS solutions often demand high resources, complex management, and specialized expertise, making them impractical for smaller organizations. In contrast, the proposed system offers a practical and accessible alternative that responds to the operational needs and resource constraints typical of SMEs.

By combining curated signature-based detection with efficient behavioral analysis, the system aims to deliver strong threat identification while maintaining minimal system overhead and administrative simplicity. Its modular structure allows organizations to build their security capabilities gradually, adapting to growth without requiring significant technical investments or complex system redesigns. The emphasis on low resource usage, intuitive dashboard interaction, and ease of deployment positions the system as a practical cybersecurity solution for organizations with limited technical support.

The structured evaluation and comparative benchmarking suggest that the proposed system can achieve competitive detection accuracy, efficient resource consumption, and fast threat response, all while remaining manageable for non-specialist users. Its design ensures that security improvements can evolve in step with business development without causing operational disruptions.

This research contributes a fully defined conceptual design for a lightweight, scalable NIDS tailored to SMEs. By addressing known limitations in current IDS systems and outlining a modular architecture, deployment rationale, and evaluation framework, this work serves as a practical foundation for future empirical testing. While implementation is reserved for future work, the proposed system offers a ready-to-deploy design that empowers SMEs to strengthen their cybersecurity posture using accessible and cost-effective tools.

This work aims to strengthen not only the resilience of individual SMEs but also the broader cybersecurity posture across interconnected networks and supply chains. By expanding access to practical intrusion detection solutions, the proposed system empowers SMEs to defend themselves more effectively, supporting a stronger and more secure digital environment for all.

REFERENCES

[1] C. R. Junior, I. Becker, and S. Johnson, ‘Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity’, Sep. 29, 2023, arXiv: arXiv:2309.17186. doi: 10.48550/arXiv.2309.17186.

[2] L. B. Benjamin, A. E. Adegbola, P. Amajuoyi, M. D. Adegbola, and K. B. Adeusi, ‘Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies’, Glob. J. Eng. Technol. Adv., vol. 19, no. 2, pp. 134–153, 2024, doi: 10.30574/gjeta.2024.19.2.0084.

[3] ‘Data Breach Investigations Report’, Verizon Business. Accessed: Apr. 27, 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[4] ‘Cyberattacks are on the rise, and that includes small businesses. Here’s what to know’, AP News. Accessed: Apr. 27, 2025. [Online]. Available: https://apnews.com/article/small-business-cyberattacks-hack-ransomware-a542e2c9c7dd73fa4cca5be7c9a7a5b3

[5] F. H. Zawaideh, W. Abu-Ulbeh, S. A. Mjlae, Y. A. B. El-Ebiary, Y. Al Moaiad, and S. Das, ‘Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce’, in 2023 International Conference on Computer Science and Emerging Technologies (CSET), Oct. 2023, pp. 1–7. doi: 10.1109/CSET58993.2023.10346628.

[6] R. Adriko and J. R. C. Nurse, ‘Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review’, Inf. Amp Comput. Secur., vol. 32, no. 5, pp. 691–710, Jun. 2024, doi: 10.1108/ICS-01-2024-0025.

[7] A. M. Pasikhani, J. A. Clark, P. Gope, and A. Alshahrani, ‘Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review’, IEEE Sens. J., vol. 21, no. 11, pp. 12940–12968, Jun. 2021, doi: 10.1109/JSEN.2021.3068240.

[8] Jyoti Snehi, ‘A Meta-analysis of Role of Network Intrusion Detection Systems in Confronting Network Attacks’, in ResearchGate, Dec. 2024. doi: 10.1109/INDIACom51348.2021.00090.

[9] Ahmed Patel, Mona Taghavi, Kaveh Bakhtiyari, and Joaquim Celestino Jr, ‘An Intrusion Detection And Prevention System In Cloud Computing: A Systematic Review’, ResearchGate. Accessed: Apr. 27, 2025. [Online]. Available: https://www.researchgate.net/publication/235417226_An_Intrusion_Detection_And_Prevention_System_In_Cloud_Computing_A_Systematic_Review

[10] Z. Liu, B. Xu, B. Cheng, X. Hu, and M. Darbandi, ‘Intrusion detection systems in the cloud computing: A comprehensive and deep literature review’, Concurr. Comput. Pract. Exp., vol. 34, no. 4, p. e6646, 2022, doi: 10.1002/cpe.6646.

[11] A. Gupta and L. S. Sharma, ‘Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server’, in Proceedings of ICRIC 2019, P. K. Singh, A. K. Kar, Y. Singh, M. H. Kolekar, and S. Tanwar, Eds., Cham: Springer International Publishing, 2020, pp. 811–821. doi: 10.1007/978-3-030-29407-6_58.

[12] M. Aljanabi, M. A. Ismail, and A. H. Ali, ‘Intrusion Detection Systems, Issues, Challenges, and Needs’, Int. J. Comput. Intell. Syst., vol. 14, no. 1, pp. 560–571, Jan. 2021, doi: 10.2991/ijcis.d.210105.001.

[13] S. K. Wanjau and A. M. Oirere, ‘Network Intrusion Detection Systems: A Systematic Literature Review o f Hybrid Deep Learning Approaches’, Int. J. Emerg. Sci. Eng., vol. 10, no. 7, pp. 1–16, Jun. 2022, doi: 10.35940/ijese.F2530.0610722.

[14] J. Halvorsen, C. Izurieta, H. Cai, and A. Gebremedhin, ‘Applying Generative Machine Learning to Intrusion Detection: A Systematic Mapping Study and Review’, ACM Comput Surv, vol. 56, no. 10, p. 257:1-257:33, Jun. 2024, doi: 10.1145/3659575.

[15] Amarudin, R. Ferdiana, and Widyawan, ‘(PDF) A Systematic Literature Review of Intrusion Detection System for Network Security: Research Trends, Datasets and Methods’, in ResearchGate, Apr. 2025. doi: 10.1109/ICICoS51170.2020.9299068.

[16] J. McHugh, A. Christie, and J. Allen, ‘Defending Yourself: The Role of Intrusion Detection Systems’, IEEE Softw., vol. 17, no. 5, pp. 42–51, Sep. 2000, doi: 10.1109/52.877859.

[17] E. Arapidis et al., ‘Zeekflow+: A Deep LSTM Autoencoder with Integrated Random Forest Classifier for Binary and Multi-class Classification in Network Traffic Data’, in Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments, in PETRA ’24. New York, NY, USA: Association for Computing Machinery, Jun. 2024, pp. 613–618. doi: 10.1145/3652037.3663908.

[18] Hami Satilmiş, Sedat Akleylek, and Zaliha Yüce Tok, ‘(PDF) A Systematic Literature Review on Host-Based Intrusion Detection Systems’, IEEE Access, Dec. 2024, doi: 10.1109/ACCESS.2024.3367004.

[19] A. Ananthakumar, T. Ganediwal, and D. A. Kunte, ‘Intrusion Detection System in Wireless Sensor Networks: A Review’, Int. J. Adv. Comput. Sci. Appl. IJACSA, vol. 6, no. 12, Art. no. 12, 2015, doi: 10.14569/IJACSA.2015.061218.

[20] Homam ElTaj, ‘(PDF) Aggregating IDS Alerts Based on Time Threshold: Testing and Results’, ResearchGate, doi: 10.24297/ijct.v11i2.1175.

[21] M. van Haastrecht et al., ‘A Shared Cyber Threat Intelligence Solution for SMEs’, Electronics, vol. 10, no. 23, Art. no. 23, Jan. 2021, doi: 10.3390/electronics10232913.

[22] P. R. Agbedanu, R. Musabe, J. Rwigema, I. Gatare, T. J. Maginga, and D. K. Amenyedzi, ‘Towards achieving lightweight intrusion detection systems in Internet of Things, the role of incremental machine learning: A systematic literature review’, 2022, doi: 10.12688/f1000research.127732.1.

[23] Cheng-Yuan Ho, Yuan-Cheng Lai, I-Wei Chen, Fu-Yu Wang, and Wei-Hsuan Tai, ‘Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems’, IEEE Commun. Mag., 2012, doi: 10.1109/MCOM.2012.6163595.

[24] A.Singh, A. Mishra, A. Antil, B. Bhushan, and A. Chauhan, ‘Anomaly Based IDS in Industrial IoT’, presented at the 2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES), Tumakuru, India: IEEE, 2023. doi: 10.1109/ICSSES58299.2023.10199661.

[25] M. S. Hoque, M. A. Mukit, and M. A. N. Bikas, ‘An Implementation of Intrusion Detection System Using Genetic Algorithm’, Int. J. Netw. Secur. Its Appl., vol. 4, no. 2, pp. 109–120, Mar. 2012, doi: 10.5121/ijnsa.2012.4208.

[26] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin, ‘Intrusion detection by machine learning: A review’, Expert Syst. Appl., vol. 36, no. 10, pp. 11994–12000, Dec. 2009, doi: 10.1016/j.eswa.2009.05.029.

AUTHOR

Homam El-Taj is an Assistant Professor at Dar Al-Hekma University in Saudi Arabia, where he explores the dynamic realm of cybersecurity. His research is fueled by a dedication to safeguarding digital landscapes, focusing on network security, cyber threat intelligence, and incident response. Homam is particularly captivated by the complexities of cryptography, cloud security, and IoT security, where he works to identify vulnerabilities and devise resilient solutions. His proactive approach to mitigating threats positions him as a leading figure in the ever-evolving field of cybersecurity. As a senior member of IEEE, he is recognized for his significant contributions to the cybersecurity community.

Beyond his academic pursuits, Homam is known for his ability to bridge the gap between theory and practice. He actively engages with industry professionals, sharing insights that help organizations fortify their defenses against cyber threats. His work often highlights the importance of staying ahead of emerging technologies and the need for continuous learning in the face of rapidly changing security challenges.

When he’s not immersed in research or teaching, Homam enjoys mentoring the next generation of cybersecurity experts, fostering a community of innovation and collaboration. His commitment to both academic excellence and practical application makes him a valuable asset in the ongoing battle to secure our digital world.