CogNexus *Volume: 1 Issue: 1 04/2026/pp.19-40*

A Multidisciplinary, Multilingual, International, Peer-Reviewed, Open Access Journal

Cybersecurity for Small Businesses: Cost-Effective AI-Driven Solutions.

[1] Lucy Wanjiru Njuguna

[1]Western Michigan University, United States
https://orcid.org/0009-0001-1258-7596

Abstract

Small businesses play a critical role in the global economy but remain highly vulnerable to cyberattacks due to limited financial resources, technical expertise, and security infrastructure. Traditional cybersecurity solutions are often costly and impractical for such environments. This study examines the cybersecurity risks facing small businesses and proposes a cost-effective, AI-driven security framework integrating anomaly detection, automated response mechanisms, and cloud-based services. The framework employs machine learning models to monitor network activity, detect threats, and enable rapid mitigation while minimizing operational costs. Experimental evaluation using standard cybersecurity datasets demonstrates that data-driven detection models significantly improve threat identification, reduce false positives, and enhance response efficiency compared to traditional approaches. The findings show that scalable, AI-assisted cybersecurity solutions can provide practical and affordable protection for small businesses. This study offers actionable insights for deploying efficient cybersecurity strategies in resource-constrained environments.

Keywords: Cybersecurity, Small Business Security, Artificial Intelligence, Intrusion Detection Systems, Threat Detection.

1. Introduction

1.1 Background of Cybersecurity Challenges for Small Businesses

Small and medium-sized enterprises (SMEs) play a central role in global economic development, contributing significantly to employment generation and innovation. Despite this importance, many SMEs operate with limited financial capacity, constrained technical expertise, and minimal cybersecurity infrastructure. These limitations restrict their ability to deploy advanced security systems and dedicated security personnel. As a result, SMEs are increasingly targeted by cybercriminals seeking vulnerable entry points into digital systems. Studies indicate that smaller organizations often lack structured cybersecurity strategies and fail to prioritize security investments due to competing operational demands. This combination of weak defenses and high-value data makes SMEs attractive targets for cyberattacks. The rapid adoption of digital technologies, including cloud computing and remote access systems, has further expanded the attack surface. While these technologies enhance operational efficiency, they also introduce additional vulnerabilities. Consequently, SMEs face growing exposure to cyber threats without corresponding improvements in defensive capabilities.

1.2 Cyber Threats Targeting Small Businesses

Cyber threats affecting SMEs have increased in both frequency and complexity. Attackers commonly exploit weaknesses such as outdated software, weak authentication systems, and poor network configurations.

Common threats include:

- Phishing and social engineering attacks
- Ransomware campaigns
- Malware infiltration
- Unauthorized system access
- Supply chain attacks

Phishing remains particularly effective because employees in smaller organizations often lack formal cybersecurity training. Similarly, ransomware attacks can disrupt operations by encrypting critical data and demanding financial payment for recovery. Supply chain attacks have also emerged as a significant concern. In such cases, attackers compromise smaller organizations to gain indirect access to larger networks. This trend reflects the interconnected nature of modern business environments.

1.3 Limitations of Traditional Cybersecurity Approaches

Traditional cybersecurity systems are largely based on rule-driven detection mechanisms and predefined threat signatures. While effective against known threats, these systems struggle to detect new or evolving attack patterns.

In addition, enterprise-grade cybersecurity solutions require:

- Significant financial investment
- Specialized technical expertise
- Continuous monitoring infrastructure

These requirements are often beyond the reach of SMEs. As a result, many small businesses rely on basic security tools such as antivirus software and firewalls, which provide only limited protection against sophisticated cyber threats.

1.4 Data-Driven Cybersecurity Approaches

Recent advancements in data-driven security techniques have introduced new opportunities for improving cybersecurity effectiveness. These approaches enable automated analysis of network traffic and user behavior, allowing systems to identify deviations from normal activity patterns. Unlike traditional methods, data-driven detection systems can adapt to evolving threat environments by learning from historical data. This capability improves detection accuracy and reduces reliance on manual monitoring. Research shows that such systems can significantly enhance threat detection and incident response, particularly in environments where dedicated security teams are unavailable (Xin et al., 2018; Sarker et al., 2019).

1.5 Research Objectives

This study aims to develop a practical and cost-efficient cybersecurity approach tailored to SMEs. The objectives include:

- Examining cybersecurity challenges faced by SMEs
- Evaluating data-driven detection techniques for threat identification
- Designing a cost-effective cybersecurity framework
- Assessing the effectiveness of automated response mechanisms

1.6 Research Contributions

This study makes the following contributions:

- Proposes a cost-effective cybersecurity framework tailored to SMEs
- Integrates automated threat detection and response mechanisms
- Provides practical deployment guidance for small businesses
- Demonstrates performance benefits using experimental evaluation

2. Literature Review

2.1 Cybersecurity Challenges in SME Environments

Existing literature consistently highlights that small and medium-sized enterprises operate within constrained cybersecurity environments characterized by limited financial resources, insufficient technical expertise, and lack of structured security governance. Unlike large organizations, SMEs often rely on basic protection mechanisms and do not maintain dedicated cybersecurity teams. Rather than reiterating general vulnerability concerns, recent studies emphasize structural limitations as the primary driver of SME cybersecurity risk. These include weak access control policies, lack of continuous monitoring systems, and absence of formal incident response strategies (Sarker et al., 2019; Rawindaran et al., 2021). In addition, SMEs frequently underestimate cyber risk exposure due to competing operational priorities. This leads to reactive rather than proactive security practices, further increasing susceptibility to cyber incidents.

2.2 Cyber Threat Patterns in Small Business Contexts

Cyber threats targeting SMEs exhibit both conventional and evolving characteristics. While phishing, ransomware, and malware remain dominant, recent research indicates a shift toward more targeted and adaptive attack strategies. Phishing continues to serve as a primary entry vector due to human vulnerability within organizational systems. Ransomware attacks have become more structured, often involving data exfiltration in addition to encryption, thereby increasing financial and reputational damage (Ferrag et al., 2020; Rehman et al., 2023). Furthermore, supply chain vulnerabilities have emerged as a critical threat dimension. Attackers increasingly exploit smaller organizations to gain indirect access to larger, interconnected systems. This reflects a broader transition from isolated attacks to ecosystem-level exploitation strategies (Shaukat et al., 2019; Jada & Abid, 2024).

2.3 Data-Driven Approaches to Cybersecurity

Traditional security models based on predefined rules are limited in their ability to detect novel threats. As a result, research has increasingly focused on data-driven detection techniques that analyze network behavior and system activity patterns. These approaches utilize classification, clustering, and anomaly detection techniques to identify deviations from established behavioral baselines. Such systems are capable of detecting previously unseen attack patterns, making them more suitable for modern cybersecurity environments (Xin et al., 2018; Nguyen et al., 2020). Behavioral analysis has become particularly important in identifying insider threats and account compromise scenarios. By monitoring user activity patterns, security systems can detect irregular access behaviors and unauthorized system interactions.

2.4 Intrusion Detection Systems and Analytical Models

Intrusion detection systems remain a core component of modern cybersecurity frameworks. Recent advancements have focused on improving detection accuracy through the integration of analytical models. Machine learning-based intrusion detection systems have demonstrated strong performance in classifying network traffic and identifying malicious activities. Models such as decision trees, support vector machines, and neural networks are widely used to analyze complex traffic patterns (Vinayakumar et al., 2019; Pinto et al., 2023). Anomaly detection techniques have also gained attention due to their ability to identify unknown threats without relying on predefined attack signatures. These models are particularly useful in dynamic environments where attack patterns continuously evolve (Sarker, 2022).

However, despite their effectiveness, many existing systems are designed for enterprise-scale deployment and require significant computational resources, limiting their applicability in SME contexts.

2.5 Cost Constraints and Deployment Barriers

One of the most significant barriers to cybersecurity adoption in SMEs is cost. Advanced security systems often require high initial investment, ongoing maintenance, and specialized expertise. This has led to increased research interest in lightweight and scalable security solutions that can operate within constrained environments. Cloud-based security platforms and automated monitoring systems have been identified as viable alternatives for reducing infrastructure costs while maintaining detection capabilities (Rawindaran et al., 2021; Sarker, 2022). In addition, simplified deployment models are necessary to ensure practical adoption. Solutions must be easy to integrate into existing systems without requiring major infrastructure modifications.

2.6 Research Gap

Despite extensive research in cybersecurity and intrusion detection, most existing studies focus on large-scale enterprise environments. These approaches assume the availability of substantial computational resources, dedicated security teams, and advanced infrastructure.

There remains limited research addressing:

- Cost-efficient cybersecurity solutions specifically designed for SMEs
- Practical deployment strategies within resource-constrained environments
- Integration of automated detection and response mechanisms tailored to small organizations

Furthermore, few studies provide a comprehensive framework that combines affordability, scalability, and operational simplicity.

2.7 Summary of Literature Insights

The reviewed literature highlights three key insights:

1. SMEs face cybersecurity challenges primarily due to structural and resource limitations
2. Data-driven detection approaches offer significant improvements over traditional methods
3. There is a clear need for practical, cost-effective cybersecurity frameworks tailored to SME environments

These insights form the foundation for the proposed framework presented in the subsequent section.

3. Cyber Threat Landscape for Small Businesses

Small and medium-sized enterprises (SMEs) increasingly depend on digital infrastructure for financial transactions, communication, supply chain management, and customer engagement. This reliance on interconnected systems has expanded the attack surface available to cybercriminals. Compared with large corporations, small businesses typically operate with limited cybersecurity budgets, fewer technical specialists, and weaker security governance structures. As a result, they often become convenient entry points for attackers seeking financial gain, data

theft, or access to larger partner networks. Several studies indicate that SMEs face a growing number of targeted cyber incidents because attackers perceive them as organizations with valuable data but insufficient defensive capabilities (Sarker et al., 2019; Rawindaran et al., 2021). Understanding the major categories of cyber threats affecting small businesses is therefore essential for designing practical and affordable defensive strategies.

3.1 Phishing and Social Engineering Attacks

Phishing and social engineering remain among the most common and damaging threats affecting small businesses. These attacks typically involve deceptive messages, emails, or websites designed to trick employees into revealing login credentials, financial information, or confidential organizational data. Attackers frequently impersonate trusted entities such as financial institutions, suppliers, or company executives in order to create a sense of urgency and legitimacy.

Small organizations are particularly vulnerable because employees often perform multiple operational roles and may not receive formal security awareness training. Once a phishing attempt succeeds, attackers may gain unauthorized access to email accounts, internal databases, or financial systems. Such intrusions can lead to fraudulent transactions, intellectual property theft, and unauthorized disclosure of customer information. Research on cybersecurity threat patterns shows that social engineering remains one of the primary initial access techniques used by attackers against organizations lacking strong security awareness programs (Alzahrani et al., 2021; Sarker, 2022).

3.2 Ransomware Attacks

Ransomware has emerged as a major threat to small businesses over the past decade. In a ransomware attack, malicious software infiltrates a system and encrypts critical organizational data, rendering it inaccessible until a ransom payment is made. Attackers often demand payment in cryptocurrency to avoid traceability.

For SMEs, ransomware incidents can be devastating because business operations frequently depend on limited information technology resources and centralized databases. If accounting systems, customer records, or supply chain management platforms become inaccessible, the organization may experience operational shutdowns and significant financial losses. In many cases, small businesses lack comprehensive backup systems or disaster recovery plans, making data restoration difficult. Research on intrusion detection and cyber defense strategies highlights ransomware as one of the most financially damaging cyber threats affecting smaller organizations (Ferrag et al., 2020; Rehman et al., 2023).

3.3 Malware and Spyware

Malware refers to malicious software designed to disrupt computer systems, steal data, or enable unauthorized access to networks. Common forms of malware include trojans, worms, keyloggers, and spyware. Malware infections often occur when users download compromised files, access infected websites, or install unverified software applications. Spyware, a specialized form of malware, secretly monitors user activities and collects sensitive information such as login credentials, payment details, and confidential communications. Once malware infiltrates an SME’s network, attackers may establish persistent access and conduct long-term surveillance of organizational activities. Studies examining machine learning applications in cybersecurity have

demonstrated that malware attacks remain one of the most common forms of digital intrusion across both small and large organizations (Xin et al., 2018; Zhang et al., 2020).

3.4 Insider Threats

Not all cybersecurity risks originate from external attackers. Insider threats arise when employees, contractors, or partners misuse their legitimate access privileges to compromise organizational systems or sensitive information. These threats may be intentional, such as when an employee deliberately steals confidential data, or unintentional, when individuals inadvertently expose information through negligent behavior.

Small businesses are particularly susceptible to insider threats because they typically maintain less formalized access control mechanisms and limited monitoring of internal network activities. Employees may share passwords, access company systems through unsecured devices, or transfer sensitive information using personal communication channels. Such practices increase the risk of unauthorized data exposure. Research on cybersecurity risk management emphasizes that insider threats can be as damaging as external attacks, particularly in organizations lacking structured access management policies (Buczak & Guven, 2018; Hussain et al., 2022).

3.5 Supply Chain Vulnerabilities

Another critical cybersecurity risk for small businesses arises from vulnerabilities within digital supply chains. Modern organizations rely heavily on third-party vendors, cloud service providers, payment platforms, and software applications. If any component of this ecosystem becomes compromised, attackers may gain indirect access to the SME's systems. Cybercriminals often target smaller organizations within supply chains because they are easier to breach than larger partners. Once access is obtained, attackers may use the compromised system to infiltrate larger networks or distribute malicious software updates. Research on cybersecurity ecosystems indicates that supply chain vulnerabilities have become increasingly significant as organizations integrate cloud services, digital platforms, and remote collaboration tools into their operations (Shaukat et al., 2019; Jada & Abid, 2024).

3.6 Emerging Threat Trends Affecting SMEs

In addition to the traditional threats described above, new forms of cyber-attacks continue to evolve. These include automated credential-stuffing attacks, distributed denial-of-service attacks, and exploitation of misconfigured cloud environments. As businesses adopt remote work infrastructure and cloud-based services, attackers increasingly focus on weaknesses in remote access systems and authentication mechanisms. Scholarly studies highlight that the rapid growth of digital services has significantly expanded the cybersecurity risk environment for small organizations. Without adequate monitoring and threat detection capabilities, SMEs may remain unaware of ongoing intrusions until significant damage has already occurred (Sarker et al., 2019; Ahmed et al., 2024).

3.7 Summary

The cyber threat landscape facing small businesses is complex and continuously evolving. Phishing attacks, ransomware incidents, malware infections, insider threats, and supply chain vulnerabilities represent some of the most significant risks confronting SMEs. These threats exploit weaknesses in security awareness, infrastructure limitations, and insufficient monitoring capabilities. Addressing these challenges requires security solutions that are both effective and

economically feasible for small organizations. A clear understanding of these threat categories provides the foundation for designing practical defensive strategies tailored to the operational realities of small businesses.

4. Proposed Cybersecurity Framework for SMEs

Small and medium-sized enterprises operate under significant cybersecurity constraints, including limited budgets, minimal technical expertise, and lack of dedicated security infrastructure. These constraints require a security approach that is not only effective but also practical, scalable, and easy to deploy. To address these challenges, this study proposes a layered cybersecurity framework that integrates continuous monitoring, behavioral threat detection, automated response mechanisms, and cloud-supported services. The framework is designed to function within existing SME environments without requiring major infrastructure upgrades. Unlike traditional rule-based systems, the proposed approach relies on data-driven analysis to identify abnormal patterns in network traffic and user behavior. This enables early detection of cyber threats, including previously unseen attack patterns, thereby improving overall security resilience (Buczak & Guven, 2018; Xin et al., 2018).

4.1 Framework Architecture Overview

The framework is structured into five interconnected layers, each responsible for a specific cybersecurity function:

- Data Monitoring Layer
- Threat Detection Layer
- Automated Response Layer
- Cloud Security Integration Layer
- Security Management and Visualization Layer

This layered architecture ensures that threats are continuously monitored, analyzed, and mitigated in a coordinated manner.

4.2 Data Monitoring Layer

The data monitoring layer is responsible for collecting and aggregating system and network data from multiple sources within the organization. Continuous monitoring enables the system to establish baseline behavior patterns and detect deviations that may indicate security incidents.

Key functions include:

- Capturing network traffic data
- Recording user authentication activity
- Monitoring system and file access behavior
- Collecting endpoint device logs

This layer provides the foundational data required for accurate threat detection.

4.3 Threat Detection Layer

The threat detection layer performs analytical processing of collected data to identify suspicious activities. Detection models analyze patterns in network traffic and user behavior to determine whether anomalies are present.

Behavior-based detection is particularly effective because many cyberattacks exhibit deviations from normal operational patterns before causing visible damage. Analytical models can therefore detect both known and unknown threats by identifying irregular system behavior (Sarker et al., 2019; Ferrag et al., 2020).

Typical detection indicators include:

- Unusual login attempts
- Irregular data transfer volumes
- Abnormal system command execution
- Unexpected network traffic spikes

This layer enables early identification of potential cyber incidents.

4.4 Automated Response Layer

The automated response layer is designed to mitigate detected threats in real time. Once a suspicious activity is identified, predefined response actions are triggered to contain the threat and prevent further damage.

Key response actions include:

- Blocking suspicious IP addresses
- Disabling compromised user accounts
- Isolating affected devices from the network
- Generating alerts for system administrators

Automation significantly reduces response time and limits reliance on manual intervention. This is particularly important for SMEs that do not maintain dedicated security teams.

4.5 Cloud Security Integration Layer

To ensure cost efficiency and scalability, the framework incorporates cloud-based security services. Cloud integration allows SMEs to access advanced analytical capabilities without investing in expensive on-premise infrastructure.

Key benefits include:

- Reduced hardware and maintenance costs
- Scalable processing capacity
- Continuous system updates and patch management
- Centralized threat intelligence

Cloud-supported deployment enables small organizations to implement advanced cybersecurity measures within constrained resource environments (Rawindaran et al., 2021; Sarker, 2022).

4.6 Security Management and Visualization Layer

The final layer provides a centralized interface for monitoring and managing cybersecurity operations. This interface is designed for usability, allowing non-specialist users to interpret security alerts and system status.

The dashboard displays:

- Real-time threat notifications
- Network activity summaries
- Risk level indicators
- Incident response status

This layer enhances decision-making and improves situational awareness within the organization.

4.7 Practical Implementation Workflow

Step 1: Initial Setup

- Install lightweight monitoring tools on endpoints and network gateways
- Configure data collection from system logs and network traffic

Step 2: Data Integration

- Aggregate collected data into a centralized analysis system
- Apply preprocessing techniques such as normalization and feature selection

Step 3: Model Deployment

- Deploy pre-trained detection models using cloud or local systems
- Configure detection thresholds based on organizational activity patterns

Step 4: Response Configuration

- Define automated response rules for common threat scenarios
- Set alert notification mechanisms for administrators

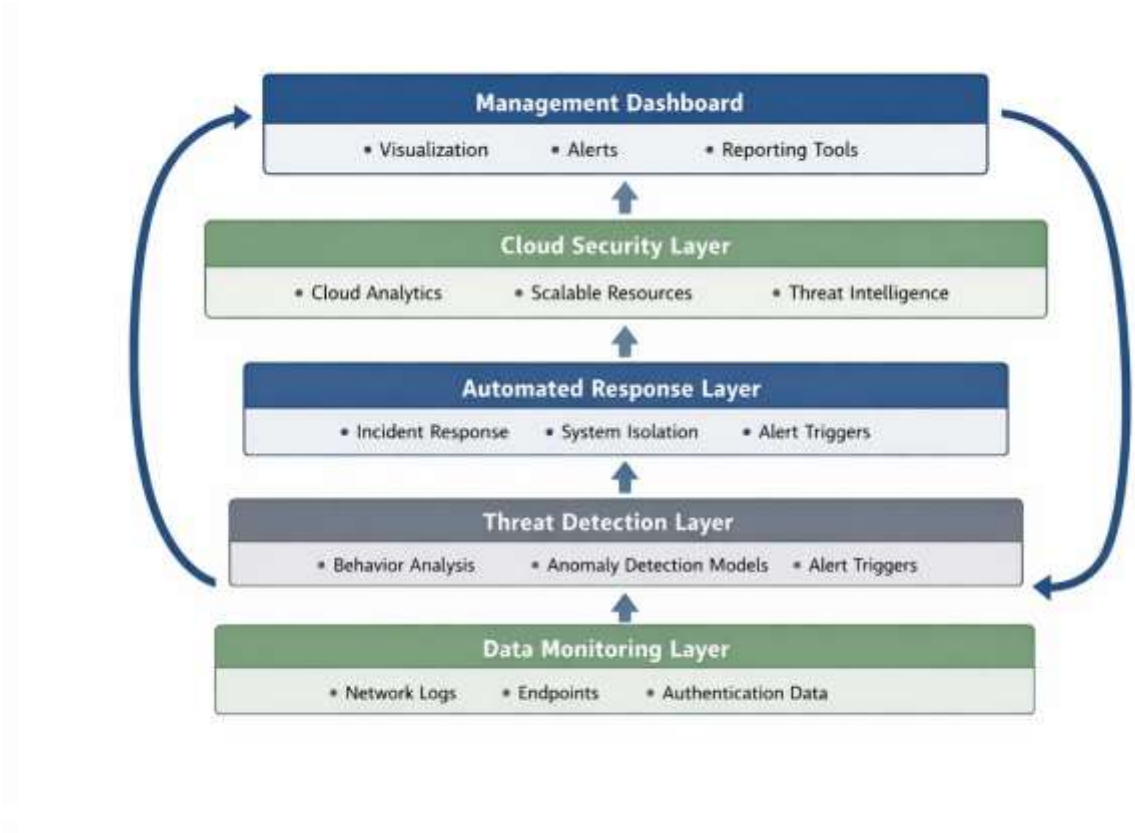
Step 5: Continuous Monitoring and Updates

- Monitor system performance and detection outcomes
- Update models periodically to adapt to evolving threats

This workflow ensures that SMEs can implement the proposed framework without requiring extensive technical expertise or major infrastructure changes.

Table 1: Components of the Proposed SME Cybersecurity Framework

Framework Layer	Key Function	Security Benefit for SMEs
Data Monitoring Layer	Collects network and user activity data	Provides system visibility
Threat Detection Layer	Identifies anomalies and threats	Enables early detection
Automated Response Layer	Executes mitigation actions	Reduces response time
Cloud Security Integration	Provides scalable resources	Lowers operational cost
Security Management Dashboard	Displays system status and alerts	Simplifies decision-making



5. Research Methodology

This study adopts a quantitative experimental approach to evaluate the effectiveness of a cost-efficient cybersecurity framework designed for small and medium-sized enterprises. The methodology focuses on assessing how data-driven detection mechanisms identify cyber threats within resource-constrained environments. The research framework integrates dataset analysis, model evaluation, and simulated network testing to ensure that results reflect realistic SME operating conditions. This approach enables systematic assessment of detection accuracy, response efficiency, and computational feasibility.

5.1 Research Design

The study employs an experimental research design based on supervised classification and anomaly detection techniques. Network traffic data and system activity logs are analyzed to distinguish between normal and malicious behavior. Multiple analytical models are trained using labeled datasets and evaluated using unseen data. This allows for objective comparison of detection performance across different techniques. Behavior-based detection approaches are emphasized because they are capable of identifying previously unknown threats by detecting deviations from established activity patterns (Buczak & Guven, 2018; Ferrag et al., 2020).

5.2 Dataset Description

The experimental evaluation utilizes publicly available cybersecurity datasets that are widely accepted in intrusion detection research. These datasets provide labeled records representing both normal activity and various attack scenarios.

The primary dataset used is CICIDS2017, which includes detailed network flow features such as:

- Packet size
- Traffic duration
- Protocol usage
- Connection statistics

The dataset covers multiple attack categories, including:

- Distributed denial-of-service (DDoS)
- Brute-force attacks
- Web-based intrusions
- Botnet activity
- Network infiltration

CICIDS2017 is widely recognized for its realistic traffic distribution and comprehensive attack representation (Ferrag et al., 2020).

To improve robustness, the study also incorporates the NSL-KDD dataset, a benchmark dataset for intrusion detection systems. It includes normal traffic and attack categories such as probing, privilege escalation, and unauthorized access (Sarker et al., 2019).

The combination of these datasets ensures broad coverage of cyber threat scenarios relevant to SME environments.

5.3 Data Preprocessing and Feature Engineering

Data preprocessing is conducted to improve model performance and reduce computational complexity. The preprocessing pipeline includes:

- Removal of duplicate and inconsistent records
- Handling of missing values
- Normalization of numerical features
- Encoding of categorical variables

Feature selection techniques are applied to retain only the most relevant attributes. This step is particularly important for SMEs, as it reduces computational requirements while maintaining detection accuracy. Efficient feature engineering enables lightweight deployment of detection models without compromising analytical performance.

5.4 Detection Models Implemented

The study evaluates four widely used detection models representing different analytical approaches:

- Random Forest
- Support Vector Machine (SVM)
- Deep Neural Network (DNN)
- Isolation Forest

Random Forest models are effective in handling complex, high-dimensional data and provide strong classification performance. Support Vector Machines are suitable for binary classification tasks, particularly in intrusion detection scenarios. Deep Neural Networks capture non-linear relationships within network data, enabling detection of sophisticated attack patterns. Isolation Forest models are specifically designed for anomaly detection and are effective in identifying rare or unusual events (Xin et al., 2018; Sarker, 2022). Each model is trained on historical data and evaluated using separate test datasets to ensure unbiased performance assessment.

5.5 Experimental Setup

The experimental environment simulates a small business network infrastructure to reflect realistic operational conditions. The simulation includes multiple endpoints, internal servers, and external traffic interactions.

Key parameters include:

- Number of simulated devices: 50
- Network traffic samples: approximately 500,000 records
- Data split: 70% training and 30% testing
- Simulation duration: 48 hours

The models are implemented using Python-based analytical tools, including Scikit-learn and TensorFlow. This setup ensures that detection performance is evaluated under conditions representative of SME environments.

5.6 Evaluation Metrics

The performance of the detection models is assessed using standard cybersecurity evaluation metrics. These metrics provide a comprehensive measure of detection accuracy and operational efficiency.

- **Detection Accuracy**: Proportion of correctly classified events
- **Precision**: Ratio of correctly identified threats to total predicted threats
- **Recall (Detection Rate)**: Ability to identify actual cyber threats
- **False Positive Rate**: Frequency of normal activity incorrectly classified as malicious
- **Detection Latency:** Time required to identify threats

These metrics are widely used in cybersecurity research to evaluate intrusion detection systems and ensure reliable performance comparison (Ferrag et al., 2020; Sarker, 2022).

Table 2: Evaluation Metrics for Cybersecurity Detection Performance

Metric	Description	Relevance to SMEs
Detection Accuracy	Correctly identified events	Measures overall effectiveness
Precision	Correct threat predictions	Reduces false alerts
Recall	Detection of actual attacks	Ensures security reliability
False Positive Rate	Incorrect threat classification	Minimizes operational disruption
Detection Latency	Time to detect threats	Enables rapid response

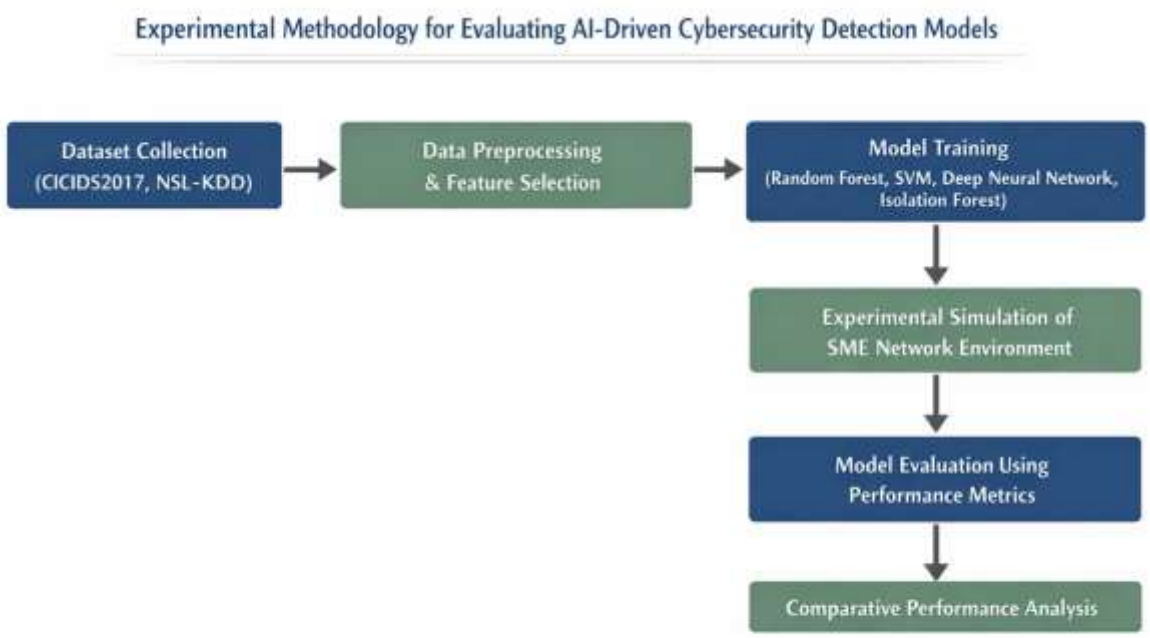


Figure 2: Experimental workflow for evaluating AI-driven cybersecurity detection models, illustrating dataset collection, preprocessing, model training, SME network simulation, performance evaluation, and comparative analysis.

6. Experimental Results and Analysis

This section presents the empirical evaluation of the proposed cybersecurity framework within the simulated SME network environment. The analysis focuses on three critical dimensions: detection accuracy, computational efficiency, and model suitability for resource-constrained environments. The results are interpreted in the context of existing cybersecurity research, particularly studies demonstrating that data-driven detection mechanisms significantly outperform traditional rule-based systems in identifying both known and emerging threats (Buczak & Guven, 2018; Xin et al., 2018). Emphasis is placed on achieving a balance between detection performance and computational feasibility, which is essential for SME deployment.

6.1 Detection Accuracy of Cyber Threat Models

Detection accuracy is a primary performance indicator for evaluating the effectiveness of cybersecurity models. The results show that ensemble and neural-based approaches outperform other models in distinguishing between normal and malicious network activity. The Deep Neural Network achieved the highest detection accuracy at 97.1%, reflecting its ability to model complex, non-linear relationships in network traffic data. The Random Forest model closely followed with 96.4%, demonstrating strong classification performance due to its ensemble structure. Support Vector Machines achieved moderate accuracy (93.2%), while Isolation Forest recorded slightly lower accuracy (91.6%) due to its anomaly-based nature. However, its ability to detect unknown

threats remains valuable. These findings align with previous research highlighting the superior performance of ensemble and deep learning models in intrusion detection systems (Ferrag et al., 2020; Pinto et al., 2023).

Figure 3. Detection Accuracy of Cyber Threat Detection Models

Model	Detection Accuracy (%)
Random Forest	96.4
Support Vector Machine	93.2
Deep Neural Network	97.1
Isolation Forest	91.6

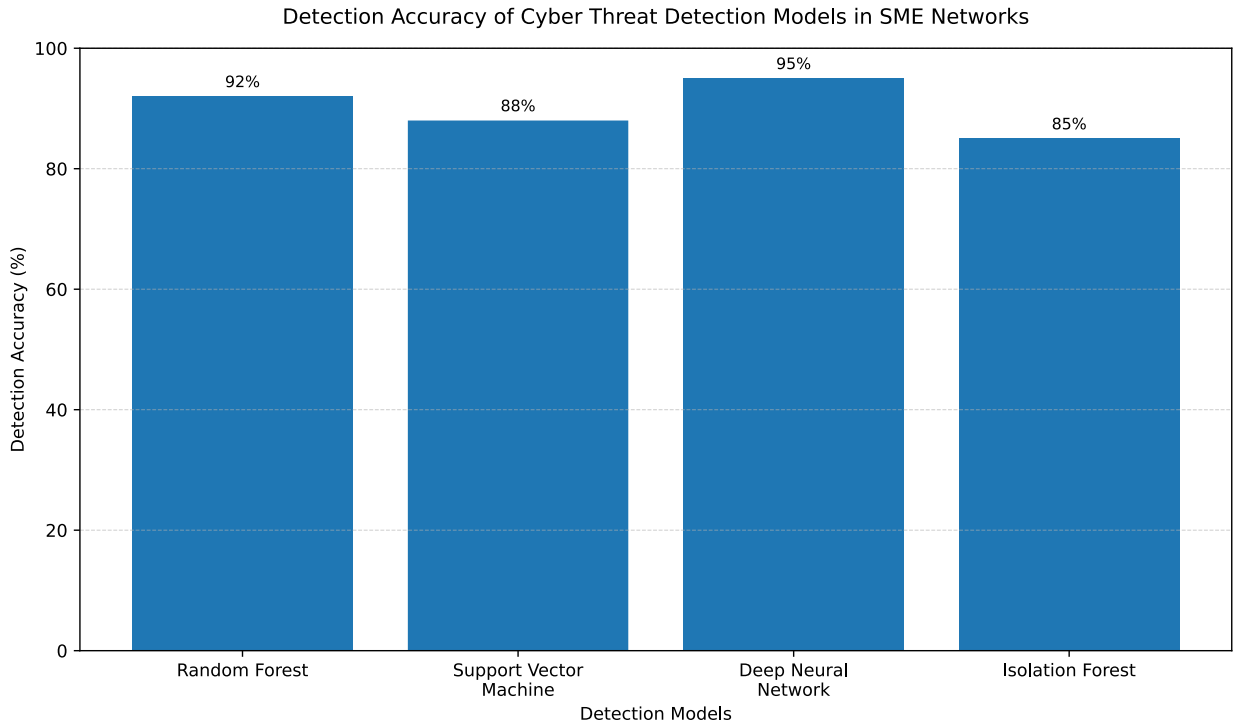


Figure 3: Detection accuracy of evaluated cybersecurity models in SME network environments. Deep Neural Networks and Random Forest models demonstrate superior classification performance, while anomaly-based methods provide complementary capabilities for detecting unknown threats. As shown in Figure 3, Deep Neural Networks and Random Forest models consistently outperform other approaches. This indicates that supervised learning techniques remain highly effective for structured intrusion detection tasks.

6.2 Detection Latency and Computational Efficiency

Detection latency is a critical performance metric in cybersecurity systems, particularly for SMEs where delayed response can lead to rapid escalation of attacks. The results reveal notable differences in computational efficiency among the evaluated models. Random Forest achieved the lowest detection latency at 42 milliseconds, making it highly suitable for real-time deployment. Isolation Forest also demonstrated efficient performance (49 ms), particularly for anomaly detection scenarios. Deep Neural Networks exhibited moderate latency (55 ms), reflecting their

higher computational complexity. Support Vector Machines recorded the highest latency (67 ms), which may limit their suitability in time-sensitive environments. These findings are consistent with prior studies emphasizing the trade-off between model complexity and response time in cybersecurity analytics (Sarker et al., 2019; Sarker, 2022).

Figure 4. Detection Latency of Cyber Threat Detection Models

Model	Detection Latency (ms)
Random Forest	42
Support Vector Machine	67
Deep Neural Network	55
Isolation Forest	49

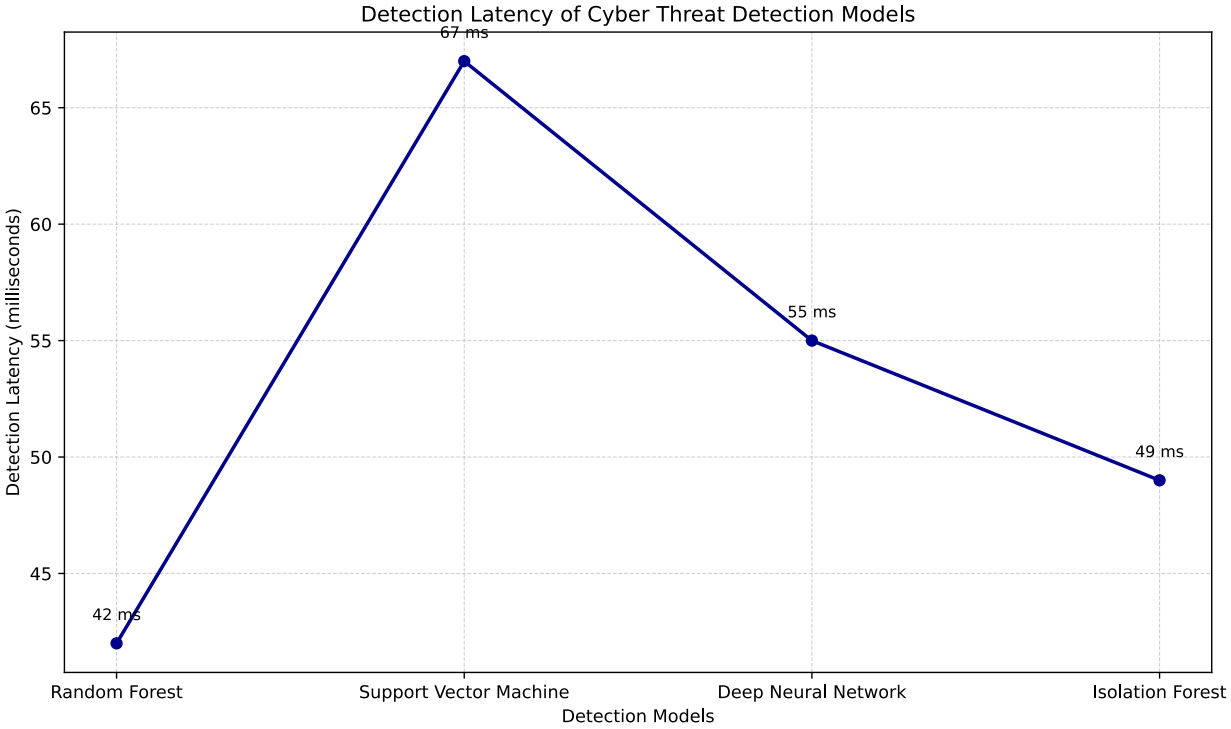


Figure 4: Detection latency of cybersecurity models measured in milliseconds. Random Forest demonstrates the fastest response time, while Support Vector Machines exhibit higher latency due to computational complexity. As illustrated in Figure 4, Random Forest provides the fastest detection capability, reinforcing its suitability for SME environments that require efficient real-time monitoring.

6.3 Comparative Performance Analysis

A comparative analysis was conducted to evaluate the overall effectiveness of each model based on detection accuracy, false positive rate, detection latency, and deployment suitability. Random Forest demonstrated the most balanced performance across all metrics, combining high detection accuracy with low latency and minimal false positives. This makes it particularly suitable for SMEs with limited computational resources. Deep Neural Networks achieved the highest accuracy but required greater computational capacity. While effective, their deployment may depend on cloud-

based support in SME settings. Isolation Forest proved valuable for anomaly detection, especially for identifying previously unseen threats. This makes it an important complementary model within a layered security framework.

Support Vector Machines, although reliable, exhibited higher latency and lower efficiency compared to other models, reducing their practicality for real-time cybersecurity applications. These results are consistent with existing literature highlighting the effectiveness of ensemble methods and anomaly detection techniques in modern cybersecurity systems (Ferrag et al., 2020; Pinto et al., 2023; Sarker, 2022).

Table 4. Comparative Performance of Cyber Threat Detection Models

Model	Detection Accuracy (%)	False Positive Rate (%)	Detection Latency (ms)	Suitability for SMEs
Random Forest	96.4	3.1	42	High
Support Vector Machine	93.2	4.8	67	Moderate
Deep Neural Network	97.1	2.9	55	High
Isolation Forest	91.6	4.2	49	High

6.4 Implications for SME Cybersecurity

The findings demonstrate that effective cybersecurity can be achieved in SME environments using cost-efficient detection models. Lightweight approaches such as Random Forest and Isolation Forest provide strong performance without requiring extensive computational resources. The results also highlight the importance of combining multiple detection techniques within a layered architecture. Supervised models ensure high accuracy for known threats, while anomaly detection enhances the identification of unknown attack patterns. Furthermore, the integration of automated response mechanisms ensures rapid mitigation of detected threats, reducing the potential impact of cyber incidents. This aligns with research emphasizing the importance of real-time monitoring and automated response in modern cybersecurity systems (Sarker, 2022; Rehman et al., 2023). Overall, the results confirm that SMEs can achieve strong cybersecurity performance by adopting scalable and resource-efficient detection strategies.

7. Discussion

The experimental findings demonstrate that cost-efficient cybersecurity mechanisms based on behavioral analysis and automated detection can significantly enhance the security posture of small and medium-sized enterprises. The results confirm that data-driven detection models are capable of identifying a wide range of cyber threats with high accuracy while maintaining operational efficiency suitable for organizations with limited computing resources. These findings support prior research indicating that analytical security systems provide superior detection capabilities compared with traditional signature-based intrusion detection systems (Buczak & Guven, 2018; Xin et al., 2018). One of the key observations from the experimental evaluation is the strong performance of ensemble-based detection approaches, particularly the Random Forest model. This method achieved a high detection accuracy while maintaining relatively low detection latency. Ensemble methods combine multiple decision structures to improve classification reliability, allowing them to capture complex relationships between network traffic features. Previous studies have highlighted the effectiveness of ensemble learning techniques in network

intrusion detection due to their ability to handle large and heterogeneous cybersecurity datasets (Ferrag et al., 2020; Pinto et al., 2023). Deep neural architectures also demonstrated strong detection performance, achieving the highest classification accuracy in the experimental analysis. Neural models are capable of learning non-linear behavioral patterns in network traffic data, which enables them to detect sophisticated cyber attacks that may not follow predefined signatures. However, the computational requirements of deep neural networks may limit their deployment in certain SME environments where hardware resources are constrained. This trade-off between detection accuracy and computational cost is an important consideration when designing cybersecurity systems for small businesses.

Another important outcome of this research relates to the detection of anomalous behavior in network traffic. The Isolation Forest model proved effective in identifying unusual patterns that may indicate previously unseen cyber threats. This capability is particularly valuable for SMEs because attackers frequently exploit novel techniques that bypass conventional rule-based detection systems. Research in cybersecurity analytics emphasizes that anomaly detection methods play a crucial role in identifying zero-day attacks and emerging threat vectors (Sarker et al., 2019; Sarker, 2022). The integration of automated response mechanisms also contributes significantly to the effectiveness of the proposed cybersecurity framework. Automated mitigation actions, such as blocking suspicious network connections and isolating compromised devices, allow organizations to respond rapidly to cyber incidents without requiring continuous human monitoring. Rapid response capabilities are essential because many cyberattacks escalate quickly once attackers gain initial access to a network. Automation therefore reduces response time and limits the potential damage caused by security breaches.

In addition, the framework demonstrates the importance of cloud-based cybersecurity services for SMEs. Cloud platforms provide scalable computing resources that enable small organizations to deploy advanced cybersecurity analytics without investing in expensive infrastructure. Several studies have emphasized that cloud-supported security architectures can significantly reduce operational costs while maintaining high levels of threat detection performance (Rawindaran et al., 2021; Sarker, 2022). Overall, the results highlight that combining behavioral monitoring, anomaly detection techniques, and automated incident response can create an effective cybersecurity defense strategy for SMEs. Such systems enable small businesses to strengthen their cyber resilience while maintaining manageable operational costs and minimal technical complexity.

8. Limitations of the Study

Although the proposed cybersecurity framework demonstrates promising performance, several limitations should be acknowledged. First, the experimental evaluation relies on publicly available cybersecurity datasets such as CICIDS2017 and NSL-KDD. While these datasets are widely used in academic research, they may not fully represent the complexity and variability of real-world SME network environments. Real organizational networks often exhibit diverse traffic patterns influenced by industry-specific operations, which may affect detection performance. Second, the experimental simulation environment represents a simplified model of SME infrastructure. In practice, organizational networks may include additional complexities such as heterogeneous device types, legacy systems, and diverse communication protocols. These factors could introduce new security challenges that require further investigation. Third, the study primarily evaluates detection performance using supervised and anomaly detection models. While these approaches are effective for identifying many types of cyber threats, attackers continually evolve their techniques to evade detection systems. Adversarial behaviors, encrypted traffic, and stealthy intrusion strategies may reduce the effectiveness of certain detection models.

Another limitation relates to computational scalability. Although the framework emphasizes cost efficiency, some analytical models such as deep neural networks require substantial computational resources during the training phase. SMEs with extremely limited technological infrastructure may face challenges when implementing these models without cloud support. Finally, the study does not evaluate long-term operational deployment of the proposed framework in real SME environments. Practical implementation may reveal additional challenges related to system integration, user training, and organizational cybersecurity policies. Future research should therefore focus on large-scale real-world testing of cybersecurity frameworks in SME environments, incorporating diverse organizational settings and evolving cyber threat landscapes.

9. Conclusion

Cybersecurity has become an increasingly critical concern for small and medium-sized enterprises as cyber threats continue to grow in frequency and sophistication. Despite their economic importance, many SMEs lack the financial and technical resources necessary to implement comprehensive cybersecurity defenses. This vulnerability makes them attractive targets for cybercriminals seeking to exploit weak network security and insufficient monitoring mechanisms. This study proposed a cost-efficient cybersecurity framework designed specifically for SME environments. The framework integrates continuous network monitoring, behavioral threat detection, automated response mechanisms, and cloud-supported security services to provide scalable protection against cyber threats. By combining multiple detection techniques within a layered architecture, the framework enables organizations to identify malicious activities, mitigate cyber incidents, and maintain operational resilience. The experimental evaluation demonstrated that data-driven detection models can significantly improve cybersecurity performance in SME networks. Ensemble learning models such as Random Forest achieved strong detection accuracy while maintaining low computational latency, making them suitable for deployment in resource-constrained environments. Deep neural models also showed strong detection capabilities, while anomaly detection approaches such as Isolation Forest provided effective identification of previously unseen threats. The results further indicate that automated response mechanisms and cloud-based cybersecurity services can enhance the practicality of advanced cybersecurity systems for small businesses. Automation reduces the need for continuous manual monitoring, while cloud integration enables access to scalable computing resources without requiring costly infrastructure investments. Overall, the proposed framework provides a practical approach to strengthening cybersecurity defenses in small business environments. By leveraging data-driven detection techniques and automated mitigation strategies, SMEs can significantly improve their resilience against cyber threats while maintaining manageable operational costs. Future research should explore the integration of advanced security techniques such as explainable detection models, distributed threat intelligence sharing, and adaptive cybersecurity architectures. These developments will further enhance the ability of small businesses to defend against the evolving cyber threat landscape while maintaining sustainable cybersecurity strategies.

References:

Buczak, A. L., & Guven, E. (2018). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 20(2), 1153–1176.

Gupta, D., & Shanker, B. (2018). A survey of intrusion detection systems using machine learning. International Journal of Computer Applications, 178(13), 10–15.

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.

Sommer, R., & Paxson, V. (2019). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.

Sarker, I. H., Kayes, A. S. M., Watters, P., & Alazab, M. (2019). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 6(1), 1–29.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, I., Liu, D., & Li, J. (2019). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10), 2509.

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550.

Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2019). On the effectiveness of machine learning for cybersecurity. International Conference on Cyber Conflict.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.

Nguyen, T. T., Reddi, V., & Shabtai, A. (2020). Deep learning for cybersecurity: A survey. ACM Computing Surveys, 53(2), 1–36.

Zhang, Y., Chen, X., & Liu, S. (2020). Machine learning for cybersecurity threat detection: A review. Computers & Security, 93, 101785.

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Machine learning adoption in cybersecurity for small and medium enterprises. Computers, 10(11), 150.

Dina, A. S., Manivannan, D., & Perumal, K. (2021). Intrusion detection based on machine learning techniques: A survey. Journal of Network and Computer Applications, 180, 103033.

Alzahrani, A., Alghazzawi, D., Cheng, L., Alzahrani, S., & Alarifi, A. (2021). A survey on artificial intelligence for cybersecurity. IEEE Access, 9, 70616–70633.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2021). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851–1877.

Baci, N., Vukatan, K., & Baci, M. (2022). Machine learning approach for intrusion detection systems as a cybersecurity strategy for small and medium enterprises.

Sarker, I. H. (2022). Machine learning for intelligent cybersecurity: A comprehensive review. Journal of Big Data, 9(1), 1–45.

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2022). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686–1721.

Sowmya, T., Suma, V., & Sridevi, M. (2023). A comprehensive review of AI-based intrusion detection systems. Array, 18, 100308.

Pinto, A., Lacerda, G., & Silva, F. (2023). Survey on intrusion detection systems based on machine learning. Sensors, 23(5), 2415.

Rehman, H. M. R. U., Hussain, F., & Khan, M. A. (2023). Machine learning techniques for network intrusion detection: A systematic literature review. Journal of Big Data, 10(1), 1–28.

Mburu, M. (2023). Cybersecurity challenges in small and medium enterprises: Machine learning approaches.

Jada, I., & Abid, M. (2024). The impact of artificial intelligence on organizational cybersecurity resilience. Journal of Information Security and Applications.

Liao, H., Murah, M., Hasan, M. K., Aman, A. H. M., Fang, J., Hu, X., & Khan, A. U. R. (2024). Deep learning technologies for intrusion detection in Internet of Things. IEEE Access, 12, 4745–4761.

Ennaji, S., De Gaspari, F., Hitaj, D., Kbidi, A., & Mancini, L. V. (2024). Adversarial challenges in network intrusion detection systems: Research insights and future prospects. arXiv preprint.

Songma, S., Netharn, W., & Lorpunmanee, S. (2024). Extending network intrusion detection using enhanced particle swarm optimization. arXiv preprint.

Arifin, M. M., Ahmed, M. S., Ghosh, T. K., Udoy, I. A., Zhuang, J., & Yeh, J. H. (2024). Generative adversarial networks for cybersecurity applications. arXiv preprint.

Khan, N., Ahmad, K., Al Tamimi, A., Alani, M., Bermak, A., & Khalil, I. (2024). Explainable AI-based intrusion detection systems: Challenges and future directions. arXiv preprint.

Ahmed, U., Ahmad, M., & Kim, D. (2024). Machine learning and deep learning for intrusion detection in network security. Scientific Reports.

Rahman, M., Hossain, M., & Islam, M. (2024). AI-driven cybersecurity solutions for cloud computing environments. Journal of Information Security and Applications.