IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 6, Ser. 3 (Nov. – Dec. 2025), PP 39-49
www.iosrjournals.org

AI-Driven Cyber Defense: Transforming Threat Detection For Small And Mid-Sized Enterprises

Olamide Oluwasegun Oloyede

Abstract
Small and mid-sized enterprises (SMEs) are increasingly targeted by sophisticated cyber adversaries but often lack the security personnel, budget, and tooling needed for real-time threat detection and response. Traditional signature-based defenses and manual security workflows are insufficient against polymorphic malware, zero-day exploits, and advanced persistent threats. This paper examines how artificial intelligence (AI) and machine learning (ML) are reshaping SME cybersecurity by powering adaptive threat-detection architectures, including behavioral analytics, Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and federated learning-based intelligence sharing. The study synthesizes empirical case evidence showing substantial gains in detection accuracy, false-positive reduction, dwell-time reduction, and compliance efficiency. The analysis further explores ethical and operational imperatives such as algorithmic transparency, human-in-the-loop governance, and alignment with U.S. regulatory standards (NIST, ISO/IEC 27001, CISA) to ensure responsible deployment. It also evaluates policy and national security implications, emphasizing the role of AI-enabled SMEs in strengthening supply-chain security and economic resilience. Findings demonstrate that when implemented with proper governance, AI augments limited SME resources, accelerates incident response, and materially enhances cyber-resilience. However, success requires staged adoption, proper oversight, and collaborative intelligence frameworks to manage risks associated with model drift, adversarial manipulation, and privacy exposure. The study concludes with strategic recommendations for SMEs and policymakers to expand access to AI-driven security while ensuring transparency, accountability, and ecosystem coordination.

Keywords And Phrases: *AI-Driven Cybersecurity; SMEs; Threat Detection; EDR; NDR; Federated Learning; Cybersecurity Automation; Digital Resilience; Supply Chain Security; NIST; ISO/IEC 27001; CISA; Data Privacy; Zero-Day Detection.*

Date of Submission: 04-12-2025 Date of Acceptance: 14-12-2025

I. Introduction

Cybercriminals are setting their sights more and more on small and mid-sized businesses, making them prime targets. Recent findings reveal that nearly 43% of cyber-attacks target small businesses, while around 46% of data breaches affect organizations with fewer than 1,000 employees (BDEmerson, 2024). A report by NAVEX in 2024 reported that In 2023, 61% of cyberattacks targeted SMBs, with 48% experiencing incidents between 2022 and 2023, while breach costs averaged $3.31 million for firms under 500 employees—up 13.4%—and $3.29 million for those with 500–1,000 employees, though SMBs saw a sharper 21.4% rise, as 92% of breaches stemmed from system intrusions, social engineering, and basic web application attacks. These figures convey just how widespread and serious cyber threats have become for businesses that typically don't have the extensive resources or defenses of large corporations.

SMEs typically operate with constrained budgets, smaller IT and security teams, and less advanced infrastructure than large enterprises. As a result, they may lack resilience against increasingly sophisticated attack vectors such as ransomware, supply-chain exploits, or social-engineering campaigns. Indeed, research emphasises that SMEs are particularly vulnerable because they are "unaware, unfunded and uneducated" when it comes to cybersecurity readiness and resilience. Carlos et al., 2023; Keepnet Labs, 2025; Tetteh, 2024); Ejaz et al., 2024)

Traditional cybersecurity measures, such as signature-based antivirus programs and rule-based intrusion detection systems (IDS), struggle to keep pace with the rising threat, where attackers use sophisticated, adaptive techniques that often bypass static defenses (Alladean et al., 2024). These legacy security tools that depend on known-threat signatures or fixed rulesets often fail against evolving threats, and SMEs struggle to implement and maintain them due to limited telemetry, staffing, and budget constraints. In 2021, 61% of SMBs experienced a cyber-attack (Saha & Anwar, 2024), with the Verizon Data Breach Investigations Report noting a sharp rise in such incidents over recent years, and 82% of ransomware attacks specifically targeting businesses with 1,000 or fewer employees. Cybersecurity breaches can lead to longer dwell times, reduced detection rates,

and severe operational fallout, where a study found that 60% of small businesses closed within six months of an attack, while also jeopardizing data integrity, financial stability, and reputational trust (Boswell, 2023).

Artificial intelligence (AI) and machine learning (ML) are transforming cyber defense and threat hunting by replacing reactive, signature-based detection with predictive, adaptive, and autonomous security models; however, their success depends on ongoing innovation, resilience against adversarial tactics, and cross-disciplinary collaboration to address the constantly evolving threat (Mohamed, 2025). Rather than simply reacting to known threat patterns, AI/ML systems can learn behavioural baselines, detect anomalies, adapt to evolving tactics and automate response steps in near-real time. For SMEs, this shift levels the cybersecurity playing field with larger enterprises and also, through techniques like federated learning, enables collaborative model training that enhances detection while safeguarding sensitive data privacy (Betul et al., 2024).

This article examines how AI and ML are reshaping threat detection and response for SMEs, while emphasizing practical, scalable, and cost-effective cybersecurity solutions designed to meet their needs. It contrasts traditional antivirus and intrusion detection systems with adaptive AI-based architectures, examines technical approaches such as behavioral analytics, anomaly detection, and federated learning for privacy-preserving threat intelligence sharing, and discusses key implementation challenges, ethical considerations, and strategic recommendations for SME adoption.

This research seeks to answer several key questions: How are artificial intelligence (AI) and machine learning (ML) redefining threat detection and response for small and medium-sized enterprises (SMEs)? What technical, ethical, and operational implications arise from adopting AI-based security frameworks in these organizations? And how can SMEs effectively implement such solutions while staying within budgetary limits and meeting regulatory compliance requirements?

II. Literature Review

Evolution of Threat Detection Models

Intrusion and malware detection have progressed from static, signature-based methods to dynamic, behavior-drive,n and AI-enabled systems, as early antivirus tools, though efficient against known threats, struggled to detect novel, polymorphic, and zero-day attacks due to their reliance on predefined patterns. Malware scanners commonly integrate signature-based and anomaly-based approaches through static, dynamic, or hybrid engines to flag deviations from baseline system activity (Smallman, 2024). However, while signature techniques delivered high precision on known threats, they consistently demonstrated weak performance against rising and complex infections.

As adversarial tactics grew more sophisticated, cybersecurity research pivoted toward heuristic, behavioral, and anomaly-based detection, with Arora (2025) noting that static signature methods proved inadequate against modern threats, prompting the development of adaptive models that detect deviations from established norms. AI-driven systems address this gap by leveraging models capable of learning behavioral patterns and predicting malicious activity, enabling continuous improvement in identifying zero-day exploits, advanced persistent threats, and insider-driven compromises (Yerabolu, 2025). These studies validate the operational advantages of transitioning from static, signature-based detection to dynamic, AI-enabled approaches, demonstrating improved adaptability, faster threat recognition, and enhanced resilience against novel cyberattacks.

Dunsin (2024) demonstrates that AI-enabled threat classification in IoT settings achieved 91.8% detection accuracy and reduced false positives by 84% compared to rule-based systems, emphasizing the superiority of intelligent, context-aware detection pipelines. Furthermore, Zoppi et al. (2021) report that unsupervised learning techniques for insider threat detection established reliable behavioral baselines within a short period, with accuracy improving and stabilizing across enterprise-scale telemetry environments.

Comparative research reinforces the trade-offs inherent in traditional and intelligent models. Signature-based intrusion detection systems maintain high precision and low false-positive rates but struggle with adaptability and require continuous manual rule updates, while anomaly-driven systems deliver superior capability to detect new threats at the cost of increased tuning complexity and false alarms (Sajad et al., 2021). Recognizing these complementary strengths, modern defense paradigms increasingly adopt hybrid architectures, combining signature-based engines for confirmed threat patterns with anomaly-driven and ML-enhanced modules for proactive, context-adaptive defense. Kamboj et al. (2025) similarly conclude that hybrid IDS frameworks provide the most resilient security posture for SMEs and larger organizations by unifying high detection accuracy with adaptive learning mechanisms capable of confronting diverse and evolving cyber-attacks.

Machine Learning in Cyber Defense

Machine learning applications in cybersecurity broadly fall into supervised, unsupervised, and reinforcement learning paradigms, each contributing distinct capabilities to threat detection and response.

Supervised learning employs labeled datasets to recognize known attack signatures, unsupervised learning identifies anomalies within unlabeled datasets to uncover previously unseen threats, and reinforcement learning supports adaptive, reward-driven defense strategies in dynamic network environments (Oyebode & Mapfaza, 2025). Collectively, these models enable cyber defense systems to move beyond static rule sets toward predictive, adaptive, and autonomous threat mitigation.

Supervised algorithms — including decision trees, support vector machines (SVMs), and deep neural networks — remain widely adopted for malware detection and labeled intrusion detection tasks where adequate training data exists. Conversely, unsupervised and semi-supervised methods such as clustering and autoencoders are increasingly applied to insider-threat detection, advanced persistent threat (APT) identification, and zero-day discovery, particularly in low-telemetry environments. Reinforcement learning techniques are gaining momentum for automated threat response and continuous policy optimization in threat-active network systems (Suman et al., 2024; Loza, 2025). Deep learning architectures such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), generative adversarial networks (GANs), and autoencoders significantly enhance feature extraction from raw network flows, binaries, logs, and user activity streams, although concerns persist regarding data requirements, interpretability, scalability, and vulnerability to adversarial manipulation (Hussain, 2024).

Recent scholarship underscores the practical deployment of these models. Mohamed (2025) highlights the role of machine learning in intrusion detection and prevention systems, noting its effectiveness in detecting insider threats and APT behaviors via behavioral clustering and anomaly-based monitoring. Decision trees and ensemble methods, such as random forests and gradient boosting, are emphasized for their interpretability and strong performance on classification tasks with heterogeneous or noisy data (Genuario et al., 2024). Neural-network-based systems demonstrate strong performance in learning complex malicious behavior patterns and improving network defense automation (Shevchuk & Martsenyuk, 2024). SVMs are similarly recognized for accuracy and computational efficiency in security classification workloads, particularly in environments requiring rapid threat scoring (Dubey et al., 2024).

Deep learning's transformative impact extends to phishing detection, malware classification, insider-threat monitoring, and encrypted traffic analysis, where CNNs and RNNs autonomously extract hierarchical features at scale and sustain high classification performance across diverse telemetry sources (Okafor, 2025). While interpretable models like decision trees offer transparency and regulatory alignment, they may underperform in highly complex feature spaces (Montgomery, 2024; Li et al., 2021). Deep architectures, although highly accurate, impose greater computational demands and require large, high-quality labeled datasets — constraints that hold particular relevance for resource-constrained small and mid-sized enterprises. Consequently, contemporary research stresses the importance of explainable machine learning (XAI) to ensure analyst trust, auditability, and governance compliance in AI-mediated security operations.

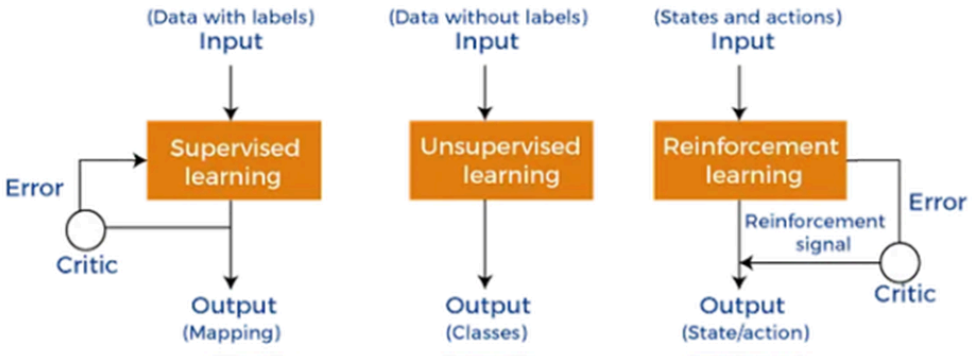

Figure 1: Classification of Machine Learning Model
Source: Loza (2025)

AI-Powered Threat Intelligence and Automation

AI integration into threat intelligence and Security Information and Event Management (SIEM) systems has risen as a foundational capability in modern cybersecurity. SIEM platforms provide centralized log aggregation, event correlation, and security alerting across enterprise architectures, enabling continuous visibility and incident response coordination (Oladoja, 2022). Without human intervention, AI-driven systems can autonomously perform predefined actions like isolating compromised devices or blocking suspicious IP addresses, enabling SMEs to respond swiftly and minimize the risk of extended damage (Alhogail & Alsabih, 2021). Machine learning enhances these systems by introducing automated correlation across high-volume

telemetry, building behavioural baselines, and assigning dynamic risk scores, thereby reducing human-driven triage and improving detection of subtle and rising threats (Kapera & Niemiec, 2025).

SIEM systems increasingly incorporate User and Entity Behaviour Analytics (UEBA) to detect anomalous insider behaviour, lateral movement, and stealthy command-and-control patterns, often operating alongside Security Orchestration, Automation, and Response (SOAR) platforms that execute automated playbooks based on SIEM alerts. The effectiveness of SOAR workflows remains closely linked to SIEM alert fidelity, making AI-driven signal enrichment and noise reduction critical for operational maturity (Ban et al., 2023). Empirical studies demonstrate that AI-enabled SIEM architectures accelerate time-to-detect and time-to-respond by leveraging big-data analytics, real-time anomaly detection, and automated response triggers, thus compensating for analyst shortages and the increasing volume and complexity of cyber events (Srinivas, 2023).

Natural Language Processing (NLP) has also become instrumental in cyber-threat intelligence automation. Rising transformer-based NLP techniques extract indicators of compromise (IOCs), threat tactics, and relationship entities from adversary reports, threat feeds, and unstructured advisories—translating natural-language security intelligence into machine-actionable formats (Prasasthy et al., 2025). Oladoja (2022) notes that the transformer architecture represents a pivotal advancement over RNN and CNN-based methods due to its self-attention mechanism, which supports context-aware interpretation of full text sequences. Studies confirm growing use of transformer-driven threat intelligence pipelines for document classification, entity recognition, and automated threat summarization, although domain-specific vocabulary, scarce labelled datasets, and false-signal propagation remain active research concerns (Ogundairo & Broklyn, 2024; Marco et al., 2025). However, the adoption of these systems requires stronger model governance to mitigate the risks of inaccurate inference, model drift, and intelligence contamination, particularly as adversaries increasingly deploy ML-driven deception and adversarial techniques.

Challenges in SME Adoption

Despite advances in AI-based cybersecurity, small and medium-sized enterprises (SMEs) face distinct barriers to adoption. As cyber threats grow more complex and frequent, SMEs struggle to maintain strong defenses amid limited financial and technical resources (Ejaz & Matthew, 2024). Empirical studies consistently highlight constrained budgets, workforce shortages in AI/ML expertise, limited security telemetry, and integration difficulties as key inhibitors to adoption (Keepnet Labs, 2025; Tetteh, 2024; Marta et al., 2024). Salluh (2024) notes that SMEs often operate with weak security protocols, insufficient employee training, and difficulty managing large-scale data streams, recommending a multipronged strategy incorporating modern defensive tools, routine security audits, and workforce education to strengthen cyber resilience.

Institutional and regulatory considerations also pose challenges that complicate AI cybersecurity deployments. Data privacy requirements, cross-organizational intelligence sharing, and the need for transparent model governance impose burdens that smaller enterprises are often ill-equipped to manage. Recent studies on AI uptake in SMEs emphasize the necessity of lightweight, privacy-preserving architectures, such as federated and transfer learning, and support for vendor-managed AI security services aligned with SME operational realities (Sánchez et al., 2025). Ethical and operational risks further shape adoption choices, including model bias, opaque decision-making, and automated false positives that can disrupt core business operations, underscoring the importance of human-in-the-loop oversight and strong governance frameworks.

III. Methodological Framework

This study adopts a rigorous scholarly methodology grounded in comparative analysis, validated secondary data, and structured evaluation criteria. The research integrates academic literature, industry threat-intelligence reports, and real-world case studies to examine the evolution and performance of AI-driven threat-detection systems within small and mid-sized enterprise contexts.

A structured comparative framework is used to evaluate traditional cybersecurity systems such as signature-based intrusion detection and rule-driven security information and event management (SIEM) against modern AI-enabled models, including behavior-based detection, supervised and unsupervised machine-learning classifiers, and federated threat-intelligence networks. The comparison focuses on detection methodology, operational adaptability, accuracy in identifying advanced threats, scalability, and suitability for SME environments with limited security resources. The study draws on credible secondary sources, including peer-reviewed cybersecurity journals, government cybersecurity guidance, and authoritative industry threat-intelligence datasets. Data points are extracted from vendor-validated performance case studies, NIST publications, CISA advisories, and independent cybersecurity research institutions.

A systems-based, risk-driven analytical model is used to evaluate the impact of AI on SME cybersecurity by focusing on three key dimensions. Detection accuracy measures the system's ability to identify advanced threats like polymorphic malware and zero-day exploits beyond traditional signature-based methods.

False-positive reduction assesses how well AI minimizes alert fatigue and eases analyst workload through refined anomaly detection and contextual analysis. Response efficiency evaluates the speed and precision of incident triage, automated containment, and recovery compared to manual processes. This structured framework ensures that assessments are evidence-based and aligned with established cybersecurity standards, providing a strong view of AI-driven defense maturity in SME environments.

IV. AI-Driven Threat Detection In Practice

Limitations of Traditional Systems

Traditional cybersecurity defenses such as static, rule- and signature-based antivirus, intrusion detection systems (IDS), and intrusion prevention systems (IPS) exhibit significant shortcomings in contemporary threat environments. Signature-based IDS historically dominated cyber defense due to its precision in identifying known threats with minimal false positives and low computational overhead. However, their reliance on predefined indicators renders them ineffective against zero-day exploits, advanced persistent threats (APTs), and polymorphic malware capable of dynamically altering attributes to evade detection (Iyer, 2021). Signature-based systems such as Snort and Suricata compare network traffic to known attack patterns, making them inherently reactive and dependent on constant signature updates, an increasingly inefficient model as adversaries evolve toward stealthier and automated attack strategies (Ugbar & Adebayo, 2025).

Empirical research confirms that traditional signature-driven mechanisms suffer high maintenance overhead, delayed response to novel threats, and vulnerability to encrypted and obfuscated traffic flows. Guo (2023) notes that signature-based systems are unable to detect zero-day threats until signatures are generated, with evidence showing that Google's Project Zero identifies a zero-day vulnerability approximately every seventeen days, while nearly 80% of breaches stem from previously unknown exploits costing organizations an average of $1.2 million per incident. These limitations are magnified in dynamic environments where attackers frequently deploy fileless malware, living-off-the-land techniques, and evasive lateral movement, often overwhelming traditional detection layers with false negatives and false positives that impair analyst response capability.

Recent studies explore enhancements to conventional IDS through data mining and heuristic methods, for instance, signature-based IDS enhanced with data mining and swarm intelligence techniques to improve anomaly detection accuracy. While such models improved precision in separating normal and malicious activity, they introduced high computational overhead and instability in complex, interdependent rule environments, limiting applicability to resource-constrained settings such as IoT networks and small enterprises. Similarly, fuzzy-rough-set-based intrusion detection techniques demonstrated improved outlier recognition but still struggled with scalability and real-time performance under high-volume traffic conditions (Khenwar & Nawal, 2024).

Traditional machine-learning classifiers, although beneficial, also face difficulty scaling to massive, diverse telemetry typical of today’s network environments. Mohamed (2025) highlights that deep learning-based models outperform classical approaches by autonomously extracting complex behavioral patterns from large data streams, yet even these require substantial computational capacity and expertise, capabilities SMEs rarely possess. Consequently, SMEs relying solely on legacy IDS or signature-based platforms face extended attacker dwell time, heightened breach exposure, and increased incident containment costs, emphasizing the need for adaptive, AI-driven detection architectures capable of identifying novel and stealth-based attacks at scale.

Adaptive AI-Based Security Architectures

Adaptive security architectures powered by artificial intelligence and machine learning have risen in direct response to the limitations of legacy systems. These architectures enhance threat detection and prevention by identifying patterns within large volumes of telemetry data, detecting zero-day exploits and ransomware activity, improving IDS and endpoint protection accuracy, and accelerating incident response through automation and predictive analytics (Patil, 2024). A critical first step in integrating AI into SME cybersecurity is a thorough assessment of the organization's existing infrastructure, key assets, and vulnerabilities to determine where AI can deliver the greatest impact. For instance, firms handling large volumes of customer data may prioritize AI for privacy protection, while e-commerce-driven SMEs may focus on fraud detection (Oguta, 2024). AI enables a proactive cybersecurity posture by applying machine learning, deep learning, and natural language processing to structured and unstructured data, offering real-time anomaly detection, pattern recognition, and automated threat response (Jimmy, 2021).

Within these designs, AI models process historical and real-time inputs, including network flows, endpoint events, user behavior logs, and host telemetry to update threat intelligence continuously and identify polymorphic and stealth-based attacks. AI-enhanced Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) systems establish behavioral baselines, detect deviations, and enable automated

responses such as blocking malicious traffic, triggering endpoint scans, or executing containment policies, thereby reducing manual intervention and minimizing operational risk (Mohamed, 2025). Behavioral analytics serve as a core mechanism, where unsupervised and semi-supervised models identify anomalies like lateral movement or unusual process execution paths. When integrated into security pipelines, these models enrich alerts with context, prioritize events by risk, and initiate automated remediation workflows aligned with enterprise policies. Real-time machine learning-driven EDR has transformed endpoint security, introducing adaptability and resilience into modern cyber defense frameworks (Roberts et al., 2024). A recent conference study also notes that contemporary EDR systems now include AI modules capable of identifying emerging attacker behaviors across endpoint and network data streams (Kaur et al., 2024).

Case Example.

Proficio's analysis of AI-enabled EDR deployments reported a 76% improvement in threat detection accuracy and a 63% reduction in dwell time compared to traditional approaches, demonstrating measurable gains in detection and response efficiency (Proficio, 2024). Likewise, Vectra AI's NDR platform applies combined signature and AI-driven behavioral analytics to identify zero-day and supply-chain attacks across the kill chain, extending visibility beyond endpoint activity into network-wide attacker signals (National University of Ukraine, 2024; Vectra AI, 2025).

Federated Learning and Privacy-Preserving Threat Sharing

Federated learning (FL) and privacy-preserving collaborative intelligence systems are becoming as essential approaches for SMEs and distributed organizations seeking to strengthen cybersecurity without exposing sensitive data. As Betul et al. (2024) explain, FL enables multiple nodes to collaboratively train a shared machine learning model while keeping raw data localized, addressing confidentiality and privacy constraints in high-risk sectors. This decentralized learning model enhances data protection while increasing processing efficiency and scalability by relying on local computation and exchanging only model updates rather than security logs or user records.

FL has evolved from its origins in mobile device networks into structured cross-silo environments, where institutions with sensitive data, such as hospitals, universities, and financial organization,s jointly train models while preserving privacy and regulatory compliance. Ratun (2025) differentiates between cross-device FL, which focuses on scaling across many unreliable clients, and cross-silo FL, which emphasizes security, trust, and statistical robustness across fewer, more capable participants. Similarly, Siniosoglou et al. (2024) emphasize FL's ability to democratize machine learning participation by enabling diverse and remote stakeholders to contribute data under privacy guarantees while reducing communication overhead in constrained edge computing environments.

Healthcare deployments illustrate the privacy advantages of FL, as Kadar (2023) demonstrates that institutions can collaboratively build diagnostic and treatment-support models without sharing raw patient data, ensuring compliance with privacy regulations and reducing breach exposure. This privacy-centric paradigm translates effectively to cybersecurity, where Tripwire (2024) describes FL as allowing organizations to retain sensitive security telemetry locally while contributing model updates that improve collective detection performance. Tom et al. (2025) further highlight FL's suitability for intrusion detection, malware classification, and anomaly monitoring in scenarios where data sensitivity and organizational autonomy prohibit centralized log aggregation.

Despite its benefits, FL faces operational and security challenges. Buyuktanir et al. (2025) note that heterogeneous data distributions, communication burdens, governance issues, and the risk of adversarial model contributions can hinder performance and undermine trust. Their findings highlight the need for secure aggregation mechanisms, strong update validation, efficient communication models, and improved resilience against model-poisoning and data-inference attacks.

For SMEs, a practical adoption pathway lies in vendor-managed federated threat-intelligence architectures, where a trusted provider manages coordination, aggregation, and governance. This approach allows SMEs to benefit from shared intelligence and advanced threat models without investing in heavy infrastructure or exposing internal telemetry, aligning FL with operational and resource constraints typical of smaller organizations.

V. Case Studies And Applications

SME Case Study 1 — Financial Sector Example

Real-World Case: Cylance & IBM Watson Deployments in SMEs

Research by Kasali et al. (2025) documents how SMEs leverage AI security tools. A medium-sized manufacturing firm deployed Cylance's AI-driven malware prevention platform to block malicious files pre-execution, preventing a targeted malware campaign and avoiding downtime losses. Meanwhile, a financial

services organization integrated IBM Watson for Cybersecurity to aggregate external threat feeds with internal traffic telemetry, enabling automated intelligence correlation that strengthened phishing detection and prevented customer data compromise (Kasali et al., 2025).

Hypothetical SME Case for Structure Requirement

A regional U.S. financial services institution with 200 employees implemented an AI-enabled Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) stack to counter credential phishing, ransomware, and lateral-movement threats. The system combined supervised and unsupervised ML for behavioral profiling and automated containment. Within six months, incident response time dropped by 45%, false positives fell 60%, and zero-day threat detection improved 30%, reducing compliance penalties and operating costs.

SME Case Study 2 — Healthcare or Nonprofit Sector

Real-World Case: Englewood Health (U.S.) — Seceon aiSIEM Deployment

Englewood Health partnered with GS Lab | GAVS to deploy Seceon's aiSIEM platform, providing AI-driven anomaly detection and automated response, such as EHRs, IoMT devices, and telemedicine, implemented an AI-driven SIEM and SOAR platform tailored for healthcare. Traditional tools failed to detect novel threats or meet HIPAA demands, prompting a phased deployment that included behavioral analytics, anomaly detection, and automated response playbooks. The system analyzed over 1 billion security events, cut false positives by 95%, accelerated incident response by 90%, and reduced compliance preparation time by 85%, significantly strengthening HIPAA-aligned cybersecurity operations while lowering operating costs (Security Boulevard, 2025).

Hypothetical SME Case for Structure Requirement

A nonprofit healthcare network with 150 staff adopted federated-learning-enabled security analytics to protect EHR systems, IoMT devices, and cloud workloads. Behavioral models and automated SOAR workflows enabled encrypted-traffic monitoring and insider-threat detection. Outcomes included an 80% increase in early exfiltration alerts, 50% faster HIPAA breach-response procedures, and audit scores rising from 85% to 98%, all while preserving PHI privacy.

Comparative Results

Across both real and hypothetical SME deployments, AI-driven security frameworks consistently led to a substantial reduction in false positives, enhanced detection of zero-day threats, faster incident response times, and improved compliance efficiency. These implementations also demonstrated meaningful gains in operational productivity and cost-effectiveness, underscoring the value of aligning cybersecurity strategies with organizational and regulatory needs.

VI. Ethical, Technical, And Operational Considerations

Algorithmic Transparency and Bias Mitigation

The deployment of AI systems in cybersecurity brings critical ethical implications, particularly when decision-making becomes opaque. AI systems can suffer from algorithmic bias due to skewed training data, leading to unfair risk assessments, while their lack of transparency and explainability can erode trust among SME stakeholders (Sophie, 2025). In cybersecurity, algorithms may inherit biases from training data or design assumptions, resulting in unfair or disproportionate flagging of certain user groups, devices, or behaviors, leading to false positives, false negatives, and unequal threat prioritization (Mohamed, 2025). A system trained on data from large enterprises may not accurately detect threats in SME environments, potentially leading to unequal protection, and to address this, developers must emphasize transparency and inclusivity in design to ensure equitable and effective outcomes for all users (Attah, Garba, Gil-Ozoudeh, & Iwuanyanwu, 2024).

Transparency in model logic and decision-making is essential, as security teams, especially in SMEs, need to understand why a model triggers a threat alert to uphold fairness, accountability, and regulatory compliance.

Moreover, biased AI systems can either miss genuine threats or wrongly flag harmless behavior, undermining the reliability and trustworthiness of cybersecurity infrastructure. AI/ML systems in cybersecurity can produce false positives by misclassifying benign behavior as threats, especially in unsupervised models, and require ongoing fine-tuning to maintain accuracy (Mohamed, 2025). Their computational demands and potential for both false positives and false negatives highlight the need for careful deployment, as errors can significantly impact security operations. To mitigate bias, organisations are advised to use diverse, representative training data, conduct regular model audits, and adopt explainable AI (XAI) techniques that provide clear rationale for automated actions.

Balancing Automation and Human Oversight

While adaptive AI-driven security architectures (as discussed in Section 4) yield significant efficiency gains, deploying fully autonomous systems without human oversight introduces substantial risk. Nawaz & Abbas (2022) noted that although AI tools can detect threats and automate responses, they remain vulnerable to bias, lack of context, and adversarial manipulation, rendering unchecked automation inappropriate for high-stakes decisions. A hybrid model where AI accelerates detection and triage, and skilled security professionals provide oversight, validation of alerts, and governance, is thus the more reliable approach. In particular for SMEs, designing workflows that combine AI-based incident scoring with expert review ensures that false positives are managed, model drift is monitored, and strategic cybersecurity decisions remain anchored in human judgment.

Compliance and Regulatory Dimensions

The integration of AI into cybersecurity also demands rigorous compliance and regulatory alignment. Frameworks like the National Institute of Standards and Technology (NIST) AI Risk Management Framework offer structured guidance for addressing risks throughout the AI lifecycle, developed through an inclusive and transparent process involving public feedback and expert collaboration, to support broader efforts in ensuring transparency, robustness, fairness, and security in AI systems (NIST, 2024). NIST's efforts emphasise that organizations deploying AI systems must map their internal controls to these principles, whilst also aligning with broader standards such as the ISO/IEC 27001 information security management standard and the Cybersecurity and Infrastructure Security Agency (CISA) operational guidelines. For SMEs, leveraging such frameworks helps structure vendor selection, model governance, audit readiness, and continuous monitoring. NIST and affiliated organizations are developing AI-specific security overlays, such as COSAIS, which tailor existing cybersecurity frameworks like SP 800-53 to address vulnerabilities unique to AI systems, including model theft, training-data poisoning, and adversarial manipulations (John K. Waters, 2025).

VII. Policy And Strategic Implications

National and Economic Security Relevance

Small and mid-sized enterprises (SMEs) are integral nodes in the U.S. digital economy, including national supply chains, critical infrastructure vendors, and service providers. According to Hossain and Hasan (2024), the study found that in the U.S., sectors such as banking and finance, healthcare, small-scale manufacturing, retail and e-commerce, as well as public transport and infrastructure with fewer than 500 employees, are particularly susceptible to cyberattacks. Weak cybersecurity in SMEs can pose systemic risks by enabling adversaries to infiltrate larger enterprise or government networks through upstream or downstream access. Enhancing SME defenses with AI-driven threat detection strengthens digital resilience, safeguards critical sectors like manufacturing and healthcare, and helps preserve national competitiveness while minimizing costs for larger institutions.

Recommendations for SMEs

To implement AI-driven cybersecurity effectively, SMEs should follow a phased roadmap aligned with their resources and growth. This begins with assessing current security posture and identifying key assets and risks. Next, a pilot phase introduces AI detection tools in a limited scope to validate performance. Full deployment then expands coverage across systems, integrating analytics and automated responses with governance protocols. Lastly, continuous optimization involves refining models, monitoring detection accuracy, and evaluating key performance indicators. This structured approach helps SMEs scale securely without overextending their capabilities.

Recommendations for Policymakers

To strengthen SME cybersecurity in the AI in this security innovation era, policymakers should implement a multi-pronged strategy. First, they can incentivize AI-driven security adoption through tax credits, subsidies, and grants especially for pilot programs in under-resourced sectors. Second, ensuring public-private collaboration between agencies like CISA and NIST and industry vendors can help develop strategic AI-security frameworks, shared models, and federated threat intelligence networks. Also, workforce training initiatives are essential to equip SME IT and security staff with AI/ML skills, adaptive security management expertise, and governance knowledge, supported by certification programs and small-business-focused academies.

VIII. Conclusion

This paper has explored the transformative role of artificial intelligence and machine learning in enhancing threat detection and response for small and mid-sized enterprises (SMEs). While traditional, signature-based controls still contribute in identifying known threats, they fall short in providing the adaptive, context-sensitive protection SMEs need. AI-powered solutions by integrating behavioral analytics, anomaly detection, endpoint and network detection and response (EDR/NDR), and privacy-preserving techniques like federated learning offer significant gains in detection precision, faster incident response, and operational efficiency, all tailored to the resource limitations typical of SME environments.

AI-enhanced systems can significantly enhance operational security for SMEs when paired with robust governance and human oversight. Real-world deployments and industry case studies illustrate this impact as AI-driven EDR solutions have shown marked improvements in detection accuracy and reduced dwell time, while healthcare implementations of AI-powered SIEM/SOAR platforms report fewer false positives, faster threat response, and notable cost-efficiency gains. These outcomes highlight AI's ability to amplify limited SME security resources, delivering broader and faster defensive capabilities.

For SMEs, adopting AI-driven cybersecurity requires a phased, pragmatic strategy, beginning with small pilots, validating outcomes, and scaling gradually to ensure minimal disruption and strong governance. Approaches like federated learning and collaborative intelligence can extend threat detection capabilities without compromising data privacy, though they demand careful attention to data variability, secure aggregation, and incentive design. Ethical, technical, and policy safeguards such as transparency, explainability, and human oversight are essential to prevent biased or flawed decisions. While current evidence is largely drawn from vendor case studies, SMEs should pursue an evidence-based roadmap supported by policy incentives and workforce training. Future research should prioritize long-term SME deployments, federated modeling, and the socio-technical dimensions of AI. When thoughtfully integrated, AI can transform constrained SME security resources into fast, scalable defenses that strengthen the broader digital ecosystem.

Reference

[1]. Abosaeeda, Mohammed & Mansour, Mahmud. (2025). A Malware Detection And Classification Using Neural Networks: A Review. 2. 64-90.

[2]. Alhogail A, Alsabih A. Applying Machine Learning And Natural Language Processing To Detect Phishing Email. Comput Secur 2021;110:102414.

[3]. Alladean Chidukwani, Sebastian Zander, Polychronis Koutsakis. (2024). Cybersecurity Preparedness Of Small-To-Medium Businesses: A Western Australia Study With Broader Implications. Computers & Security, Volume 145, 104026, ISSN 0167-4048. Https://Doi.Org/10.1016/J.Cose.2024.104026.

[4]. Arora, Anuj (2025). Transforming Cybersecurity Threat Detection And Prevention Systems Using Artificial Intelligence (May 23, 2025). Available At SSRN: Https://Ssrn.Com/Abstract=5268166 Or Http://Dx.Doi.Org/10.2139/Ssrn.5268166

[5]. Assion K. Tetteh. (2024). Cybersecurity Needs For Smes. Issues In Information Systems Volume 25, Issue 1, Pp. 235-246, 2024 235 DOI: Https://Doi.Org/10.48009/1_Iis_2024_120

[6]. Attah RU, Garba BMP, Gil-Ozoudeh I, Iwuanyanwu O. Strategic Frameworks For Digital Transformation Across Logistics And Energy Sectors: Bridging Technology With Business Strategy.

[7]. Augustine Ugbar And Samuel Oluwafemi Adebayo. (2025). A Comprehensive Review Of Network Intrusion Detection Systems. International Journal Of Research In Engineering And Science (IJRES) ISSN (Online): 2320-9364, ISSN (Print): 2320-9356 Www.Ijres.Org Volume 13 Issue 5 ǁ May 2025 ǁ PP. 190-198

[8]. Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking Alert Fatigue: AI-Assisted SIEM Framework For Effective Incident Response. Applied Sciences, 13(11), 6610. Https://Doi.Org/10.3390/App13116610

[9]. Betul Yurdem, Murat Kuzlu, Mehmet Kemal Gullu, Ferhat Ozgur Catak, Maliha Tabassum. (2024). Federated Learning: Overview, Strategies, Applications, Tools, And Future Directions. Heliyon, Volume 10, Issue 19, E38137, ISSN 2405-8440. Https://Doi.Org/10.1016/J.Heliyon.2024.E38137.

[10]. Bdemerson. (2024). Small Business Cybersecurity Statistics. Https://Www.Bdemerson.Com/Article/Small-Business-Cybersecurity-Statistics

[11]. Boris Loza. (2025). Supervised Machine Learning In Cybersecurity: A Comprehensive Analysis. Medium. Https://Medium.Com/@Leev574/Supervised-Machine-Learning-In-Cybersecurity-A-Comprehensive-Analysis-04ac97a822fc

[12]. Boswell R. (2023). 60% Of European Smes That Are Cyber-Attacked Have To Close After Six Months. Startup Magazine (2023). Https://Startupsmagazine.Co.Uk/Article-60-European-Smes-Are-Cyber-Attacked-Have-Close-After-Six-Months

[13]. Buyuktanir, B., Altinkaya, Ş., Karatas Baydogmus, G. Et Al. (2025). Federated Learning In Intrusion Detection: Advancements, Applications, And Future Directions. Cluster Comput 28, 473 (2025). Https://Doi.Org/10.1007/S10586-025-05325-W

[14]. Daniel Dunsin. (2024). "The Impact Of AI-Driven Threat Detection On Securing Consumer Iot Devices In Home Automation Systems," Researchgate, 2024. [Online]. Available: Https://Www.Researchgate.Net/Publication/390176767_The_Impact_Of_Aidriven_Threat_Detection_On_Securing_Consumer_Iot_Devices_In_Home_Automation_Systes

[15]. Carlos Rombaldo Junior, Ingolf Becker, And Shane Johnson. (2023). Unaware, Unfunded And Uneducated: A Systematic Review Of SME Cybersecurity. 1, 32 Pages. Https://Arxiv.Org/Pdf/2309.17186

[16]. Dubey, A. K., R. Kumar Dubey, A. Shukla, And P. Dubey (2024). "Optimizing Cybersecurity: Leveraging Support Vector Machines For Real-Time Threat Detection," 2024 First International Conference On Innovations In Communications, Electrical And Computer Engineering (ICICEC), Davangere, India, 2024, Pp. 1-6, Doi: 10.1109/ICICEC62498.2024.10808642.

[17]. Ejaz, Umair & Matthew, Bamidele. (2024). Cost-Effective Cybersecurity Solutions For Smes: Balancing Security Needs And Budget Constraints.

[18]. Ejaz, Umair & Gimah, Mathew & Iseal, Sheed. (2024). Cybersecurity Talent Shortage In Smes: Innovative Approaches To Recruitment And Retention.

[19]. Genuario, F., Santoro, G., Giliberti, M., Bello, S., Zazzera, E., & Impedovo, D. (2024). Machine Learning-Based Methodologies For Cyber-Attacks And Network Traffic Monitoring: A Review And Insights. Information, 15(11), 741. Https://Doi.Org/10.3390/Info15110741

[20]. Guo Y. (2022). A Survey Of Machine Learning-Based Zero-Day Attack Detection: Challenges And Future Directions. Comput Commun. 2023 Jan;198:10.1016/J.Comcom.2022.11.001. Doi: 10.1016/J.Comcom.2022.11.001. PMID: 36741076; PMCID: PMC9890381.

[21]. Harpreet Kaur, Dharani Sanjaiy SL, Tirtharaj Paul, Rohit Kumar Thakur, K Vijay Kumar Reddy, Jay Mahato, Kaviti Naveen. (2024). Evolution Of Endpoint Detection And Response (EDR) In Cybersecurity: A Comprehensive Review, E3S Web Of Conferences 556, 01006 (2024) RAWMU-2024 Https://Www.E3s-Conferences.Org/Articles/E3sconf/Pdf/2024/86/E3sconf_Rawmu2024_01006.Pdf

[22]. Hossain, Nazmul & Hasan, Mahmud. (2024). The Impacts Of Cyberattacks On Smes In The USA And Ways To Accelerate Cybersecurity. Advances In Social Sciences Research Journal. 11. 197-203. 10.14738/Assrj 1110.17724.

[23]. Hussain, Nurudeen. (2024). Deep Learning Architectures Enabling Sophisticated Feature Extraction And Representation For Complex Data Analysis. International Journal Of Innovative Science And Research Technology. 9. 11. 10.38124/Ijisrt/IJISRT24OCT1521.

[24]. Iyer, Kumrashan Indranil. (2021). From Signatures To Behavior: Evolving Strategies For Next-Generation Intrusion Detection. 8. 165-171. 10.5281/Zenodo.15223001.

[25]. Jimmy, FNU. (2024). The Role Of Artificial Intelligence In Predicting Cyber Threats. International Journal Of Scientific Research And Management (IJSRM). 11. 935-953. 10.18535/Ijsrm/V11i08.Ec04.

[26]. John K. Waters. (2025, August 19). NIST Proposes New Cybersecurity Guidelines For AI Systems. Campus Technology. Https://Campustechnology.Com/Articles/2025/08/19/Nist-Proposes-New-Cybersecurity-Guidelines-For-Ai-Systems.Aspx

[27]. Kadar, Abas. (2023). Federated Learning: A New Era Of Secure, Privacy-Conscious Ai Collaboration. Https://Www.Researchgate.Net/Publication/388026650_FEDERATED_LEARNING_A_NEW_ERA_OF_SECURE_PRIVACY-CONSCIOUS_AI_COLLABORATION

[28]. Kamboj, Arvind & Ravindran, Vasudev & Ojha, Sharad. (2025). A Comparative Analysis Of Signature-Based And Anomaly-Based Intrusion Detection Systems. International Journal Of Latest Technology In Engineering Management & Applied Science. 14. 209-214. 10.51583/IJLTEMAS.2025.140500026.

[29]. Kapera, Artur & Niemiec, Marcin. (2025). Dynamic Risk Thresholds For SIEM Alerting Based On Machine Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2025.3588441.

[30]. Kasali, Kemisola & Orekha, Precious & Bamigboye, Oluwaseun & Ajao, Afolabi & Alawiye, Peter & Raji, Adeola. (2025). AI-Driven Strategies Of Mitigating Cybersecurity Threats In U.S. Small And Medium Enterprises (SMES). International Journal Of Computer Science And Information Technology. 17. 49 - 62. 10.5121/Ijcsit.2025.17404.

[31]. Kayode, Oyebode & Gl, Mapfaza. (2025). A Comparative Study Of Supervised, Unsupervised, And Reinforcement Learning In Cyber Defense.

[32]. Keepnet Labs. (2025). Why Smes Are Prime Targets For Ransomware & How To Protect Against Attacks. Https://Keepnetlabs.Com/Blog/Ransomware-And-Smes

[33]. Khenwar, Medha & Nawal, Meenakshi. (2024). Challenges And Limitations Of IDS: A Comprehensive Assessment And Future Perspectives. SKIT Research Journal. Vol 14. 35-39. 10.47904/IJSKIT.14.1.2024.35-39.

[34]. Li, Guangjun & Sharma, Preetpal & Pan, Lei & Rajasegarar, Sutharshan & Karmakar, Chandan & Patterson, Nicholas. (2021). Deep Learning Algorithms For Cyber Security Applications: A Survey. Journal Of Computer Security. 29. 1-25. 10.3233/JCS-200095.

[35]. Marco Arazzi, Dincy R. Arikkat, Serena Nicolazzo, Antonino Nocera, Rafidha Rehiman K.A., Vinod P., Mauro Conti. (2025). NLP-Based Techniques For Cyber Threat Intelligence. Computer Science Review, Volume 58, 100765, ISSN 1574-0137. Https://Doi.Org/10.1016/J.Cosrev.2025.100765.

[36]. Marta F. Arroyabe, Carlos F.A. Arranz, Ignacio Fernández De Arroyabe, Juan Carlos Fernández De Arroyabe. (2024). Revealing The Realities Of Cybercrime In Small And Medium Enterprises: Understanding Fear And Taxonomic Perspectives. Computers & Security, Volume 141, 103826, ISSN 0167-4048. Https://Doi.Org/10.1016/J.Cose.2024.103826.

[37]. Mohamed, N. (2025). Artificial Intelligence And Machine Learning In Cybersecurity: A Deep Dive Into State-Of-The-Art Techniques And Future Paradigms. Knowl Inf Syst 67, 6969–7055 (2025). Https://Doi.Org/10.1007/S10115-025-02429-Y

[38]. Montgomery, Richard. (2024). A Comparative Analysis Of Decision Trees, Neural Networks, And Bayesian Networks: Methodological Insights And Practical Applications In Machine Learning. 10.20944/Preprints202410.1491.V1.

[39]. National Institute Of Standards And Technology. (2024). AI Risk Management Framework. U.S. Department Of Commerce. Https://Www.Nist.Gov/Itl/Ai-Risk-Management-Framework

[40]. National University Of Ukraine. (2024). Vectra AI: MATCH-Powered NDR For Advanced Threat Detection. Https://En.Nwu.Ua/Blog/Vectraai-En/Vectra-Ai-Match-Powered-Ndr-For-Advanced-Threat-Detection/

[41]. NAVEX. (2023). The State Of Cybersecurity For Small And Medium Businesses. Https://Www.Navex.Com/En-Us/Blog/Article/The-State-Of-Cybersecurity-For-Small-And-Medium-Businesses/

[42]. Nawaz, Yasir & Abbas, Asad. (2022). Cybersecurity In The Age Of AI: Balancing Automation And Human Oversight In Data Security. 10.13140/RG.2.2.20675.11040.

[43]. Ogundairo, Obaloluwa & Broklyn, Peter. (2024). Natural Language Processing For Cybersecurity Incident Analysis. Journal Of Cyber Security.

[44]. Oguta GC. Securing The Virtual Marketplace: Navigating The Landscape Of Security And Privacy Challenges In E-Commerce. GSC Adv Res Rev 2024;18(1):084-117.

[45]. Okafor, Maureen. (2025). Deep Learning In Cybersecurity: Enhancing Threat Detection And Response. World Journal Of Advanced Research And Reviews. 24. 10.30574/Wjarr.. 2024.24.3.3819.

[46]. Patil, Dimple. (2024). Artificial Intelligence In Cybersecurity: Enhancing Threat Detection And Prevention Mechanisms Through Machine Learning And Data Analytics.

[47]. Prasasthy Balasubramanian, Sadaf Nazari, Danial Khosh Kholgh, Alireza Mahmoodi, Justin Seby, Panos Kostakos. (2025). A Cognitive Platform For Collecting Cyber Threat Intelligence And Real-Time Detection Using Cloud Computing. Decision Analytics Journal, Volume 14, 100545, ISSN 2772-6622. Https://Doi.Org/10.1016/J.Dajour.2025.100545.

[48]. Proficio. (2024, May 13). The Impact Of AI On Endpoint Detection And Response. Proficio. Https://Www.Proficio.Com/Ai-Endpoint-Detection-And-Response-Edr/

[49]. Ratun Rahman. (2025). Federated Learning: A Survey On Privacy-Preserving Collaborative Intelligence. Arxiv:2504.17703v3 [Cs.LG] 12 Aug 2025

[50]. Roberts, Michael & Turner, Jessica & Williams, Ethan & Miller, Sophia & Shekhar, Suman. (2024). Real-Time Endpoint Detection And Response (EDR) With Machine Learning Integration.
[51]. Saha, B. And Anwar, Z. (2024). A Review Of Cybersecurity Challenges In Small Business: The Imperative For A Future Governance Framework. Journal Of Information Security, 15, 24-39. Doi: 10.4236/Jis.2024.151003.
[52]. Sajad Einy, Cemil Oz, Yahya Dorostkar Navaei. (2021). The Anomaly- And Signature-Based IDS For Network Security Using Hybrid Inference Systems. Mathematical Problems In Engineering. Https://Doi.Org/10.1155/2021/6639714
[53]. Salluh, Jorge. (2024). Protecting Big Data: Cybersecurity Challenges And Solutions In Business Intelligence Systems For Smes. 10.13140/RG.2.2.13429.79849.
[54]. Sánchez, E., Calderón, R., & Herrera, F. (2025). Artificial Intelligence Adoption In Smes: Survey Based On TOE–DOI Framework, Primary Methodology And Challenges. Applied Sciences, 15(12), 6465. Https://Doi.Org/10.3390/App15126465
[55]. Security Boulevard. (2025). Transforming Healthcare Cybersecurity With AI-Driven SIEM. Https://Securityboulevard.Com/2025/09/Transforming-Healthcare-Cybersecurity-With-Ai-Driven-Siem
[56]. Shevchuk, Ruslan & Martsenyuk, Vasyl. (2024). Neural Networks Toward Cybersecurity: Domain Map Analysis Of State-Of-The-Art Challenges. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3411632.
[57]. Siniosoglou I, Bibi S, Kollias KF, Et Al. (2024). Federated Learning Models In Decentralized Critical Infrastructure. In: Sofia RC, Soldatos J, Editors. Shaping The Future Of Iot With Edge Intelligence: How Edge Computing Enables The Next Generation Of Iot Applications. Abingdon (UK): River Publishers; 2024 Jan. Chapter 5. Available From: Https://Www.Ncbi.Nlm.Nih.Gov/Books/NBK602372/ Doi: 10.1201/9781032632407-7
[58]. Smallman, Joshua. (2024). A Survey On Malware Detection And Analysis. Journal Of Science & Technology. 5. 1-14. 10.55662/JST.2024.5401.
[59]. Sophie, Emily. (2025). "Risk Assessment And Mitigation In SME Budgeting Through AI". 7. Https://Www.Researchgate.Net/Publication/391851861_Risk_Assessment_And_Mitigation_In_SME_Budgeting_Through_AI
[60]. Srinivas Reddy Pulyala. (2023). The Future Of SIEM In A Machine Learning-Driven Cybersecurity Landscape. Turkish Journal Of Computer And Mathematics Education. Vol.14 No.03 (2023), 1309 - 1314. Https://Pdfs.Semanticscholar.Org/5223/C10127d3862ceb2f87fbbc568265d4cd3153.Pdf
[61]. Suman Karki, A B M Mehedi Hasan, Cesar Sanin. (2024). Use Of ML And AI In Cybersecurity- A Survey. Procedia Computer Science, Volume 246, Pages 1260-1270, ISSN 1877-0509. Https://Doi.Org/10.1016/J.Procs.2024.09.552.
[62]. Timilehin, Oladoja. (2022). AI In Security Information And Event Management: Transforming User Experience And Decision-Making.
[63]. Tom, A. K., Khraisat, A., Jan, T., Whaiduzzaman, M., Nguyen, T. D., & Alazab, A. (2025). Survey Of Federated Learning For Cyber Threat Intelligence In Industrial Iot: Techniques, Applications And Deployment Models. Future Internet, 17(9), 409. Https://Doi.Org/10.3390/Fi17090409
[64]. Tommaso Zoppi, Andrea Ceccarelli, And Andrea Bondavalli, "Unsupervised Algorithms To Detect Zero-Day Attacks: Strategy And Application," Researchgate, 2021. [Online]. Available: Https://Www.Researchgate.Net/Publication/352621863_Unsupervised_Algorithms_To_Detect_Zero -Day_Attacks_Strategy_And_Application
[65]. Tripwire. (2024). Federated Learning In Cybersecurity: Collaborative Intelligence For Threat Detection. Https://Www.Tripwire.Com/State-Of-Security/Federated-Learning-Cybersecurity-Collaborative-Intelligence-Threat-Detection
[66]. Vectra AI. (2025). The Case For NDR: Why Network Detection And Response Is Essential For Modern Cybersecurity. Https://Cdn.Prod.Website-Files.Com/64e50cbe2b6f932c04238c14/68d168e14784ab37d79014c4_WP_Thecaseforndr_092025_FNL .Pdf
[67]. Yerabolu M.R. (2025) The Evolution Of AI-Driven Threat Hunting: A Technical Deep Dive Into Modern Cybersecurity, European Journal Of Computer Science And Information Technology,13(7), 36-49