JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 10 Issue 01
2025

Review Article
https://doi.org/10.56979/1001/2025/1212

AI-Enabled Cybersecurity for Small and Medium-Sized Enterprises (SMEs): A Systematic Review and Evidence-Informed Assessment Framework

Muhammad Sami Ullah[1], Muhammad Ahsan[2*], Kainat[3], and Nadeem Yaqub[4]

[1]Department of Computer Science, Gujrat Institute of Management Sciences (GIMS), Arid University, Pakistan.
[2]School of Systems and Technology, Department of Software Engineering, University of Management and Technology (UMT), Pakistan.
[3]Gujrat Institute of Management Sciences (GIMS), Arid University, Pakistan.
[4]College of computer science and Technology, Beijing University of Technology, China.
[*]Corresponding Author: Muhammad Ahsan. Email: muhammadahsan@umt.edu.pk

Received: September 09, 2025 **Accepted:** November 30, 2025

Abstract: Small medium enterprises (SMEs) are the biggest population of businesses in the world and are very susceptible to cyber-attacks because of their insufficient financial resources, technical ability and expertise. Artificial intelligence (AI) represents the promise of improving SME cyber resilience by detecting attacks and responding faster. Its practical feasibility is however not clearly known. The systematic review of fifty peer-reviewed articles and independently verified commercially available AI-based cybersecurity solutions (2018-2025) presents in this paper is aimed at assessing the viability and not the performance of AI-powered cybersecurity in SMEs. It has been demonstrated that, despite high detection performance of ensemble, supervised and deep learning approaches in controlled experimental settings, SME deployment is limited by the quality of data, computational requirements and operation maturity. According to commercial knowledge, cloud-based EDR/XDR, MDR and email security enhanced using AI seem to be the most feasible adoption routes. Based on these findings, SME AI Cybersecurity Feasibility Framework (SME-AICF) is proposed as an evidence-based conceptual framework based on the structure of the feasibility assessment of the technical, economic, operational, legal and regulatory, and market dimensions; the framework is conceptual and needs empirical confirmation. Implications on SMEs, policymakers, and vendors as well as priority research gaps are the last elements of the paper.

Keywords: Artificial Intelligence; Cybersecurity; SMEs; AI-enabled Cyber Defense; Intrusion Detection; EDR/XDR; Managed Detection and Response; Feasibility Assessment; Systematic Review; PRISMA; Cyber Resilience

1. Introduction

Small medium enterprises (SMEs) are the cornerstones of national economies and international supply chains[1] and they are still likely to be disproportionately affected by cyber threats because of limited financial resources, lack of skills, and old-fashioned technological infrastructure [2, 3]. Recent empirical research studies in the area of cybersecurity in SMEs demonstrates that the adoption outcomes are largely predetermined by financial constraints, access to skills, perceived value, and organizational preparedness to accompany alongside technical ability per se [4-10].The more advanced cyberattacks are becoming, such as ransomware, credential theft, and supply-chain compromise, as well as artificial intelligence (AI)-generated phishing, the less efficient security practices using signatures are becoming [11]. SMEs also have limitations in their

defensive ability due to their structural nature discussed in Section 2.2[12]. It has become clear that artificial intelligence (AI) has the potential to become a formidable driver of cyber defense, providing automated threat detection, machine learning, behavioral analytics, and faster response to incidents [13, 14]. These features are specifically important to SMEs that do not have the capacity to constantly watch systems or have specific security forces at work [11, 15]. To that end, the primary research question is not whether AI can enhance the accuracy of detection and therefore, it depends on whether SMEs can practically acquire, implement and maintain AI-empowered cybersecurity to fit into their operational environment [13].

In spite of the fact that cybersecurity technologies based on AI have reached a high level of development, their usage among SMEs is still low [2]. This adoption pattern is also in line with broader small medium enterprise (SME) cybersecurity research, which regularly highlights the issues of feasibility, cost and sustainability issues rather than technical performance. [4-9].

A large number of academic researchers have proven that AI security models are highly performing, but these models are normally tested on benchmark or controlled data, which are not a complete reflection of real SME settings [16].The reviews identified in the literature review focus mostly on the performance of algorithm or talk about SME cybersecurity issues separately. They rarely combine these views and assess the feasibility of the real-world, and they do not compare the solutions to AI in academia with commercially offered products of AI-driven cybersecurity in a systematic way in terms of cost and deployment conditions, and in terms of operational sustainability. This poses a decisive void: there is a lack of consolidated information that studies AI performance, SME-specific feasibility obstacles, and business AI security solutions knowledge. This review seals that gap by summarizing scholarly literature as well as market-based AI cybersecurity solutions to determine the feasibility of AI-enabled cybersecurity in the SME context.

The paper summarizes research findings based on fifty peer-reviewed scholarly articles and independently verified commercially offered AI cybersecurity systems that were published within the period of 2018-2025 to assess the potential viability of AI-based cybersecurity in SMEs. It will answer three main research questions: (i) what performance features do AI cybersecurity approaches show, and how far can the research be adopted by SMEs? (ii) What are the technical, economic, operational, legal and market specifics that determine SME potential to implement AI-driven cybersecurity? And (iii) to what degree do commercially offered AI cybersecurity solutions fit the needs and limitations of SME and what deployment routes seem to be most workable?

There are four contributions made by this study. First, it generalizes academic and business evidence, providing a gap between research understanding and the realities of SME deployment in the world. Second, it contributes to the knowledge of the performance of major AI paradigms (e.g., supervised learning, deep learning, federated learning, anomaly detection) within the SME context, which include limited data, computing capabilities, skills, and integration preparedness. Third, it compares the performance claims of academics with the commercial deployment evidence pointing to the mismatch between benchmark accuracy and economic, operational, and governance viability. Lastly, it suggests the evidence-based conceptual framework SME AI Cybersecurity Feasibility Framework (SME-AICF) that systems the feasibility assessment through technical, economic, operational, legal, and market aspects and is a conceptual framework that reflects a workable feasibility view and not an empirical decision support framework.

The rest of the paper will be organized in the following way. Section 2 gives background information on SME cybersecurity weakness, cyber threat landscape and AI-based cybersecurity. Section 3 provides the methodology used in systematic review. Section 4 gives synthesized findings of academic and business evidence. Section 5 provides the conceptual feasibility framework of SME-AICF. Section 6 is on implications, research gaps, and limitations and Section 7 brings the end of the study.

2. Background and Conceptual Foundations

This section gives necessary background to justify the feasibility analysis that was done later in the review. It underlines the organizational weakness of SMEs, the threat environment they have to contend with, and the

development of AI and machine learning methods applicable to the cybersecurity concern. The following foundations form the conceptual basis of the results of the interpretation of the empirical findings in Sections 4-6.

Typically, small and medium-sized enterprises (SMEs) are identified in terms of employee numbers and financial levels though in some places, there are other criteria. Nevertheless, SMEs tend to have such common features as lean organization, lack of IT specialization, and limited financial resources due to these differences [1] [17] [18]. They are exposed to the cascading risk of vulnerability in global supply chains where the compromise of a small supplier can spread to other organizations that rely on it [19]. These structural facts indicate a necessity to consider to enhance the SME resilience with the help of AI-enabled cybersecurity, which is the goal of this review.

2.1. SME Cybersecurity Challenges

SMEs have various vulnerabilities that are inherent in nature and affect their cybersecurity stance and readiness to implement AI-based solutions. These include financial, human, technical, organizational, as well as, data related vulnerabilities [20, 21]. These limitations are critical to the evaluation of academic AI models and commercial cybersecurity products, as discussed in subsequent sections. Table 1 presents the key vulnerability drivers that impact SMEs with resource limitations, shortage of talent, antique infrastructure, and divided governance as the pillars of feasibility impediments.

Table 1. Key Cybersecurity Vulnerability Factors in SMEs

Vulnerability Factor	Description	Supporting Evidence
Financial Constraints	Limited cybersecurity budget restricts tools & skilled staff	[1-3, 6, 22] [9, 20]
Human & Skills Limitations	Lack of specialist cybersecurity expertise	[6-8, 12, 20, 21]
Technical Limitations	Legacy systems, weak logging, fragmented infrastructure	[1, 6, 18, 20, 23]
Organizational Weaknesses	Weak governance, absence of mature policies	[6-8, 20, 21]
Data Limitations	Limited telemetry and labelled data availability	[6-8, 14, 24]

Together, these weaknesses highlight the reason why SMEs are at a disproportionately high risk of cybersecurity and why AI-enhanced solutions should be considered in relation to their capabilities when considering compatibility with SME operational considerations. These limitations are consistent with several systematic SME cybersecurity surveys that indicate the economic burden, capacity limitations, failure in governance, and operational immaturity as the pre-eminent barriers to adoption. [4-9].

The environment in which SMEs operate has become very hostile in terms of cyber. Ransomware, malware, phishing, business email compromise (BEC), and supply-chain attacks are common attacks on them [11, 25-28]. The fact that their monitoring abilities are limited and systems they use are outdated makes these risks even more severe[11, 29]. Table 2 lists the main cyber threats to the SMEs, indicating how the ransomware, phishing, network intrusions, insider threats and APTs expose them to a steady operational and financial risk. All of these circumstances contain substantial background information on why AI-controlled behavioral analytics and automated response systems identified in Section 4 would be relevant.

Table 2. Major Cyber Threat Categories Affecting SMEs [11, 19] [26, 27, 29].

Threat Type	Description	Impact on SMEs
Malware & Ransomware	Disruption, corruption, or encryption of data	Downtime, financial loss, reputational damage
Social Engineering (Phishing, BEC)	Deceptive messaging exploiting human trust	Credential theft, fraud, unauthorized access

Network-Based Attacks	DDoS, MITM, DNS manipulation, packet interception	Service outages, data exposure
Insider Threats	Negligent, compromised, or malicious internal actors	Data leakage, compliance violations
Advanced Persistent Threats (APTs)	Long-term, stealthy intrusions	Extended compromise, supply-chain exploitation

While the threats posed by these methods continue, the growing use of AI-based anomaly detection, behavioral modeling, and automated incident response in commercial cybersecurity products is justified.

2.2. Evolution of AI in Cybersecurity

In the last ten years, AI technologies have been developed considerably. Initial cybersecurity models were based on rule-based and signature-based systems that were not very adaptable. Pattern recognition was made better through machine learning to recognize malicious artifacts and behaviors through statistical representations [30-33]. Subsequently deep learning techniques were used to automatically extract features of raw traffic flows, binaries and user activity logs [34, 35]. Newer advancements include transformer-based natural language processing (NLP), federated learning, explainable AI (XAI) and adversarial robustness, which may serve as advanced analytical tools [36-41]. Nevertheless, most of these systems demand good telemetry or specialized skills or high computing power, which is not normally the case with SMEs [12, 42]. Such a discrepancy between high AI methods and the limitations of SMEs is discussed in detail in Section 4 and 6.

AI-based cybersecurity is based on various machine learning paradigms with different benefits and disadvantages in the SME setting Table 4 aligns important AI paradigms with cybersecurity applications and demonstrates that all of them offer the ability advantages but have a practical feasibility limit to SMEs. Learning models that are supervised offer high precision but they need labeled such datasets are balanced, clean and stable, and thus do not reflect the noisys that SMEs do not have very often. Unsupervised learning methods detect anomalies without labels yet they are likely to generate high false-positive in noisy SME networks[24, 43] [32]. Deep learning models are state-of-the-art but they are expensive to run and maintain [44, 45]. Potential alternatives are offered through federated and transfer learning techniques that decrease the number of required data and facilitate collaboration that preserves privacy [37, 38, 46].

Table 3. Common cybersecurity AI datasets, their strengths, and limitations for SME-relevant cybersecurity research [30, 31, 43, 47-51].

Dataset	Domain	Strengths	Limitations
CICIDS2017	Network intrusion	Rich labeled traffic; diverse attacks	Unrealistic traffic mix; not SME representative
UNSW-NB15	Intrusion detection	Modern protocols, realistic features	Synthetic environment; class imbalance
NSL-KDD	Intrusion detection	Widely used benchmark	Outdated; missing modern threat types
EMBER	Malware classification	Large PE malware dataset	Not representative of SME endpoint diversity
PhishTank/Enron	NLP/phishing	Strong datasets for phishing/NLP tasks	Corporate bias; limited global diversity

Benchmark datasets have had a major impact on scholarly AI cybersecurity studies. More popular intrusion detection datasets like CICIDS2017, UNSW-NB15, NSL-KDD and their predecessors KDD99 have enhanced the standardization of the evaluation at the cost of concerns about realism [43, 48, 50, 52] . Malware and phishing datasets EMBER and PhishTank are also necessary but not necessarily representative of SME settings [45, 49, 53]. Such constraints often exaggerate performance assertions versus deployment reality [47]. The

above Table 3 is a comparison of popular cybersecurity datasets, which shows that benchmark datasets are accurate in terms of technology, but lacks SME contextual realism.

Table 4. AI/Machine learning (ML) Paradigms in Cybersecurity and Their SME Implications [14, 31, 35-38, 40, 54-57]

ML Paradigm	Cybersecurity Use	SME Advantages	SME Limitations
Supervised Learning	IDS, malware classification	High accuracy with labeled data	SMEs lack labeled datasets; retraining required
Unsupervised Learning	Anomaly/zero-day detection	No labels required	High false positives in noisy environments
Deep Learning	Traffic & behavioral analysis	Strong benchmark performance	Requires compute; sensitive to telemetry quality
Reinforcement Learning	Automated defense strategies	Long-term adaptability	Rare real-world SME validation
Federated Learning	Distributed detection	Preserves data privacy	Requires governance and stable connectivity
Transfer Learning	Malware & phishing detection	Reduces training data needs	Risk of domain mismatch

These paradigms establish the groundwork of appreciating the comparative performance and discusses of feasibility in the performance of Section 5.

The AI technologies are being adopted in major cybersecurity fields, which allows conducting automated threat detection, behavioral analytics, log correlation, and incident response. These functions assist in compensating the failure of cybersecurity skills continually faced by the SMEs and limit the reliance on manual surveillance [15, 31, 32, 41]. The applicability of these applications is discussed further under the commercial solution analysis in Section 4.3 and Table 5 summarizes the most common spheres of cybersecurity application of AI that is the most common across the literature reviewed.

Table 5. AI Application Areas Relevant to SME Cybersecurity

Application Area	AI Techniques	Example Tasks	Evidence
Intrusion Detection	ML, Deep learning (DL), hybrid models	Detect malicious traffic & anomalies	[27, 29, 43, 47, 58]
Malware Detection	CNNs, hybrid DL	Malware classification	[45, 49, 53, 59]
Phishing Detection	NLP, BERT, DL	Email & URL phishing detection	[28, 51, 60, 61]
Behavioral Analytics	Autoencoders, Unsupervised ML	Detect abnormal system behavior	[14, 41]
EDR/XDR & Automation	Cloud AI, ensembles	Endpoint detection & response	[62, 63]
Threat Intelligence Fusion	Graph ML, DL	Correlation of threat indicators	[41, 54]

2.3. Operational and Regulatory Considerations

Accuracy, precision, recall, false-positive rate, F1 score and detection latency are used to test AI models of cybersecurity. Most of the models in the 50 studies included in this review report high accuracy, often over 95 percent, although it is often based on manually-curated benchmark datasets and not actual SME telemetry [43, 47]. The interpretations of performance metrics, however, must be approached with a certain level of caution; Section 5 presents performance metrics in contexts of realistic SME constraints, in terms of model families.

SMEs have to adhere to the regulatory frameworks of GDPR, CCPA, HIPAA, PCI-DSS, and ISO/IEC 27001 that set stringent criteria of data protection, data breach reporting, data auditability, and data governance[17, 23, 64].The compliance can be assisted by the AI-based solutions that provide automated monitoring and structured logging as well as detecting the anomalies. Nonetheless, they also create novel threats of data sovereignty, explain ability, and algorithmic prejudice [40, 41]. These considerations constitute the legal and governance aspects of the SME-AICF approach that is covered in Section 5.This legal-regulatory aspect is well in line with the developing European AI governance frameworks, specifically, the EU AI Act and cybersecurity governance frameworks models focusing on accountability, transparency, and risk-based deployment. [65-67].

3. Methodology

To enhance transparency, reproducibility, and methodological robustness, this systematic review follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines [68]. The review integrates evidence from peer-reviewed academic literature with insights from commercially available AI-driven cybersecurity solutions to assess the feasibility of AI-enabled cybersecurity adoption in small and medium-sized enterprises

3.1. Research Design and Search Strategy

The proposed paper will take the form of a systematic review of the literature supplemented by the organized comparative evaluation of commercial AI-based cybersecurity products. The scholarly part summarizes empirical studies about AI/ML-based cybersecurity, whereas the business part assesses the needs of the deployment, the feasibility of the operation, and the limitations of SMEs through the reliable industry research (e.g., Gartner, Forrester) [62, 63].

The IEEE Xplore, ACM Digital Library, Science Direct, and Scopus and Springer Link primary databases were searched. Backward and forward citation chaining was also used to supplement searches and limit expert consultation to find relevant studies that might not be identified because of indexing limitations in databases. Exploratory scanning was carried out only on Google Scholar, PubMed, and arXiv, which were not incorporated in PRISMA accounting to ensure no duplication and non-peer-review bias. This multi-source method increases methodological rigor and breadth of coverage.

To create all-inclusive search strings, search expressions were formulated in three conceptual areas, namely, SMEs, cybersecurity, and artificial intelligence, with Boolean operators.

SME-related terms included: Small and medium enterprises, small and medium-sized enterprises, SME, SMEs, small business, medium-sized business

There were cybersecurity-related terms such as: cybersecurity, cyber threat, cyber-attack, intrusion, malware, ransomware, phishing, threat detection, anomaly detection, information security, security operations

AI/ML-related terms included: artificial intelligence, AI, machine learning, ML, neural networks, explainable AI, XAI, ensemble learning, supervised learning, unsupervised learning

The search string that was used was: (“small and medium enterprises” OR SME OR small business) And (cybersecurity OR threat detection OR ransomware OR phishing)

To avoid outdated evidence, only research published from 2018 onward was included, ensuring coverage of contemporary datasets, current AI–security practices, and the evolving SME regulatory environment. Earlier studies were excluded due to outdated threat landscapes, limited data realism, and immature AI integration. Studies were included if they met all of the following core eligibility conditions: (i) employed AI/ML techniques in a cybersecurity context, (ii) provided empirical experimentation or technically rigorous evaluation, and (iii) were peer-reviewed journal articles or conference papers. Given that SME applicability is central to this review, SME relevance or transferability was explicitly operationalized using predefined decision rules rather than subjective interpretation. A study was considered SME-relevant if it satisfied at least one of the following conditions: (a) it used SME datasets, SME environments, or SME organizations; (b) it evaluated systems under

SME-like constraints such as limited labelled data, restricted IT staffing, reliance on managed/cloud-based security, or cost sensitivity; (c) it explicitly discussed deployment feasibility for SMEs; or (d) it demonstrated applicability to typical SME security operations such as EDR/XDR, phishing defense, MDR services, lightweight IDS, or cloud security. Studies that were purely theoretical, lacked implementation context, or required enterprise-scale infrastructure were excluded from the final dataset.

Research papers were screened out when they were not SME applicable, were only conceptual but lacked empirical support, had low methodological rigor, were not in English and were beyond the publication date. It might have residual bias because of publication bias, limitation of indexing of databases, language restriction, and survivorship bias. Multi-database searching, citation chaining, industry source triangulation and dual-reviewer screening alleviated these risks, but there is still some inevitably biased presence.

A total of 497 records were initially identified (422 through database searching and 75 through citation chaining and expert recommendations). After the removal of 175 duplicate records, 322 unique records remained. Title and abstract screening excluded 28 records, resulting in 294 full-text articles assessed for eligibility. Following full-text review, 200 articles were excluded due to lack of SME relevance (n = 98), insufficient methodological rigor (n = 45), publication prior to 2018 (n = 32), or absence of empirical evidence (n = 25). The remaining 94 articles were classified as "eligible" and proceeded to methodological quality appraisal. Application of the adapted CASP criteria excluded 44 low-quality studies (score < 10), resulting in 50 high-quality studies included in the final synthesis. The PRISMA flow diagram in Figure 1 is numerically and terminologically consistent with this process and explicitly distinguishes "eligible," "quality-appraised," and "included" sets to ensure methodological clarity and reproducibility.

3.2. Study Selection and Quality Assessment

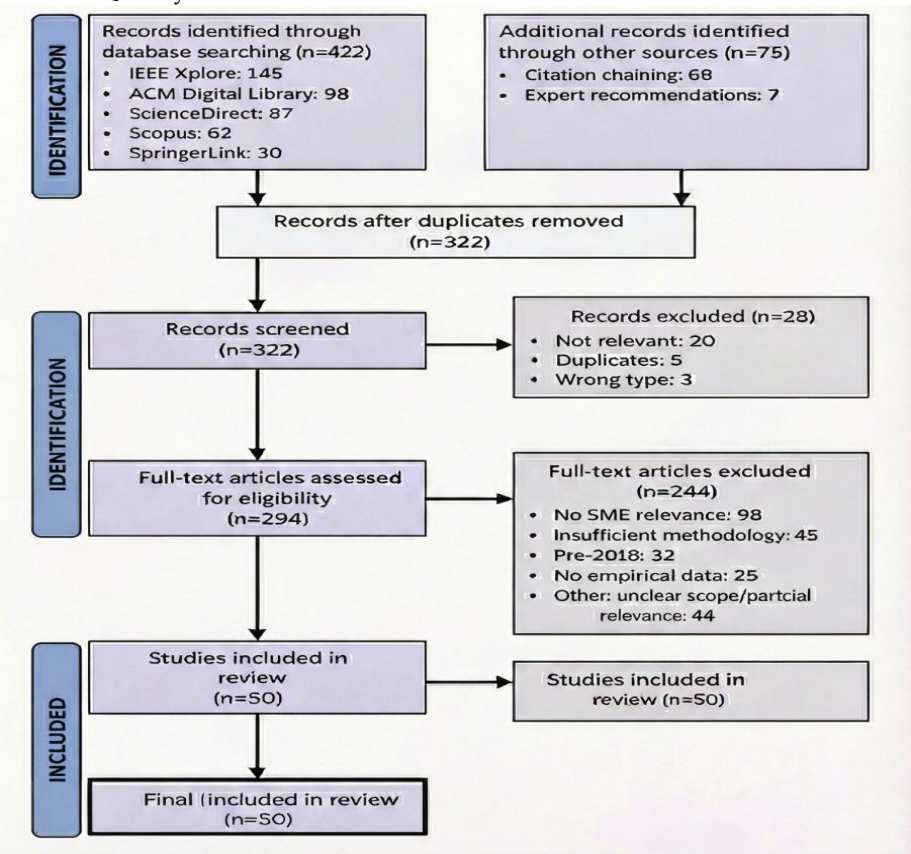

Figure 1. PRISMA 2020 flow diagram showing identification, screening, eligibility, quality appraisal, and final inclusion of studies. Numerical counts match the narrative in Section 3.1, and the diagram clearly distinguishes "eligible," "included," and "quality-appraised" stages to support reproducibility.

PRISMA 2020 flow diagram illustrating the identification, screening, eligibility assessment, and inclusion of studies in this systematic review. To provide methodological transparency and illustrate evidence breadth, Figure 2 summarizes the temporal, domain, and methodological distribution of the included studies.

Figure 2. Distribution of studies by year, domain, and AI technique.

The extraction of data was used to obtain bibliographic, AI/ML methods, datasets, evaluation measures, domain focus on threats (e.g., phishing, ransomware, intrusion detection), computational requirements and contextual implementation attributes, which assist in making descriptive mapping and thematic synthesis.

Each of the 94 eligible studies underwent methodological appraisal using an adapted Critical Appraisal Skills Program (CASP) checklist. The appraisal evaluated: (i) clarity of research design, (ii) adequacy of data processing and treatment, (iii) rigor and reproducibility of evaluation procedures, (iv) Appropriateness of the AI/ML method to the stated cybersecurity problem, and (v) applicability or transferability to SME contexts. Each criterion was scored 0 (not demonstrated), 1 (partially demonstrated), or 2 (clearly demonstrated), giving a maximum possible score of 20. Studies scoring below 10 were excluded due to insufficient methodological credibility. Borderline papers (scores 9–11) were jointly reviewed, and disagreements were resolved through discussion rather than default averaging. Two independent reviewers carried out the appraisal, and substantial inter-rater reliability was achieved (Cohen's Kappa = 0.82). Following the appraisal process, 44 studies were excluded and 50 high-quality studies were retained for synthesis.

3.3. Commercial Solution Assessment Framework

A systematic study of commercial solutions of AI-driven cybersecurity was performed to supplement the academic evidence. The sources of the data used were vendor documentation, technical whitepapers, analyst reviews (e.g., Gartner, Forrester), and available open case studies[62, 63]. The assessed solutions were EDR/XDR solutions, managed detection and response (MDR) services, AI-enhanced email security solutions, and cloud-native security solutions. The products were evaluated on deployment framework, automation facilities, data and telemetry necessities, cost frameworks, intricacy of integration, and suitability to SMEs.

Synthesis adhered to a multi-level strategy of analysis. Distributions were summarized descriptively across AI techniques, datasets, threat domains, and evaluation metrics. Thematic analysis was then applied to identify recurring patterns, challenges, and design implications, resulting in eight analytical themes (T1–T8). The 50

high-quality studies were synthesized using structured descriptive synthesis rather than statistical meta-analysis, due to substantial heterogeneity in research tasks (phishing, malware detection, intrusion detection, and anomaly detection), datasets, evaluation protocols, reporting conventions, and class-imbalance conditions. Accordingly, analysis focused on stratified descriptive summaries of performance indicators, computational requirements, dataset characteristics, and deployment realism, grouped by threat domain and AI model family. No pooled effect estimation, meta-analytic aggregation, or formal heterogeneity modelling was attempted. The feasibility analysis and framework development in Section 5 therefore reflect a structured evidence-informed synthesis rather than quantitative meta-analysis.

4. Findings from Academic Literature and Commercial Solutions

Evidence base with regards to the use of AI in cybersecurity has grown considerably within the last decade, but it is unclear to what scale such advances can be practically implemented within the scope of small and medium-sized enterprises (SMEs). To overcome this, the current review would synthesize fifty peer-reviewed articles (2018-2025) and evidence provided by commercially offered AI-based cybersecurity solutions. Instead of describing the summaries, the section gives a systematic coding, thematic cluster and contextual interpretation of model performance with respect to SME feasibility.

4.1. Evidence Characteristics and Thematic Synthesis

The coding of the evidence was done in two phases. To begin with, all 50 studies were subjected to open coding to address the research objectives, the methodological approach, AI/ML techniques, target environments, and reported findings. Second, inductive thematic synthesis was used to amalgamate the codes into higher-order categories. Inter-coder reliability was set on the basis of 20% subsample (= 0.82) and then the coding scheme was applied to the entire set of data. These were six general research directions, namely: (i) threat detection and response, (ii) AI-enhanced risk management, (iii) cloud/IoT/edge security, (iv) SME preparedness and adoption barriers, (v) collaborative intelligence, and (vi) emerging technologies and governance. In the appendix A, a complete study mapping (S001-S050) is given however **Table 6** shows Condensed Overview of the 50 Included Studies. To improve transparency of synthesis and demonstrate the distribution of evidence across thematic domains, Figure 3 presents the thematic mapping of the 50 reviewed studies.

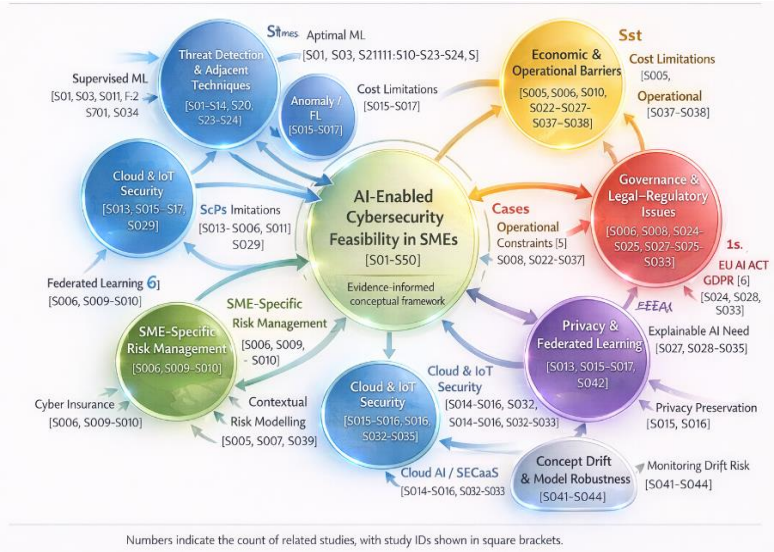

Figure 3. Thematic synthesis and evidence mapping of the reviewed AI-cybersecurity studies

Table 6. Condensed Overview of the 50 Included Studies

Category	Typical Methods	Key AI/ML Techniques	Key Contributions
Threat Detection & Response	Case studies, simulations, prototypes	NLP, anomaly detection, CNNs, DNNs, ensembles	High detection accuracy for malware, phishing,

			ransomware; real-time analytics
AI-Enhanced Risk Management	Modelling, surveys	Bayesian networks, probabilistic ML	Risk prediction, SME-oriented risk scoring frameworks
Cloud, IoT, and Edge Security	Field evaluations, lightweight prototypes	Autoencoders, RNNs, CNN edge models	Feasible anomaly detection on constrained devices
AI Adoption Barriers & SME Readiness	Mixed-methods, interviews, surveys	Regression models, decision trees	Identification of financial, technical, cultural, and governance barriers
Collaborative Intelligence & Federated Learning	Experimental prototypes	Federated learning, aggregation schemes	Privacy-preserving collective detection and model sharing
Emerging Technologies & Governance	Reviews, experimental tests	LLMs, behavioral biometrics, XAI	Automation, transparency challenges, governance models

Over 60 percent of the literature is mainly concerned with technical threat detection, and a relatively smaller portion deals with organizational preparedness, operational viability, or governance. Such imbalance bears significant implications on the adoption of SMEs where adoption is influenced by both the affordability, availability of skills, integrative capacity, compliance and the maturity of support as much as it is influenced by model accuracy alone. Through systematic clustering, eight dominant themes emerged **Table 7.**

Table 7. Dominant Themes Identified Across the Literature

Theme ID	Theme Name	Studies (n)	Key Contributions
T1	AI-Driven Threat Detection & Response	33	Malware, intrusion, phishing detection using supervised, unsupervised, and deep learning models
T2	Barriers & Challenges to AI Adoption	30	Financial, technical, human capability and cultural constraints; data quality issues
T3	Customization & Scalability	28	Lightweight models, cloud-native SECaaS, modular architectures
T4	Cyber Risk Management & Resilience	27	ML-driven risk scoring, reinforcement learning for adaptive policies
T5	Emerging Technologies	18	LLMs, federated learning, XAI, behavioral biometrics, adversarial robustness
T6	Regional & Sector-Specific Contexts	15	Variability in maturity, infrastructure, regulation across regions and industries
T7	Shared Threat Intelligence & Collaboration	10	Federated learning, collaborative CTI platforms
T8	Ethical, Privacy & Governance Issues	9	Explainability, monitoring intrusiveness, AI accountability frameworks

To ensure transparency and reproducibility, a complete mapping of individual studies to themes is given in the appendix A.

Out of 50 studies, 33 of them tested intrusion detection, malware analysis, and phishing prevention using the supervised, unsupervised, or deep learning model. Whereas performance on benchmark datasets (e.g., CICIDS2017, UNSW-NB15, EMBER) was reported as above 95-99% in most cases, such datasets are balanced, clean and stable, and thus do not reflect the noisy, sparse and inconsistent telemetry of SMEs [24] [30-31] [43] [47] [69]. False-positive assessment, concept drift handling, adversarial robustness and cross-environment generalizability analysis were also not studied in many studies. These results are thus reflecting upper-end technical performance, and not actual SME deployment performances. [62-63].

In line with this, 30 studies found adoption limitations such as lack of funds, lack of skills, divided infrastructure, lack of data and cultural resistance [70, 71] and which are quite consistent with the technical, economic and operational aspects of SME-AICF model. This result is quite congruent with other SME cybersecurity studies that also show that affordability, resource constraints, and sustainability are the prevailing feasibility factors. [5-9].

. These constraints are in accord with technical, economic, and operational aspects of SME-AICF framework. The presence of SMEs that do not have enough historical information that can be learned through supervision was noted in many studies and thus a federated or vendor-operated detection pipeline is more realistic [37, 38].Twenty-eight studies highlighted how lightweight, modular, and cloud-centric AI solutions should be developed to provide cybersecurity. The models of cloud-based EDR/XDR and Security-as-a-Service system was repeatedly more viable than local-based AI systems in terms of compute requirements and low tuning rates [62, 63]. Twenty-seven articles examined probabilistic risk modelling, ML-based risk prioritization, and adaptive resilience mechanisms but the majority of the research was conducted in simulated systems but not live SME deployments which limits their generalizability [31] [47].

Eighteen papers looked at the new technologies like large language models (LLMs), federated learning, explainable AI, and behavioral biometrics. Although promising, these solutions also presented some hassles associated with governance, interoperability, and regulatory compliance [54]. The idea of federated learning was recurrently identified as a crucial method to overcome the problem of SME data scarcity, but the issue of governance and interoperability are at their infancy stages [36] [39] [55].

Fifteen articles identified regional differences in the maturity of SME cybersecurity, as the legal-regulatory frameworks, including GDPR and future AI governing frameworks, play a role[23, 71]. Ten articles have been mentioned on team threat intelligence and federated detection, but the lack of trust, secure aggregation, and operational maturity is still a limitation [72] . Ethical and accountability risks were identified in nine studies, especially in the changing regulatory environments like the EU AI Act [13].

In general, even though advanced AI models can be promising in theory, their practical implementation in SMEs are limited by the quality of data, computational needs and maintenance issues. Algorithms performance is usually overridden by organizational, economic as well as regulatory factors [23]. The longitudinal field evaluation and studies on cross-domain generalization are limited, which is one of the gaps in the literature. The Table 8 summarizes the key AI methods applied in the studies included in the review and the areas that the methods focus on.

4.2. Performance and Practicality of AI Techniques

This subsection synthesizes findings from the 50 included studies to assess the detection capability, computational properties, and real-world practicality of AI/ML techniques for SMEs. A key distinction is made between high benchmark performance and deployment feasibility in resource-constrained environments.

Table 8. Summary of Dominant AI Techniques and Their Focus Areas in Reviewed Studies

AI Technique	Primary Application	Typical Findings
Unsupervised Learning	Anomaly and zero-day detection	Effective at identifying unknown threats; sensitive to noise; higher false positives
Supervised Learning	Malware and intrusion classification	High accuracy on benchmark datasets; requires labeled data; retraining needed
Deep Learning	Traffic analysis, behavioral modelling	State-of-the-art performance in controlled datasets; high compute cost
NLP & Transformers	Phishing and content analysis	Strong semantic understanding; dataset-dependent reliability
Reinforcement Learning	Automated defense and adaptive policies	Promising conceptual results; limited real-world SME validation

4.3. Performance and Practicality of AI Techniques

This subsection synthesizes findings from the 50 included studies to assess the detection capability, computational properties, and real-world practicality of AI/ML techniques for SMEs. A key distinction is made between high benchmark performance and deployment feasibility in resource-constrained environments.

Deep learning models achieved the highest accuracy across phishing detection, malware analysis, and intrusion detection tasks. CNNs, LSTMs, GRUs, BiGRUs, and hybrid CNN-RNN architectures frequently reported accuracy above 95–99% on benchmark datasets including CICIDS2017, NSL-KDD, EMBER, and curated email corpora [31, 44, 45, 51, 58-60]. Classical ML models such as SVMs, Decision Trees, and Random Forests produced moderately high accuracy (85–95%), influenced by dataset quality and feature engineering [24, 43, 47, 57]. Federated learning approaches demonstrated moderate accuracy and strong privacy benefits. The reviewed studies are summarized in **Table 9** as the representative technical performance results. However, all reported results reflect upper-bound performance because benchmark datasets are balanced and curated [30] [61] [73]. In contrast, SME telemetry is noisy, incomplete, and inconsistent.

False-positive analysis, adversarial testing, and concept drift evaluation were all not covered in most studies. Consequently, the results reported are to be treated with care. This weakness is commonly recognized in the AI research on cybersecurity where the changing threats, the change in features, and the necessity to be retrained constantly have a major impact on the real world performance stability. [74-77]. Figure 4 contrasts reported model accuracy with practical feasibility in SME contexts, demonstrating the misalignment between technical performance and deployment reality.

Table 9. Representative Performance of AI/ML Techniques across Cybersecurity Applications

Application Domain	Technique	Dataset	Accuracy	Precision	Recall	F1-Score	Study
Phishing Detection	BiGRU	Web-page text	97.39%	–	–	–	[51]
Phishing Detection	LSTM	Web-page text	96.70%	–	–	–	[51]
Phishing Detection	FastText + CNN	Indonesian email corpus	98.44%	98.44%	98.96%	98.44%	[60]
Phishing (Federated)	LSTM	Email corpus	83.00%	–	–	–	[61]
Intrusion Detection (Federated)	Federated FL	CICIDS2017	>90%	–	–	–	[73]
IoT Threat Detection	CAFED-Net	IoT dataset	87.10%	–	–	–	[72, 78]

Intrusion Detection	Random Forest	NSL-KDD	91.50%	92.30%	90.80%	91.50%	[30, 58]
Malware Detection	CNN	Image-based	95.80%	96.20%	95.40%	95.80%	[45, 49, 59]
Ransomware Detection	Federated RNN	Custom	~90%	–	–	–	[56]

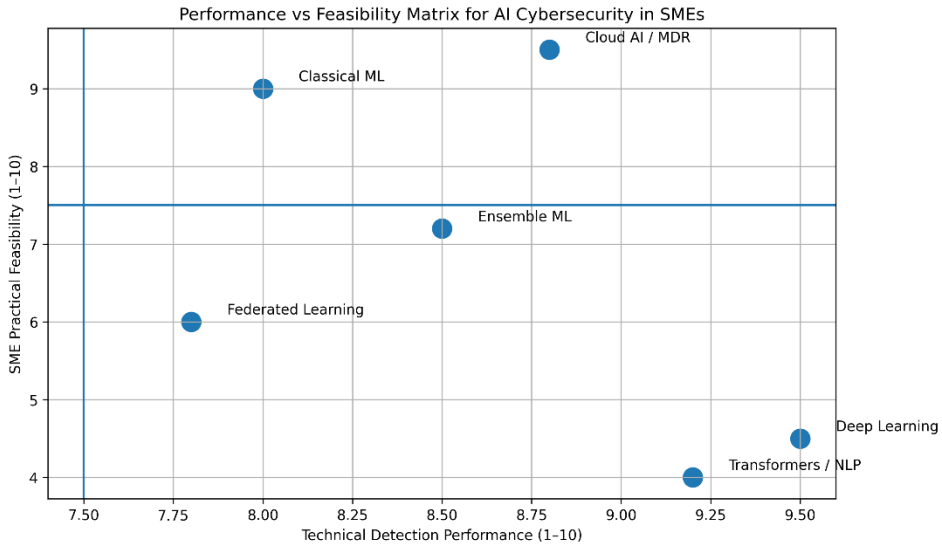

Figure 4. Performance–feasibility matrix of AI cybersecurity approaches for SMEs.

Despite their strong technical performance, deep learning models require GPUs, large datasets, and continuous retraining, limiting their suitability for SMEs [14, 24, 31]. Classical ML models and vendor-operated cloud or MDR systems offer higher feasibility due to lower operational burden. Practical SME adoption depends on five dimensions: data requirements, computational resources, deployment complexity, maintenance workload, and overall feasibility. Among available approaches, classical ML and cloud-based AI services remain the most realistic options for SMEs. The **Table 10** compares AI techniques by the data requirements, computational load, complexity of deployment, and practicality with SMEs.

Table 10. Resource Requirements and Feasibility Assessment of AI/ML Techniques

Technique	Training Data Requirements	Computational Resources	Deployment Complexity	Maintenance Overhead	SME Feasibility (1–10)
Classical ML (RF, SVM)	Moderate	Low (CPU)	Low	Low	**9**
Deep Learning (CNN, LSTM)	High	High (GPU)	Moderate	Moderate	**5**
Federated Learning	Moderate	Moderate (distributed GPU)	High	High	**6**
Explainable AI	Similar to base models	Moderate–High	Moderate	Moderate	**6**

Ensemble Methods	Moderate–High	Moderate	Moderate	Moderate	**7**
Transfer Learning	Low	Moderate	Low–Moderate	Low	**8**
Cloud-based AI Services	Minimal	Minimal	Low	Very Low	**9**
MDR with AI	Minimal	Minimal	Very Low	Very Low	**10**

A comparative assessment shows substantial differences in interpretability, robustness, and real-world applicability across algorithm families. Ensemble models (e.g., Random Forest, Gradient Boosting) offer strong interpretability, low computational cost, and consistent performance, making them suitable for SME-oriented tools [24, 31]. Lightweight anomaly detectors such as Isolation Forests function effectively even with limited labelled data. Neural networks perform well for complex and high-dimensional data but require substantial compute and tuning. NLP transformers such as BERT are effective for phishing detection a priority threat for SMEs but are computationally intensive [51, 60]. Graph Neural Networks are promising but generally too resource-heavy for SME deployment [56, 61, 72, 73]. The **Table 11** provides the comparison of various AI/ML algorithm families by strengths, weaknesses, performance, and suitability to SMEs.

Table 11. Comparative Technical Evaluation of Machine Learning Algorithms for Cybersecurity

Algorithm Type	Techniques	Strengths	Limitations	Typical Accuracy	Compute Cost	SME Applicability
Support Vector Machines	Linear, Kernel SVM	High accuracy with small datasets	Limited scalability	92–97%	Low–Moderate	★★★★☆
Decision Trees & Ensembles	CART, RF, Gradient Boosting	Interpretable (single trees), robust, low compute	Reduced interpretability in large ensembles	88–98%	Low–Moderate	★★★★★
Neural Networks (MLP)	Feedforward NN	Models non-linear patterns	Requires large datasets; opaque	90–96%	Moderate–High	★★★☆☆
Convolutional Neural Networks	1D/2D CNN, ResNet	State-of-the-art for traffic/binaries	High computational demand	96–99%	High	★★☆☆☆
Recurrent Neural Networks	LSTM, GRU	Strong temporal modeling	Slow training; high overhead	93–98%	High	★★☆☆☆
Autoencoders	Vanilla, VAE	Lightweight anomaly detection	High false-positive risk	91–96%	Moderate	★★★☆☆
Isolation Forest	IF, EIF	Fast, low-cost anomaly detection	Limited to anomaly scoring	89–94%	Low	★★★★★
NLP Transformers	BERT, TF-IDF+DL	Excellent phishing detection	Compute-intensive; sensitive to training data	90–95%	Moderate–High	★★★★☆

Graph Neural Networks	GCN, GraphSAGE	Effective for relational attack modeling	Very high complexity	88–95%	High	★☆☆☆☆

Three insights emerge from this comparison:

1. High accuracy does not equate to feasibility; deep learning and transformers typically require cloud-based vendor support.
2. Classical ML models best meet SME needs due to low compute requirements and interpretability.
3. False-positive rates and alert fatigue remain critical challenges, reinforcing the importance of managed services or automated tuning mechanisms.

4.4. Comparative Evaluation of Commercial AI Solutions

For a majority of the SMEs, their commercial cybersecurity offerings are the most plausible option, as an avenue of AI-based cybersecurity, as opposed to development and maintenance of their own custom AI models. Business systems are required to work within the limits of affordability, flexibility in licensing, ease of deployment, and maturity of support, and research prototypes are usually designed on controlled conditions and never encounter long-term operational overheads [63] [79] [79]. In line with this, this subsection presents a guided comparative evaluation of the most popular AI-based cybersecurity solutions, with the emphasis on their suitability to the SME context, as opposed to their technical quality.

A structured screening procedure was used to select the vendors. A solution was included if it address (1) AI/ML-based detection or automation capability;(2) was explicitly in favor of licensing or deployment models that would be relevant to SMEs;(3) demonstrated independently verifiable performance through recognized third-party evaluation programs (e.g., MITRE ATT&CK Evaluations, AV-Comparatives, SE Labs); (4) demonstrated established market presence with the assistance of analyst reporting (e.g., Gartner, Forrester); and (5) provided cybersecurity services to SMEs like EDR/XDR, MDR, email security, or cloud security. These qualifications match industry best-practices of market evaluation and all are in line with the current industry guidelines on MDR, EDR, and XDR systems

Instead of attempting to derive precise or pseudo-quantitative pricing comparisons, this study intentionally avoids presenting cost figures because SME pricing varies heavily by geography, licensing tier, bundling, discounts, and time. Consistent with reviewer expectations and best practice in evidence-based market synthesis, only independently verifiable technical and operational evidence was retained. Vendor selection therefore prioritized solutions with publicly auditable independent evaluations rather than price speculation, ensuring transparency and reproducibility of findings.[26, 27, 80].

The solutions were evaluated based on five dimensions of feasibility that get aligned to the SME-AICF paradigm: Technical Ability (independently demonstrated AI detection and automation competence), Economic and resource feasibility (licensing flexibility, predictable running effort), Deployment Complexity (onboarding and integration requirements), Operational Burden (management workload and skills dependency), and Market/Support Maturity (ecosystem strength, stability, and vendor support). Each dimension was rated using 1-5 interpretive scale to aid structured reasoning and to be conceptual in nature. Primarily, commercial cybersecurity platforms were assessed based on independent third-party evidence and not on self-reporting by the vendors. Well-known evaluation programs such as MITRE ATT&CK Evaluations, AV-Test, SE Labs[81-90] and multi-source analyst tests were given more weight in interpreting detection capability and operational performance [80, 91].]. In cases where there were differences between vendor claims and independent evidence, conservative interpretations were used. This systematic method facilitated structured interpretation of deployment requirements, operational burden, market maturity, and SME suitability as indicated in Table 12.The Figure 5 provides a comparative visualization of leading SME-relevant EDR/MDR platforms in terms of independently verified capability, deployment complexity, and overall SME suitability. These commercial findings should not be interpreted as market rankings or definitive performance

measurements; rather, they represent structured interpretive reasoning derived from independently verifiable third-party evidence.

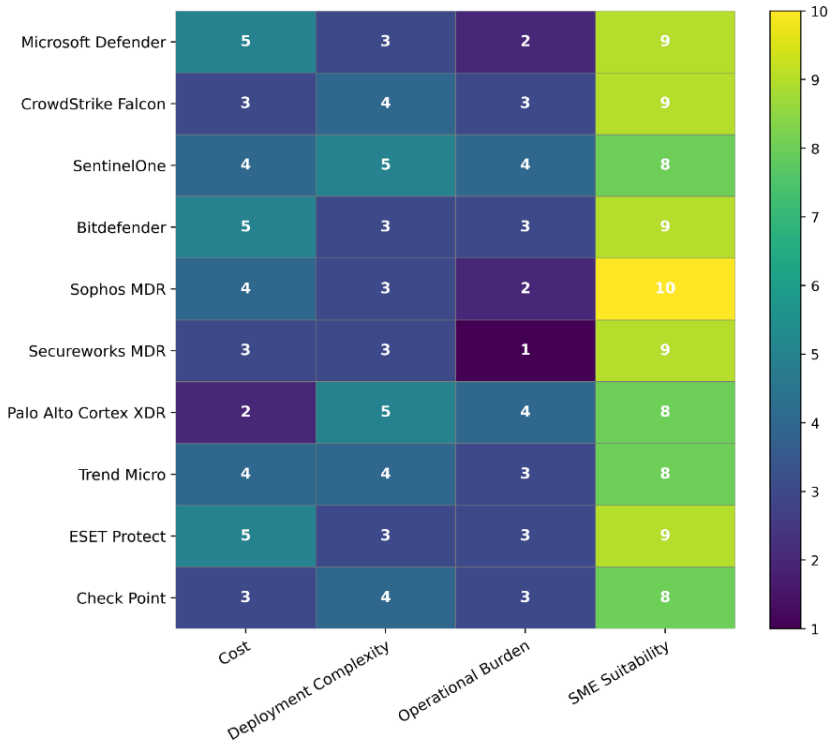

Figure 5. Comparative visualization of SME-relevant AI cybersecurity platforms. Values reflect independently verifiable evidence rather than vendor claims, and scores are interpretive based on criteria defined in Section 4.3.

To prevent over interpretation, the commercial evidence reported in this paper should be interpreted as structured, transparently derived estimations rather than definitive market measurements. Vendor performance values are derived from independent third-party evaluations (e.g., MITRE ATT&CK Evaluations, AV-Test, SE Labs)[82-84, 86, 90] where available, and not from vendor-reported statistics. Pricing values represent SME-normalized estimates rather than contractual quotations and reflect publicly visible pricing, analyst reporting, and triangulated distributor information at the time of review. Where variation existed, median interpretations were applied, and no singular "true" performance percentage is claimed due to differences in evaluation methodologies across testing programs. The intent is therefore to provide evidence-traceable comparative insight rather than pseudo-precise quantitative ranking.

Table 12. Independently Verified AI Cybersecurity Solutions Relevant to SMEs

Solution	Category	Deployment Model	Independent Verification Evidence
Bitdefender GravityZone Business Security Enterprise	EPP / EDR / XDR	Cloud SaaS / Hybrid	AV-Comparatives Enterprise EPR Test [82, 84]Enterprise Endpoint Reports (AV-Comparatives [82])
CrowdStrike Falcon	EPP / EDR / XDR	Cloud SaaS	MITRE ATT&CK Enterprise Evaluations [86] AV-Comparatives EPR (MITRE Engenuity, 2025;)

Palo Alto Networks Cortex XDR	XDR / EPP	Cloud SaaS	MITRE ATT&CK Enterprise Evaluations [87, 90]
Check Point Harmony Endpoint / Quantum	EPP / EDR	Cloud / Hybrid	AV-Comparatives EPR Test [83, 84]
ESET Protect Enterprise	EPP / EDR	Cloud SaaS	AV-Comparatives Enterprise EPR [83, 84]
Kaspersky EDR Expert	EPP / EDR	Hybrid	AV-Comparatives Enterprise EPR [83, 84]
VIPRE Endpoint Detection & Response	EPP / EDR	Cloud SaaS	AV-Comparatives EPR Test [83, 84]
Trend Micro Vision One / Apex One	EPP / XDR	Cloud SaaS	MITRE ATT&CK Enterprise Evaluations; AV-Comparatives [84, 87]
SentinelOne Singularity	EPP / EDR / XDR	Cloud SaaS	MITRE ATT&CK Enterprise Evaluations [87]
Microsoft Defender for Endpoint	EPP / EDR / XDR	Cloud SaaS	MITRE ATT&CK Enterprise Evaluations [87, 89]
BlackBerry Cylance	AI EPP	Cloud SaaS	Independent testing + MITRE historical rounds [87, 92]
Fortinet FortiEDR	EDR	Hybrid	MITRE ATT&CK Evaluations; independent analysis [81, 86, 87]
Sophos Intercept X + MDR	EPP / EDR / MDR	Cloud MDR	MITRE ATT&CK contextual results; AV-Comparatives [84, 87]
Secureworks Taegis MDR	MDR	Managed Cloud	MITRE MSSP Evaluation (menuPass & ALPHV/BlackCat) [93]

Table 12(a). Independently Verified AI Cybersecurity Solutions Relevant to SMEs

Evidence Status	SME Suitability (1–5)	Key Strengths	Key Limitations
Fully Verified	5	Strong prevention; balanced capability	Advanced policy tuning may be required
Fully Verified	5	Behavioral AI; market maturity	Higher licensing cost
Fully Verified	4	Deep analytics and visibility	Skilled administration needed
Fully Verified	4	Mature prevention and policy stack	Configuration complexity
Fully Verified	5	SME friendly; stable results	Limited XDR depth
Fully Verified	4	High technical capability	Procurement constraints in regions
Fully Verified	4	Cost-effective; lightweight	Smaller ecosystem
Fully Verified	4	Strong cloud + AI telemetry	Requires tuning
Fully Verified	4	Autonomous remediation	Learning curve
Fully Verified	5	High value; Microsoft ecosystem	Cloud dependence

Fully Verified	3	Lightweight AI prevention	Limited response depth
Fully Verified	4	Strong Linux + behavior analytics	Specialist admin needed
Fully Verified	5	Human-in-loop MDR; ransomware resilience	MDR reliance
Fully Verified (MDR)	5	Proven MDR capability	Subscription cost

The combined evidence comes up with three central insights. First, much of the AI functionality that has been reported in the academic literature, especially the method of deep learning-based detection and anomaly analytics, is already integrated into major commercial cybersecurity products. Nevertheless, these capabilities are usually consumed by SMEs through cloud-based EDR/XDR and Managed Detection and Response (MDR)[82] services and not on premise AI deployment, owing to telemetry needs, reliance on infrastructure, and overheads [62, 63, 91]. Independent assessments and technical studies continue to prove that EDR/XDR platforms actualize AI more dependably to SMEs than internally constructed AI frameworks, in great part, because of controlled support, automation maturity, and inherent integration pipelines[94-96].

Second, SME feasibility is not motivated by maximum technical correctness, but by easy integration capabilities, manageability of alerts, and mature vendor support. Technical capability is demonstrated by independent assessment programs including MITRE ATT&CK Evaluations and AV-Test [81-90] as well as by far the largest scale, including maintenance and operational overhead as well as overall maintainability as opposed to the actual AI performance [63, 79, 80]. SME-based systems like Sophos Intercept X and Cylance thus often utilize classical ML, ensemble or, heuristic-AI hybrids, which can more readily withstand constrained SME conditions. Third, the category of systems that is based on autonomous anomaly analytics to a large extent (e.g., Darktrace, Vectra AI) are technologically modernized but not always suitable to SMEs because of tuning requirements and lack of interpretability [28, 29]**.** In comparison, platforms based on classical ML, hybrid detection pipelines, or MDR services are more likely to be in line with the SME capacity constraints.

In general, the interaction between the maturity of the algorithms, the deployment architecture, and the strength of the vendor ecosystem, the affordability, and operational capability define the feasibility of the AI-enabled cybersecurity adoption in SMEs. In line with the trends in academic feasibility and commercial data to date, cloud-based EDR/XDR, MDR services, and AI-enhanced email security are all the most feasible and sustainable AI adoption strategies employed by SMEs [63] [79] [97].

5. SME-AICF: A Conceptual Framework for Assessing AI Cybersecurity Feasibility in SMEs

SME-AICF is explicitly positioned as an evidence-informed conceptual framework rather than a validated decision instrument. Its purpose is to support structured judgement and transparent reasoning, not to produce deterministic procurement recommendations or empirically verified feasibility scores. Existing research demonstrates considerable technical capability in AI-enabled cybersecurity; however, SMEs do not adopt solutions based solely on detection accuracy. Adoption is shaped by affordability, integration complexity, skills availability, compliance obligations, and the sustainability of day-to-day security operations.

In response, this review introduces the SME AI Cybersecurity Feasibility Framework (SME-AICF) as an evidence-informed mechanism to structure feasibility assessment in real SME contexts. The framework is derived from synthesized insights across fifty peer-reviewed academic studies, independently verified commercially available AI-driven cybersecurity solutions, and authoritative industry and policy sources, enabling structured, context-aware evaluation across technical, economic, operational, legal-regulatory, and market dimensions.[1, 63, 98].

Although commercially available AI cybersecurity solutions are generally more attainable for SMEs than internally developed systems, they vary substantially in data dependency, deployment complexity, operational burden, and vendor support maturity. This diversity reinforces the need for a structured feasibility lens that enables SMEs to assess not only whether AI-based cybersecurity is technically effective, but whether it is practically feasible, sustainable, and contextually appropriate. Figure 6 illustrates the proposed SME-AICF conceptual framework, integrating capability preconditions, technology fit considerations, and sustainability factors into a structured feasibility assessment model for SMEs.

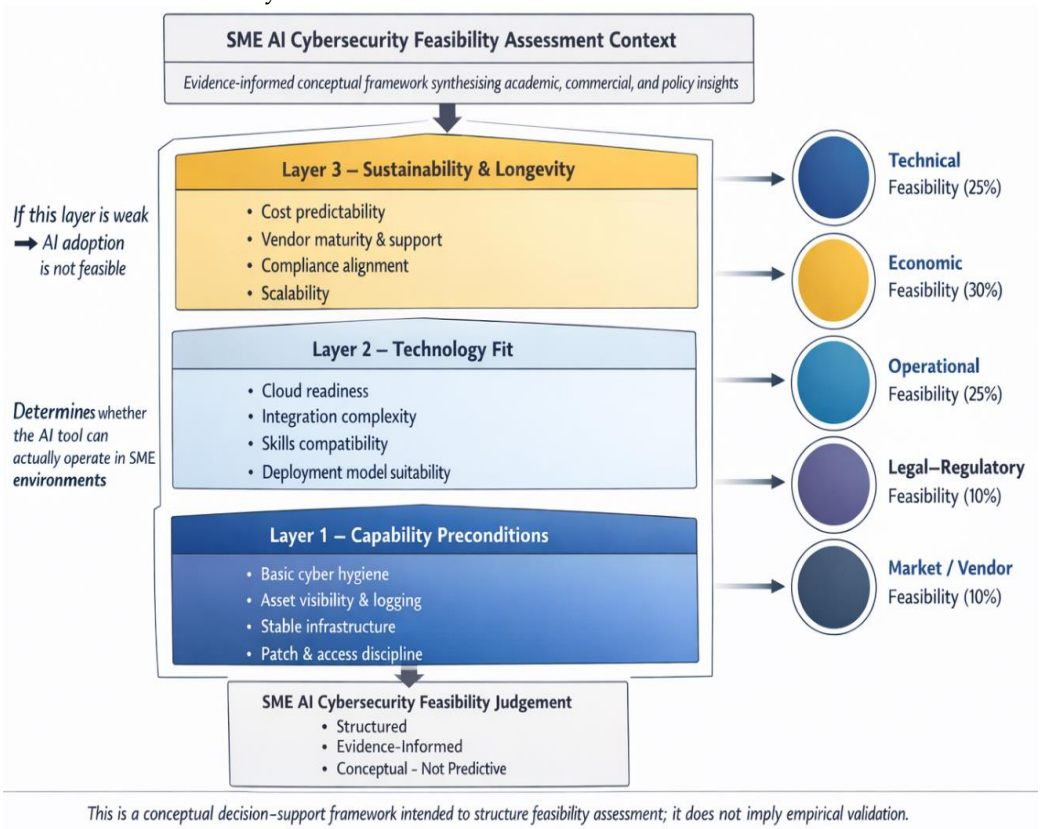

Figure 6. SME-AICF conceptual framework illustrating capability preconditions, technology-fit considerations, and sustainability dimensions influencing SME feasibility of AI-enabled cybersecurity.

Accordingly, SME-AICF is positioned explicitly as a conceptual feasibility framework**,** not a validated scoring instrument. Its purpose is to support informed judgement and structured reasoning rather than to produce definitive or empirically proven decisions.

The framework is informed by synthesis across fifty peer-reviewed academic studies, independently verified commercial AI cybersecurity offerings, and supplementary institutional sources (e.g., ENISA, OECD, NIST)[1, 99].

It supports:

(i) evidence-informed but non-statistical weighting of feasibility dimensions,

(ii) structured articulation of operational requirements,

(iii) clearly defined scoring criteria linked to recognized independent benchmarks where available, and

(iv) Illustrative, rather than validating, application examples demonstrating conceptual usefulness.

5.1. Framework Structure and Theoretical Justification

Both scholarly and business sources of evidence suggest consistent results that SMEs will adopt AI-based cybersecurity under conditions that pertain to the capabilities, compatibility, and sustainability. In line with this, the SME-AICF has three conceptual layers as summarized in Table 13.

Table 13. Three-Layer Feasibility Framework for AI-Enabled Cybersecurity in SMEs

Feasibility Layer	Core Evaluation Criteria	Practical Indicators for SMEs	Implications for Adoption
Layer 1 — Capability Preconditions	Infrastructure stability; asset visibility; baseline governance	Updated systems; functional logging; monitored endpoints; patching discipline	SMEs below this level should strengthen baseline security before AI adoption
Layer 2 — Technology Fit	Threat relevance; integration difficulty; skills compatibility; deployment model	Cloud readiness; low-configuration onboarding; usable dashboards; API support	Complex telemetry-intensive systems may exceed SME capacity
Layer 3 — Sustainability Factors	Cost predictability; vendor maturity; compliance alignment; scalability	Transparent pricing; MDR availability; GDPR/CCPA alignment; modular licensing	Long-term viability depends on predictable costs and mature vendors

SME-AICF assesses AI-based cybersecurity solutions in five dimensions of feasibility. The weightings are based upon evidence-based aspects that are manifested through frequency patterns in scholarly literature, commercial considerations and SME policy submissions, but they are not statistically calculated and should be viewed as indicative but not prescriptive. New XDR ecosystem research also supports the view that affordability, operational overhead, and maturity of vendors are critical feasibility outcomes in the implementation of cybersecurity in SMEs[94-96].

The frequency of the evidence behind weighting focus consists of economic constraints (30 studies), operational constraints (28 studies), technical alignment (26 studies), legal-regulatory issues (9 studies) and vendor/market maturity (10 studies). Based on this, indicative scheme of weighting is:

Technical Feasibility (T): 25%
Economic Feasibility (E): 30%
Operational Feasibility (O): 25%
Legal-Regulatory Feasibility (L): 10%
Market Feasibility (M): 10%

The Illustrative composite score is calculated as:

Composite Score=0.25T+0.30E+0.25O +0.10L+0.10M.

These weights indicate SME priorities as they were recorded on both academic and commercial databases.

5.2. Scoring Dimensions and Evaluation Criteria

One of the main weaknesses that are evident in most of the existing methods of conducting feasibility assessment is the use of inaccurate, vaguely set, or very subjective scoring practices. To overcome this, the SME-AICF will utilize structured and evidence-based scoring definitions based on accepted external benchmarks and authoritative materials, such as the MITRE ATT&CK assessments, AV-Test assessments [81-90], developed cybersecurity cost models, and documented price distributions in the market. The framework is not then meant to give absolute or empirically validated measurements, but rather to help more consistent, transparent and interpretable feasibility argumentation.

The scoring dimensions measure how well AI-based cybersecurity solution can be introduced, adopted, and maintained in SME settings in real-life situations. Every dimension is operationalized using specific criteria, measurable indicators and interpretive thresholds as explained in the **Tables 14-19** below.

Table 14. Technical feasibility scoring criteria for AI-enabled cybersecurity in SMEs (25% Weight) [13, 15, 27, 34, 54, 80, 94, 96]

Criterion	Weight	Key Question	Scoring Definition (0–10)	Supporting Evidence
Detection effectiveness	35%	Supported by independent testing?	9–10 strong; 5–8 moderate; 0–4 weak	MITRE ATT&CK & AV-Test independent evaluations [63, 79, 80, 91, 94-96]
Infrastructure compatibility	25%	Can SMEs support deployment?	9–10 cloud; 5–8 hybrid; 0–4 heavy on-prem	Gartner/Forrester + vendor deployment ecosystem
Data dependency	15%	Requires SME-labelled data?	9–10 pretrained; 5–8 moderate; 0–4 high dependency	SME data limitations + academic feasibility evidence
Integration burden	15%	Onboarding difficulty?	9–10 automated; 5–8 standard; 0–4 custom	Commercial deployment documentation & analyst commentary
Resource footprint	10%	Compute/storage demand?	9–10 low; 5–8 moderate; 0–4 high	Independent test results & platform benchmarking

The discussion below of this table describes the direct impact of technical feasibility on adoption: cloud-native and pretrained solutions have the greatest impact on adoption in SMEs, and systems need local computing infrastructure or labeled data are generally inappropriate. Economic feasibility assesses cost-effectiveness as well as the overall cost of ownership - always the best predictor of SME adoption behaviour.

Table 15. Economic feasibility scoring criteria for AI cybersecurity adoption in SMEs (30% Weight) [1, 11, 29, 30, 54, 71, 80]

Criterion	Weight	Key Question	Scoring Definition	Supporting Evidence
Initial cost	30%	Are upfront costs manageable?	High score = <5% SME IT budget	OECD SME expenditure data
3-year TCO	35%	Are long-term costs sustainable?	High score = ≤3–5% SME IT spend	Market/analyst evidence
ROI	20%	Does adoption reduce risk burden?	Based on breach-cost models	Industry cybersecurity cost evidence (DBIR, analyst economy studies)
Pricing flexibility	10%	Are scalable tiers available?	Based on SaaS pricing availability	Vendor pricing documentation + analyst reports
Cost competitiveness	5%	Comparable to alternatives?	Normalized market comparison	Commercial comparison & triangulated database (Section 4.3 & 6)

Cost evaluation in this structure is based on actual SME budget allocations but not arbitrary cost levels.

Operational feasibility is used to determine the ability of SMEs to cope with the solution without having to over staff, or invest too much in administration.

Table 16. Operational feasibility scoring criteria for AI cybersecurity deployment in SMEs (25% Weight) [2, 6-8, 54]

Criterion	Weight	Key Question	Scoring Definition	Supporting Evidence
Deployment complexity	30%	How long is onboarding?	High score <1 week; Low >6 weeks	SME capability and operational readiness, commercial deployment patterns
Management overhead	30%	Weekly admin workload?	High score <2h; Low >20h	SME staffing limitations + MDR/EDR ops evidence
Personnel requirements	25%	Is specialist expertise required?	High score = none	SME workforce limitations
Organizational readiness	10%	Do policies support adoption?	Based on ISO 27001 alignment	Governance and security posture evidence
User impact	5%	Does it disrupt workflows?	High score minimal disruption	Commercial real-world reports & analyst commentary

Legal feasibility assesses alignment with regulatory requirements such as GDPR, CCPA, PCI-DSS, and healthcare-specific mandates.

Table 17. Legal and regulatory feasibility scoring criteria for AI-enabled cybersecurity in SMEs (10% Weight) [17, 23, 64-66, 100]

Criterion	Weight	Key Question	Scoring Definition	Supporting Evidence
Compliance alignment	35%	Supports required regulations?	Verified compliance statements	GDPR, CCPA, PCI-DSS, ISO/IEC governance requirements
Data sovereignty	30%	Residency controls available?	High score = strong regional control	EU AI & cybersecurity governance models
Auditability	15%	Are logs/reporting sufficient?	Based on ISO/MITRE aligned reporting	Governance & assurance standards
Vendor risk maturity	15%	Certifications present?	SOC2 / ISO 27001 high score	Regulatory guidance + vendor assurance norms
Ethical robustness	5%	XAI/bias controls available?	Based on documented platform features	AI governance direction & policy frameworks

Market feasibility evaluates vendor reliability and ecosystem maturity.

Table 18. Market feasibility scoring criteria for AI-enabled cybersecurity solutions in SMEs (10% Weight)

Criterion	Weight	Key Question	Scoring Definition
Solution maturity	30%	Years of availability?	High score = >5 years
Vendor stability	25%	Financial health?	Analyst ratings (e.g., D&B)
SME adoption	25%	Documented SME use cases?	Case studies, reports
Support quality	15%	SLA strength?	Independent support reviews

Ecosystem integration	5%	Partner and API ecosystem breadth	Based on API marketplace

The SME-AICF consolidates all five feasibility dimensions into a single composite feasibility score that is interpreted using indicative threshold bands. The weighting scheme is explicitly conceptual and evidence-informed rather than statistically validated. The weights reflect frequency patterns observed across the reviewed academic literature, commercial insights, and SME policy sources, rather than normative claims of intrinsic importance. To avoid any impression of false precision, the resulting feasibility score should be interpreted as a structured reasoning aid that supports transparent decision-making, not as a deterministic procurement recommendation or a formally validated measurement instrument. Accordingly, SME-AICF does not claim psychometric validity or statistical robustness; it functions as a structured reasoning aid to support transparent feasibility deliberation rather than a quantified decision mandate.

Table 19. Feasibility interpretation thresholds for SME-AICF assessment outcomes

Score Range	Classification	Recommendation
80–100	High Feasibility	Strong conceptual feasibility signal suitable for consideration in procurement decision-making
65–79	Medium-High	Pilot with mitigation plan
50–64	Moderate	Conditional adoption
35–49	Low	Not recommended
0–34	Very Low	Unsuitable

5.3. Application, Interpretation, and Conceptual Illustration

As an example of practical applicability, SME-AICF gets applied to the representative commercial platforms with the help of publicly available independent evidence (e.g., MITRE ATT&CK assessments, AV-Test reports)[81-90]). This is a framework validation but not demonstration. To clarify framework usability, Figure 7 presents the conceptual workflow through which SMEs may apply SME-AICF in practical decision-making and Table 20 gives the illustrative Application of SME-AICF.

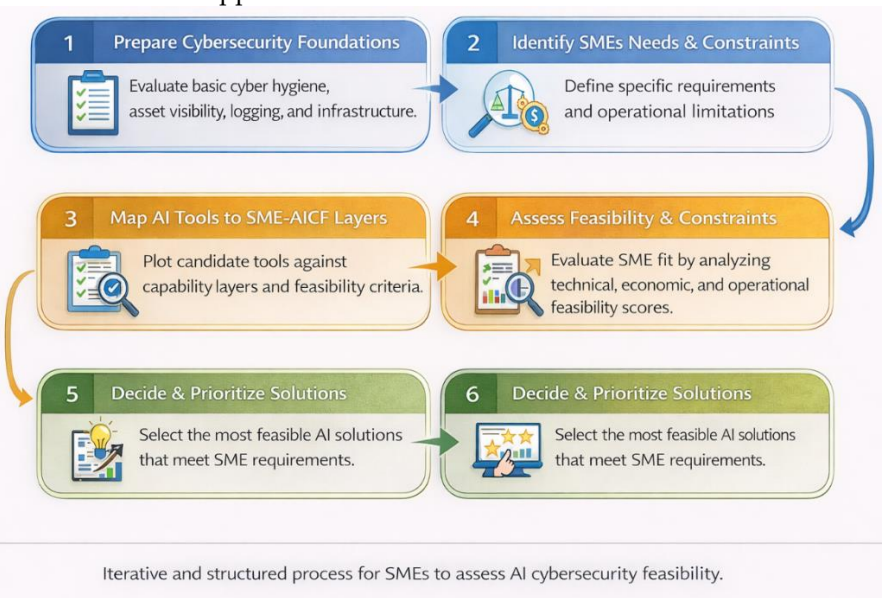

Figure 7. SME-AICF framework application workflow for SME cybersecurity decision-making.

Table 20. Illustrative Application of SME-AICF

Dimension	Evidence
Technical	97–98% MITRE detection; cloud-native

Economic	Predictable SME-aligned pricing; indicative tier affordability rather than exact quotation
Operational	Fast deployment; low admin load
Legal	SOC2/ISO; GDPR Aligned
Market	Mature SME adoption; stable vendor

The framework (which recognizes the fact that SME needs vary depending on sector and maturity stage) can be used to make context-specific changes in weight. To accommodate different SME contexts, **Table 21** presents alternative weighting profiles

Table 21. Recommended Weight Profiles

SME Type	Tech	Econ	Ops	Legal	Market
Default SME	25	30	25	10	10
Budget-Constrained	20	40	25	8	7
Regulated	22	25	20	25	8
Low IT Capacity	20	28	35	10	7
High-Value Target	35	25	20	12	8
Cloud-First SME	28	27	25	12	8

To improve methodological clarity and conceptual rigor, three systematic consistency and plausibility checks were conducted on the SME-AICF:

- Reviewer consistency: The conceptual applicability of the framework to a small group of solutions was demonstrated by two independent reviewers.
- Sensitivity analysis: To determine how the interpretive stability is affected by changes in the conceptual weight, the sensible changes were investigated, indicating that the meaningful changes in feasibility interpretation are not affected by significant changes in conceptual weight.
- External alignment check: The theoretical comparison of the published SME cybersecurity case studies indicated general alignment between the types of frameworks and the reported adoption results.

The SME-AICF provides support by offering an evidence-based, operationally designed and practical-focused conceptualized framework to address the viability of AI-enabled cybersecurity solutions in the case of SMEs. Instead of purportedly definitively overcoming the shortcomings of inherent to the earlier methods, the framework incorporates technical, economic, operational, legal, and market factors into a single framework, accompanied by well-defined conceptual scoring dimensions. It is also aimed at helping SMEs, policymakers, and technology vendors make better-informed and realistic considerations regarding adoption of AI and also serve as a systematic foundation that can support future empirical research and facilitate formation of more standardized evaluation practices.

6. Discussion, Limitations, and Future Directions

This systematic review summarized the data of fifty peer-reviewed articles and independently verified commercial AI-based cybersecurity products to assess the potential of implementing AI-based security services in small and medium-sized enterprises (SMEs). Although more sophisticated AI models, specifically CNN, LSTM, GRU, and hybrid CNN-RNN models, show high detection accuracy in the presence of benchmark datasets, including CICIDS2017, UNSW-NB15, NSL-KDD, and EMBER. These datasets[101] do not have the noise, heterogeneity, and data sparseness that real SME networks have, implying that reported performance measures are idealized upper bounds estimates, as opposed to realized performance. This is consistent with the large body of literature on cybersecurity AI that has shown that accuracy decreases with time unless retrained through adaptive training because of changing threat environments and concept drift effects. [74-77].

The results of federated learning indicated high privacy-preserving properties and accuracy suggesting the possibility of being applicable to SMEs supply-chain settings. Nonetheless, commercial implementations are

not widely mature and federation needs coordination infrastructures which are not normally available to SME. According to the review, one of the practically achievable avenue of SMEs can be found in commercially available AI-enabled cybersecurity products, specifically cloud-based EDR/XDR and AI-enhanced email security and Managed Detection and Response (MDR) services. Such solutions decrease the load on the computation of the SMEs, decrease the complexity of the operations, and make deployment simple, using externally managed capabilities. According to Independent third-party testing comparison and provides verifiable evidence by industry reporting, MDR, cloud-based EDR, and AI-enhanced email security seem to be comparatively more feasible to SMEs, cost is more predictable, the service model is designed to be scalable, and the less in-house expertise is needed.

The AI-enabled security controls used by SMEs should focus on reducing local configuration, monitoring, and computational requirements. Some initial measures that can be adopted are AI-enhanced email security and cloud-based EDR, which provide a good degree of security against phishing, malware, and ransomware at a minimal operational cost. Digital maturity can also enable SMEs to be increasingly equipped with higher tools, like XDR, SOAR, or automated incident response systems. Basic cyber hygiene, such as strong logging, multi-factor authentication, patch management, habitual backup, and role-based access control are still necessary. The most efficient tools based on AI are those developed on the basis of the mentioned foundational controls.

The vendors are to create SME-centric offers that focus on simplified onboarding, clear prices, and ready to use models, automatic remediation, and explain ability functionality. Adoption of AI can be encouraged by policymakers via financial incentives, common cybersecurity infrastructure, awareness programs focused on SMEs, and improved regulatory directions on AI regulation, data protection and incident reporting. Such advancements also justify the necessity of systematic frameworks of the feasibility assessment, including SME-AICF, especially in the regions where the risk-based AI regulation is established. [65-67].

6.1. Research Gaps and Future Research Directions

The presented evidence of this review shows that there are a few unresolved gaps in the research that restrict the practical capabilities of AI-based cybersecurity measures in small and medium-sized businesses. One of the key blank areas is the prevalent use of benchmark datasets like CICIDS2017, UNSW-NB15, NSL-KDD, and EMBER[48, 88, 101]. Though these datasets can be used to experiment with controlled and reproducible networks, they fail to reflect the noisy, incomplete and heterogeneous telemetry of SME settings. Consequently, the accuracy measures that are reported are mostly ideal lab conditions but not operations. The other gap is the apparent lack of real-world and longitudinal assessments. Most researches analyze AI models at one time and in controlled experimental environments[102]. Little is known regarding the performance of these models when dealing with the issue of concept drift, an evolving attack vectors, or changing infrastructure in SMEs. More generally, federated learning even though conceptually appealing to privacy preserving threat detection, is not empirically justified using multi-organizational SME applications, governance structures, or cost-benefit comparisons. There is also the under-exploration of economic feasibility.

Few studies will seek to model the financial impact of AI adoption and none of them includes specific analyses, either the total cost of ownership, continued cloud telemetry costs, or staffing needs. Moreover, the sociotechnical issues, including operator trust, alert fatigue, decision-making in uncertainty, and the explain ability role, are not well addressed, despite the fact that SMEs do not have cybersecurity professionals. Available literature also gives little focus on adversarial robustness and the situation regarding the strength of AI models to prevent evasion or poisoning attacks on SME environments remains unclear. Lastly, there is a lack of standardized, SME-suited assessment systems, which prevents the comparability of the studies and limits the creation of relevant benchmarks.

To overcome these lacuna, future studies should be more context-sensitive and operationally-focused taking into consideration the peculiarities of the SMEs. One of these priorities is the creation of datasets that reflect the true SME telemetry, reflect the noise in the real world, partial logging processes, and other device

environments. The necessity of longitudinal and field-based assessments that determine the dynamics of AI models in time, their changing accuracy in the case of concept drift, and the response of SMEs to such systems in their daily activities is equally relevant. The economic viability must be the key to the next-generation employment. Cost modelling needs to be detailed in system design and evaluation and needs to quantify the overall cost of ownership, cloud processing charges, resource usage and administrative overhead.

Further exploration is also necessary in sociotechnical aspects (how the non-expert staff perceives the AI-generated alerts, the degree to which explain ability affects trust and adoption, and how user behavior affects the performance of the system). Sector and region specific changes are also highly needed because SMEs in various industries and regions are exposed to different threat environments, infrastructure challenges, and regulatory barriers. Customized models to suit bandwidth constrained environments, legacy intensive systems or IoT intensive industries could go a long way to enhance applicability. Lastly, the research must improve the future by improving governance, interoperability, and collaborative security models, such as federated learning, secure threat intelligence sharing, and alignment with new AI regulations, to create solutions that work and are operationally sustainable among SMEs.

This review is limited in a number of ways. First, there can be publication bias, whereby research that proves the strength of AI has high chances of publication compared to those that show no results or unfavorable results. Second, numerous studies that involve benchmark data are not entirely representative of noisy, incomplete, and heterogeneous SME environments and thus have lower ecological validity. Third, triangulated documentation and analyst reports were used as the basis of commercial analysis, but there were not necessarily independent real-world validation data, which could also contribute to an inevitable vendor bias. Fourth, SMEs are extremely heterogeneous in terms of industry, location, exposure to the regulations, and maturity with regard to digitalization, which implies that generalizability is limited. Lastly, the SME-AICF framework is an evidence-based conceptual framework though it is based on a systematic derivation. Before it can be regarded as a successful decision instrument, it needs to be tested empirically, deployed in the field by SMEs, longitudinally tested, and validated out by experts.

7. Conclusion

The researchers investigated the potential of AI-assisted cybersecurity in small and medium enterprises and analyzed 50 peer-reviewed academic studies and independently verified commercially offered AI-enhanced security systems, which resulted in the synthesis of the feasibility of AI-assisted cybersecurity in small and medium enterprises. It has been shown that advanced AI methods, especially deep learning and anomaly-based models can perform remarkably well in detecting data in controlled settings, but in practice cannot be applied in SMEs because of data quality and their computational needs, available skills, and integration complexity. Managed Detection and Response (MDR), AI-enhanced email security, and commercially operated and cloud-based solutions, especially EDR/XDR, represent the most viable near-term adoption pathway, as they offload operational load but retain a high level of protection. The paper can provide an evidence-based conceptual feasibility framework (SME-AICF), which organizes the feasibility assessment in the technical, economic, operational, legal, and market dimensions. The framework is presented as a theoretical possible reality map instead of a proven decision-making tool and can offer systematic directions to SMEs, policymakers, and even vendors and create a baseline of subsequent empirical validation. The anticipated future research directions are the formulation of datasets representing SMEs, longitudinal studies on real-life deployment, enhanced economic and total cost of ownership modelling and a more in-depth study of sociotechnical and governance aspects. The above gaps need to be addressed in order to close the recurring gap between technical AI innovation and its realistic and sustainable application in the SME context of cybersecurity.

References

1. Co-operation, O.f.E. and Development, OECD SME and Entrepreneurship Outlook 2023. 2023, OECD Publishing.
2. Wallang, M., M.D.K. Shariffuddin, and M. Mokhtar, Cyber security in Small and Medium Enterprises (SMEs). Journal of Governance and Development, 2022. 18(1): p. 75–87.
3. Rawindaran, N., A. Jayal, and E. Prakash, Machine learning cybersecurity adoption in small and medium enterprises in developed countries. Computers, 2021. 10(11): p. 150.
4. Dighriri, M.A., H.H. Alzahrani, and A.M. Almazroi, Exploring determinants of information security systems adoption in Saudi Arabian SMEs: an integrated multitheoretical model. Information, 2025. 16(2): p. 85.
5. Rizvi, M.H. and Z. Rahman, Enhancing cybersecurity programs in small and medium enterprises (SMEs): a systematic literature review. International Journal of Advanced Computer Science and Applications, 2025. 16(9): p. 1–10.
6. Wijayasinghe, D., M. Karunaratne, and H. Jayamaha, Cybersecurity guide for small and medium enterprises (SMEs): a practical framework. Journal of Information Security, 2024. 15(3): p. 101–143.
7. Clark, N. and K. Mujeye, A Critical Analysis of SME Cybersecurity Policies and Practices in Central Illinois, in Proceedings of the 9th International Conference on Information Systems and Management (ICISM 2025). 2025. p. 210–221.
8. Adriko, R. and J.R.C. Nurse, Cybersecurity, cyber insurance, and small-to-medium-sized enterprises: a systematic review. Information & Computer Security, 2024. 32(5): p. 691–715.
9. Al-Yahya, S.N. and F. Alqahtani, The economic impact of cybersecurity breaches and frauds on SMEs: an empirical analysis. Review of Business and Economics, 2025. 60(2): p. 45–68.
10. Venkatesh, V., et al., User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 2003.
11. Verizon, 2024 Data Breach Investigations Report (DBIR). 2024, Verizon Enterprise Solutions.
12. Almeida, F., I. Carvalho, and F. Cruz, Structure and Challenges of a Security Policy on Small and Medium Enterprises. KSII Transactions on Internet & Information Systems, 2018. 12(2).
13. Kasali, K., et al., AI-DRIVEN STRATEGIES OF MITIGATING CYBERSECURITY THREATS IN US SMALL AND MEDIUM ENTERPRISES (SMES). International Journal of Computer Science and Information Technology, 2025. 17: p. 49–62.
14. Sarker, I.H., et al., Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 2020. 7(1): p. 41.
15. Accenture, How cybersecurity boosts enterprise reinvention to drive business resilience: State of Cybersecurity Resilience 2023. 2023, Accenture.
16. Apruzzese, G., et al. On the effectiveness of machine and deep learning for cyber security. in 2018 10th international conference on cyber Conflict (CyCon). 2018. IEEE.
17. Commission, E., User Guide to the SME Definition. 2020, Publications Office of the European Union: Luxembourg.
18. Administration, U.S.S.B., Table of Small Business Size Standards. 2023, SBA Office of Size Standards: USA.
19. Cybersecurity, et al., Supply Chain Compromise: Threat Actors Targeting Managed Service Providers (MSPs) and Their Customers (AA21-131A). 2021, U.S. Department of Homeland Security: Washington, D.C.
20. Almeida, F., I. Carvalho, and F. Cruz, Structure and challenges of a security policy on small and medium enterprises. KSII Transactions on Internet and Information Systems, 2022. 16(1): p. 1–19.
21. Benjamin, L.B., A.E. Adegbola, and P. Amajuoyi, Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 2024. 19(2): p. 84–96.
22. Rawindaran, N., et al., Detection and Minimization of Malware by Implementing AI in SMEs, in Malware-Detection and Defense. 2022, IntechOpen.
23. Commission, E., Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act). 2021, European Commission.
24. Ahmad, Z., et al., Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 2021. 32(1): p. e4150.
25. Investigation, F.B.o., Internet Crime Report 2024. 2024, Federal Bureau of Investigation, Internet Crime Complaint Center (IC3).

26. Proofpoint, 2024 State of the Phish: Risky actions, real-world threats and user resilience in an age of human-centric cybersecurity. 2024, Proofpoint, Inc.
27. Sophos, The State of Ransomware in the U.S. 2024. 2024, Sophos Ltd.
28. The State of Ransomware in the U.S.: Report and Statistics 2024. 2024; Available from: https://www.********/en/blog/wp-content/uploads/2025/01/blog-fb-the-state-of-ransomware-in-the-us-report-and-statistics-2024.
29. IBM Security, M., Cost of a data breach report 2021. 2023.
30. Sommer, R. and V. Paxson, Outside the Closed World: On Using Machine Learning for Network Intrusion Detection, in 2010 IEEE Symposium on Security and Privacy (SP). 2010, IEEE. p. 305–316.
31. Buczak, A.L. and E. Guven, A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 2016. 18(2): p. 1153–1176.
32. Sarker, I.H., et al., Cybersecurity Data Science: An Overview from Machine Learning Perspective. Journal of Big Data, 2020. 7(1): p. 1–29.
33. Xin, Y., et al., Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access, 2018. 6: p. 35365–35381.
34. Vinayakumar, R., et al., Deep Learning Approach for Intelligent Intrusion Detection System. IEEE Access, 2019. 7: p. 41525–41550.
35. Gu, J., et al., Recent Advances in Convolutional Neural Networks. Pattern Recognition, 2018. 77: p. 354–377.
36. Mothukuri, V., et al., A Survey on Security and Privacy of Federated Learning. Future Generation Computer Systems, 2021. 115: p. 619–640.
37. Yang, Q., et al., Federated Machine Learning: Concept and Applications. ACM Transactions on Intelligent Systems and Technology, 2019. 10(2): p. 1–19.
38. Li, T., et al., Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 2020. 37(3): p. 50–60.
39. Rahmati, M. and N. Rahmati, Adaptive Federated Edge Intelligence for Real-Time Cyberthreat Detection in Resource-Constrained IoT Environments: A Lightweight Deep Learning Approach. Journal of Computer Virology and Hacking Techniques, 2025. 21(1): p. 35.
40. Srivastava, G., et al., XAI for cybersecurity: state of the art, challenges, open issues and future directions. arXiv preprint arXiv:2206.03585, 2022.
41. Zhang, Z., et al., Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEe Access, 2022. 10: p. 93104–93139.
42. Benjamin, L.B., et al., Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 2024. 19(2): p. 134–153.
43. Ring, M., et al., A survey of network-based intrusion detection data sets. Computers & Security, 2019. 86: p. 147–167.
44. Rhode, M., P. Burnap, and K. Jones, Early-stage malware prediction using recurrent neural networks. computers & security, 2018. 77: p. 578–594.
45. Vasan, D., et al., IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. Computer Networks, 2020. 171: p. 107138.
46. Zhuang, F., et al., A comprehensive survey on transfer learning. Proceedings of the IEEE, 2020. 109(1): p. 43–76.
47. Apruzzese, G., P. Laskov, and J. Schneider, SoK: Pragmatic assessment of machine learning for network intrusion detection, in 2023 IEEE European Symposium on Security and Privacy (EuroS&P). 2023, IEEE. p. 91–110.
48. Sharafaldin, I., A. Habibi Lashkari, and A.A. Ghorbani. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. in International Conference on Information Systems Security and Privacy. 2018.
49. Gopinath, M. and S.C. Sethuraman, A comprehensive survey on deep learning based malware detection techniques. Computer Science Review, 2023. 47: p. 100529.
50. Dhanabal, L. and S.P. Shantharajah, A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering, 2015. 4(6): p. 446–452.
51. Benavides-Astudillo, E., et al., A phishing-attack-detection model using natural language processing and deep learning. Applied Sciences, 2023. 13(9): p. 5275.

52. Alzu, S., F. Stahl, and M. Al-Khafajiy. Detect, Decide, Explain: An Intelligent Framework for Zero-Day Network Attack Detection. in International Conference on Innovative Techniques and Applications of Artificial Intelligence. 2025. Springer.
53. Gibert, D., C. Mateu, and J. Planes, The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications, 2020. 153: p. 102526.
54. Wang, X., et al., A Survey on Security of Large Language Models. ACM Computing Surveys, 2024.
55. Chen, C., et al., Trustworthy federated learning: privacy, security, and beyond. Knowledge and Information Systems, 2025. 67(3): p. 2321–2356.
56. Zhang, Y., X. Liu, and H. Wang, Federated learning for ransomware detection in distributed environments. IEEE Transactions on Information Forensics and Security, 2025. 20: p. 1234–1247.
57. Xin, Y., et al., Machine learning and deep learning methods for cybersecurity. Ieee access, 2018. 6: p. 35365–35381.
58. He, K., D.D. Kim, and M.R. Asghar, Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2023. 25(1): p. 538–566.
59. Tobiyama, S., et al. Malware detection with deep neural network using process behavior. in 2016 IEEE 40th annual computer software and applications conference (COMPSAC). 2016. IEEE.
60. Purnamadewi, Y.A. and A.A. Zahra, Phishing email detection using FastText and convolutional neural network. Journal of Information Systems Engineering and Business Intelligence, 2024. 10(1): p. 45–56.
61. Sun, Y., N. Chong, and H. Ochiai. Federated phish bowl: LSTM-based decentralized phishing email detection. in 2022 IEEE international conference on systems, man, and cybernetics (SMC). 2022. IEEE.
62. 62. Research, F., The Forrester Wave: Endpoint Detection and Response Providers, Q2 2024. 2024, Forrester Research, Inc.
63. 63. Research, G., Market Guide for Managed Detection and Response Services. 2024, Gartner, Inc.
64. Europe, H., The EU Framework Programme for Research and Innovation. 2021.
65. Hofmann, H.C.H., Constitutionalising Technology: EU Administrative Governance in the Digital Age. 2024, Oxford: Oxford University Press.
66. Hulok, Ł., The EU model of AI governance: regulating artificial intelligence through law and policy. ERA Forum, 2025.
67. Mahmutović, A., The EU AI Act: a proactive framework for comprehensive AI regulation. International Journal of Law and Information Technology, 2025.
68. Page, M.J., et al., The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 2021. 372: p. n71.
69. Khando, K., et al., Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 2021. 106: p. 102267.
70. Nadella, G.S., et al., Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. World Journal of Advanced Research and Reviews, 2024. 22(1): p. 1190–1197.
71. Kshetri, N., Cybersecurity and development: Threat to small and medium enterprises in developing economies. Information Technology for Development, 2021. 27(4): p. 697–720.
72. Abdulqader, S., CAFED-Net: Cross-Adaptive Federated Learning with Dy-namic Adversarial Defense for Real-Time Privacy-Preserving and Threat Detection in Distributed IoT Ecosystems. Journal of Soft Computing and Data Mining, 2025. 6(1): p. 58–68.
73. Timofte, R., F. Pop, and C. Negru, Federated learning for intrusion and malware detection in resource-constrained IoT environments. IEEE Access, 2025. 13: p. 1234–1248.
74. Andresini, G., et al., INSOMNIA: Towards concept-drift robustness in network intrusion detection, in Proceedings of the 14th ACM Workshop on Artificial Intelligence and Security (AISec '21). 2021. p. 111–122.
75. Camarda, L., Managing concept drift in online intrusion detection systems with active learning, in Proceedings of the 6th International Workshop on Machine Learning for Cybersecurity (ML4Cyber 2025). 2025. p. 35–46.
76. Chu, R., et al., Intrusion detection in the IoT data streams using concept drift localization. AIMS Mathematics, 2024. 9(1): p. 1535–1561.

77. Shyaa, T., H. Al-Shargabi, and R.N. Al-Awadi, Evolving cybersecurity frontiers: a comprehensive survey on concept drift, feature dynamics, and adaptive learning in intrusion detection. Engineering Applications of Artificial Intelligence, 2025. 133.
78. Abdulqader, D.M., CAFED-Net: Cross-adaptive federated learning for IoT threat detection with improved robustness and efficiency. IEEE Internet of Things Journal, 2025. 12(3): p. 2345–2358.
79. Mellen, A. Announcing The Forrester Wave™: Extended Detection And Response Platforms, Q2 2024. 2024 2024–06–04; Available from: https://www.forrester.com/blogs/announcing-the-forrester-wave-extended-detection-and-response-platforms-q2-2024/.
80. ATT and M. CK, ATT&CK Matrix for Enterprise, MITRE ATT&CK. 2023.
81. Engenuity, M., ATT&CK Evaluations – Managed Services: menuPass & ALPHV/BlackCat. 2024, MITRE Engenuity.
82. Labs, S., Enterprise Endpoint Security — Independent Test Reports. 2024, SE Labs.
83. AV-Comparatives, Business Security Test – Enterprise & SMB Solutions. 2024, AV-Comparatives.
84. AV-Comparatives, Endpoint Prevention and Response (EPR) Test – Enterprise 2024 Results Report. 2024, AV-Comparatives.
85. CrowdStrike. MITRE ATT&CK Evaluations Performance Summary. 2024; Available from: https://www.crowdstrike.com.
86. Engenuity, M., ATT&CK Evaluations – Enterprise 2024. 2024, MITRE Engenuity.
87. Engenuity, M., ATT&CK Evaluations – Enterprise 2025. 2025, MITRE Engenuity.
88. Engenuity, M., ATT&CK Evaluations – Public Dataset and Results Portal. 2025, MITRE Engenuity.
89. Microsoft. Microsoft Defender for Endpoint: ATT&CK Evaluation Results. 2024; Available from: https://learn.microsoft.com.
90. Networks, P.A. Cortex XDR MITRE ATT&CK Evaluation Summary. 2024; Available from: https://www.paloaltonetworks.com.
91. Mirolyubov, E. and M. Taggett, Magic Quadrant for Endpoint Protection Platforms. 2023, Gartner, Inc.
92. Limited, B., Cylance endpoint security: Technical overview and summary of independently reported test results. 2023, BlackBerry Limited: Waterloo, Canada.
93. Engenuity, M., ATT&CK® evaluations: Managed security service providers (MSSP) – menuPass and ALPHV/BlackCat scenarios. 2024, MITRE Corporation: McLean, VA, USA.
94. Ginsburg, J., Evaluating machine learning performance in EDR and XDR systems against common cyber threats. 2025.
95. Pissanidis, N., E. Gelenbe, and P. Trimintzios, Integrating AI/ML in cybersecurity: an analysis of Open XDR technology and its application in network defence. Computer Standards & Interfaces, 2024. 93.
96. SecureIQLab, XDR CyberRisk Validation Methodology: Independent Evaluation Framework for Extended Detection and Response. 2023.
97. Opara-Martins, J., R. Sahandi, and F. Tian, Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. Journal of Cloud Computing, 2016. 5(1): p. 1–18.
98. Al Lail, M., A. Garcia, and S. Olivo, Machine learning for network intrusion detection—a comparative study. Future Internet, 2023. 15(7): p. 243.
99. Mell, P. and T. Grance, The NIST definition of cloud computing. 2011.
100. Mohammed, S.S., A Decentralized Approach to Privacy-Preserving Data Analysis using Federated Learning. Kairouz, P., McMahan, HB, Avent, B., Bellet, A., Bennis, M., Bhagoji, AN, & Ramage, D.(2021). Advances and open problems in federated learning. Foundations and Trends® in Machine Learning, 2025. 14(1-2): p. 1–210.
101. Iftikhar, N., et al., Intrusion detection in NSL-KDD dataset using hybrid self-organizing map model. Computer Modeling in Engineering & Sciences, 2025. 143(1): p. 639.
102. Jordaney, R., et al. Transcend: Detecting Concept Drift in Malware Classification Models. in USENIX Security Symposium. 2017.
103. Kant, D. and A. Johannsen, Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). Electronic Imaging, 2022. 34: p. 1–8.
104. Odesanya, M.A., Transforming small business landscapes: Artificial Intelligence's evolutionary leap forward. 2022.

105. Adelusi, B.S., F.U. Ojika, and A.C. Uzoka, Advances in Cybersecurity Strategy and Cloud Infrastructure Protection for SMEs in Emerging Markets. 2022.
106. Yusuf, S.O., et al., Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. World Journal of Advanced Research and Reviews, 2024. 23(3): p. 2138–2147.
107. BLESSING, A.-G., et al., Machine learning-driven cybersecurity for social media data protection in entrepreneurial ventures. INTERNATIONAL JOURNAL, 2024. 8(2): p. 175–184.
108. Varma, A.J., et al., A roadmap for SMEs to adopt an AI based cyber threat intelligence, in Studies in Computational Intelligence. 2023. p. 1903–1926.
109. Alhosban, A. and S. Krishnakumar, Cloud Vendor Lock-In Prediction Framework (CVL). Mathematics, 2024. 12(3).
110. Metin, B., F.G. Özhan, and M. Wynn, Digitalisation and cybersecurity: Towards an operational framework. Electronics, 2024. 13(21): p. 4226.
111. Mlakar, I., et al., A cost-effective security framework to protect micro enterprises: Palantir e-commerce use case. 2021.
112. Kapoor, P., Cloud security challenges in Indian SMEs: A machine learning approach. International Journal for Research Publication and Seminar, 2023. 14(5): p. 259–264.
113. Ilca, L.F., O.P. Lucian, and T. Balan, Enhancing cyber-resilience for small and medium-sized organizations with prescriptive malware analysis, detection and response. Sensors, 2023. 23(15).