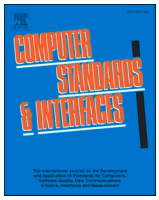
Computer Standards & Interfaces 97 (2026) 104099

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi



Integrating IoT security practices into a risk-based framework for small and medium enterprises (SMEs)

Samer Aoudi *, Hussain Al-Aqrabi

Department of Computer Information Science, Higher Colleges of Technology, Sharjah, UAE

ARTICLE INFO

Keywords:
IoT security
Risk assessment
SME cybersecurity
Threat modeling
STRIDE
CVSS
Bayesian inference

ABSTRACT

The growing integration of Internet of Things (IoT) technologies within Small and Medium Enterprises (SMEs) has introduced new operational efficiencies while simultaneously expanding the cybersecurity threat landscape. However, most SMEs lack the resources, technical expertise, and institutional maturity required to adopt existing security frameworks, which are often designed with large enterprises in mind. This paper proposes a risk-based framework specifically developed to help SMEs identify, assess, and mitigate IoT-related security risks in a structured and scalable manner. The framework integrates key components such as asset classification, STRIDE-based threat modeling, CVSS-driven vulnerability assessment, and dynamic risk prioritization through Bayesian inference. Emphasis is placed on cost-effective mitigation strategies that are feasible within SME resource constraints and aligned with regulatory requirements. The framework was validated through a real-world case study involving a digitally enabled retail SME. Results demonstrate tangible improvements in vulnerability management, security control implementation, and organizational readiness. Additionally, qualitative feedback from stakeholders highlights the framework's usability, adaptability, and minimal disruption to operations. This research bridges a critical gap in the current literature by contextualizing established cybersecurity methodologies for the SME sector and providing a practical toolset for managing IoT risks. The proposed framework offers SMEs a viable path toward improving cybersecurity resilience in increasingly connected business environments.

1. Introduction

The Internet of Things (IoT) is reshaping the digital landscape, driving innovation across industries by interconnecting billions of devices. From smart sensors and industrial controllers to home automation systems and connected medical equipment, IoT enables continuous data exchange, automation, and real-time analytics. Its widespread integration is transforming sectors such as healthcare, manufacturing, transportation, and retail. Projections indicate that IoT device adoption will exceed 39.9 billion units by 2033, outpacing traditional computing platforms such as laptops and smartphones [1].

In the business domain, IoT technologies are instrumental in boosting operational efficiency, reducing costs, and enabling agile service models. For instance, in logistics, IoT-enabled tracking systems improve supply chain visibility and inventory accuracy, minimizing losses and enhancing responsiveness [2]. In healthcare, connected medical devices allow for real-time patient monitoring and timely clinical interventions, elevating care standards [3]. SMEs, in particular, are increasingly adopting IoT solutions to streamline operations and remain competitive. However, this rapid adoption has introduced heightened cybersecurity concerns. SMEs often lack dedicated cybersecurity personnel and operate with limited financial and technical resources, leaving them especially vulnerable to IoT-specific threats and system misconfigurations.

The growth trajectory of IoT is further accelerated by advancements in artificial intelligence (AI) [4], edge computing [5–7], and 5 G networks [8]. AI-integrated IoT systems enhance threat detection and support autonomous decision-making. Edge computing enables low-latency data processing at the device level, and 5 G introduces ultra-high bandwidth and reliable communication, powering real-time industrial and smart city applications. Together, these technologies signal an era of unprecedented connectivity, in which SMEs must navigate both operational transformation and an increasingly complex cybersecurity threat landscape.

1.1. Problem statement

While the Internet of Things (IoT) offers significant operational advantages, it also exposes organizations, particularly SMEs, to

* Corresponding author.
E-mail address: samer_aoudi@hotmail.com (S. Aoudi).

https://doi.org/10.1016/j.csi.2025.104099
Received 10 June 2025; Received in revised form 3 November 2025; Accepted 21 November 2025
Available online 26 November 2025

increasingly complex and evolving cyber threats [9–11]. The diverse and heterogeneous nature of IoT devices introduces system-level challenges such as default credentials, outdated firmware, insecure communication protocols, and insufficient access controls [12–15]. These technical shortcomings, combined with limited in-house expertise and constrained budgets, hinder SMEs from effectively securing their IoT infrastructures [16]. Moreover, compliance with emerging regulations such as the European Union's General Data Protection Regulation (GDPR) and the UAE's Federal Personal Data Protection Law (PDPL) further complicates security governance for SMEs.

Several well-known cybersecurity frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [17], NIST SP 800–183 [18], ISO/IEC 27005 [19], European Union Agency for Cybersecurity (ENISA) IoT security guidelines [20,21], and the Open Web Application Security Project (OWASP) IoT Project [22], offer valuable guidance for addressing IoT risks. However, these frameworks are often too complex, resource-intensive, or abstract for SMEs to adopt without significant adaptation. Many lack actionable, SME-friendly methodologies or assume levels of organizational maturity not representative of typical small businesses [23,24].

A critical gap exists in the cybersecurity literature: the absence of a risk-based, scalable, and accessible framework that effectively addresses the specific limitations and operational realities of SMEs operating IoT environments. While numerous frameworks exist, most are designed for large enterprises and are ill-suited for small businesses with constrained resources. This study focuses specifically on SMEs that deploy IoT-enabled infrastructure, aiming to support them in managing the growing complexity of IoT-related cybersecurity risks through tailored, resource-aware risk assessment practices.

1.2. Research objectives

This research aims to develop a structured, risk-based framework tailored to the cybersecurity needs of Small and Medium Enterprises (SMEs) operating Internet of Things (IoT) environments. The proposed approach is designed to help SMEs systematically identify, assess, and mitigate IoT-related threats while accounting for their limited technical expertise and financial constraints. Rather than introducing entirely new tools, the framework repurposes and integrates well-established methodologies into a coherent, resource-aware process that SMEs can realistically adopt and sustain.

Rather than introducing novel technical tools, the framework repurposes and streamlines established methods to create a workflow accessible to SMEs with minimal cybersecurity maturity. In doing so, it contributes to the IoT security literature by addressing persistent gaps in the applicability, scalability, and adaptability of existing frameworks for SMEs. This study advances the field in three key dimensions.

First, it emphasizes SME-centricity by grounding the proposed framework in the operational realities of a real-world case study. Unlike enterprise-focused research, this study captures the practical limitations SMEs face, including limited staffing, budget constraints, and fragmented infrastructure. Second, the framework offers a multi-layered integration of essential cybersecurity practices. It links asset classification with STRIDE-based threat modeling, CVSS-informed vulnerability assessment, and Bayesian-driven dynamic risk updates into a coherent, stepwise model. While these components are well-documented individually, their consolidation for SME contexts is novel. Third, the inclusion of Bayesian post-mitigation risk reassessment enables continuous recalibration of threat likelihoods, a feature often absent from SME-targeted frameworks.

This contribution bridges the gap between complex enterprise models and the lightweight, accessible solutions SMEs need, while extending the utility of standards such as ENISA's guidelines [21] and ISO/IEC 27005 [19] by contextualizing them for low-resource environments. Moreover, the value of this research lies in its practical orientation: the proposed framework was tested in a real-world SME, yielding tangible improvements in vulnerability reduction, risk mitigation efficiency, and staff security awareness. In doing so, this study provides a pragmatic and empirically validated model that bridges the gap between complex security theory and implementable practice for SMEs [23,24].

The remainder of this paper is structured as follows. Section 2 reviews existing literature on IoT security and related frameworks, with a focus on challenges specific to SMEs. Section 3 outlines the research methodology, including the case study design and evaluation approach. Section 4 presents the proposed five-step risk-based framework. Section 5 applies the framework to a real-world SME and reports both quantitative results and qualitative feedback. Section 6 discusses the framework's effectiveness, compares it with existing standards, addresses regulatory compliance, and reflects on cost and SME applicability. Section 7 concludes the paper and outlines directions for future work.

2. Literature review

This section reviews the academic and industry literature related to IoT security, with a particular emphasis on the unique challenges faced by SMEs. It also evaluates existing cybersecurity frameworks and their limitations in SME contexts.

2.1. Foundations of IoT security challenges

The cybersecurity implications of IoT adoption have been widely discussed across academic and industry literature yet challenges specific to SMEs remain underexplored. This section reviews the foundational security concerns of IoT environments and critically examines existing frameworks and their limitations in SME contexts.

The rapid proliferation of Internet of Things (IoT) technologies has ushered in unprecedented levels of interconnectivity, automation, and operational efficiency across a wide range of sectors, including healthcare, manufacturing, logistics, and retail [3]. While this technological advancement offers substantial benefits, it also significantly enlarges the cybersecurity threat surface, introducing complex risks that are both systemic and persistent. As noted by Tawalbeh et al. [9], the decentralized architecture, device-level resource constraints, and protocol heterogeneity inherent in IoT environments collectively give rise to a multi-dimensional security landscape that defies traditional protection models. These concerns are amplified in 5G-enabled IoT deployments, which, as highlighted by Wazid et al. [8], are vulnerable to a combination of legacy threats and emerging attack vectors enabled by increased bandwidth and connectivity.

Fundamental to the cybersecurity discourse surrounding IoT is the difficulty of enforcing the foundational triad of information security: confidentiality, integrity, and availability (C.I.A). Prior research has shown that IoT ecosystems struggle to uphold these principles uniformly due to the diversity of hardware and software platforms and the often-limited computational capacity of devices [12,25]. Compounding this issue are persistent security misconfigurations, such as the widespread use of default credentials, outdated firmware, and unencrypted communication channels, vulnerabilities that remain common despite increased awareness and guidance from sources such as the OWASP IoT Project [22].

The evolution toward Industry 4.0, characterized by the convergence of IoT, cyber-physical systems, and autonomous control, has further accelerated IoT adoption across business domains [26]. However, this shift has also intensified security concerns, particularly for SMEs that lack the organizational maturity, infrastructure, and expertise required to manage these complex systems effectively. Empirical studies consistently emphasize the resulting security and privacy implications, including data leakage, unauthorized system access, and operational disruption [27]. These risks are especially pronounced in SME environments, where cybersecurity preparedness often lags behind technological adoption [28].

2.2. Existing IoT risk assessment frameworks

Multiple frameworks have attempted to codify IoT security risk management, drawing from well-established standards such as ISO/IEC 27005 [19] and NIST's Cybersecurity Framework [18]. While these frameworks provide generic guidance for identifying, assessing, and mitigating risks, their practical applicability to SMEs with limited cybersecurity maturity remains questionable [24].

ENISA [20,21] provides IoT-specific guidance by recommending baseline security controls and governance practices for critical infrastructure. However, its approach tends to be prescriptive and often assumes high organizational maturity and resourcing. Similarly, the NIST SP 800–183 report [17] conceptualizes the "Network of Things," offering terminologies and abstraction layers for risk management but stops short of operationalizing a dynamic risk response model.

Zheng et al. [29] and Queiroz et al. [30], have explored digital transformation frameworks for supply chains and smart manufacturing, respectively, but their emphasis is primarily on strategic alignment and technological enablement rather than actionable risk quantification.

This subsection reviews key frameworks that inform our approach:

- NIST Cybersecurity Framework (CSF) and NIST Special Publication 800–183: The NIST CSF is one of the most widely adopted frameworks for managing cybersecurity risks. It provides a flexible and scalable approach organized into five core functions: Identify, Protect, Detect, Respond, and Recover [17]. While the NIST CSF is comprehensive, its implementation often requires significant resources and expertise, which may be beyond the capacity of many SMEs [23].
- ISO/IEC 27005: ISO/IEC 27005 provides guidelines for information security risk management, emphasizing the importance of risk assessment and treatment [19]. Although it is highly detailed, its complexity and resource-intensive nature make it less accessible for SMEs, particularly those with limited cybersecurity expertise [24].
- OWASP IoT Project: The Open Web Application Security Project (OWASP) IoT Project focuses on identifying and mitigating common vulnerabilities in IoT devices and applications [15,22]. While it offers practical guidance, it lacks a structured risk assessment process, making it difficult for SMEs to prioritize and address risks systematically.
- ENISA IoT Security Guidelines: The European Union Agency for Cybersecurity (ENISA) has developed guidelines for securing IoT ecosystems, covering areas such as device hardening, secure communication, and lifecycle management [21]. However, these guidelines are often too generic and do not provide actionable steps for SMEs with limited technical capabilities.

2.3. Shortcomings in current approaches

Despite the availability of numerous frameworks and guidelines designed to enhance the security of IoT ecosystems [31], a persistent gap remains in their applicability to SMEs. Many of these frameworks were developed with large organizations in mind, requiring considerable technical expertise, financial investment, and operational maturity. As Chidukwani et al. [23] emphasize, most SMEs lack the resources necessary to implement comprehensive cybersecurity programs, making the adoption of existing frameworks impractical without significant adaptation. This challenge is compounded by the complexity and prescriptive nature of these models, which often overwhelm smaller organizations seeking feasible entry points into IoT security.

In addition to resource constraints, SMEs face methodological limitations in the tools commonly used for risk assessment. Czekster et al. [32] point to the rigidity of static risk models, which struggle to accommodate evolving threat landscapes or adjust post-control risk levels based on new evidence. Traditional risk matrices, while widely adopted for their simplicity, have drawn criticism for their reliance on subjective assessments and oversimplified likelihood-impact scoring systems [33]. These models frequently fail to incorporate real-time threat intelligence or context-aware decision-making, which are critical for dynamic and heterogeneous IoT environments.

Emerging approaches involving artificial intelligence (AI) and machine learning (ML) show promise in areas such as anomaly detection and automated vulnerability discovery [4,11,34]. However, such solutions are often opaque, computationally intensive, and dependent on advanced technical skills, barriers that place them out of reach for many SMEs. Research by Kong et al. [35] and Aoudi et al. [36] has advanced intelligent IoT frameworks, yet these too generally assume the availability of enterprise-grade infrastructure and cybersecurity expertise.

Moreover, the fragmented nature of IoT security standards further complicates adoption. Brass et al. [37] and Webb & Hume [38] highlight the lack of harmonized, SME-centric guidance, which results in implementation ambiguities and regulatory compliance challenges. To contextualize these issues, Table 1 summarizes the major limitations of current frameworks when applied to SMEs, including their complexity, scalability issues, and lack of actionable guidance tailored to smaller organizational contexts.

The framework proposed in this study seeks to overcome these challenges by distilling best practices from established standards such as NIST and ISO, and restructuring them into a pragmatic, lightweight, and accessible model. In doing so, it provides SMEs with a pathway to improved IoT security posture that aligns with their operational realities and capacity constraints.

2.4. Theoretical foundation

The formulation of a risk-based framework for securing Internet of Things (IoT) environments in SMEs is anchored in three foundational cybersecurity concepts: risk assessment, threat modeling, and vulnerability analysis. Together, these pillars provide the conceptual structure necessary for systematically identifying, evaluating, and mitigating the unique security challenges that arise in SME-operated IoT ecosystems. This section articulates the theoretical basis for the proposed framework, establishing its relevance and rigor in addressing real-world SME constraints.

Risk assessment is a critical process that enables organizations to identify, analyze, and evaluate risks to their digital assets, operations, and stakeholders [19]. Within the IoT domain, risk assessment facilitates the mapping of potential security threats to specific devices and services, supporting informed decision-making about risk mitigation and resource allocation. The NIST Cybersecurity Framework [18] highlights risk assessment as a central component of a proactive cybersecurity strategy. For SMEs, whose resources are often severely constrained, a well-structured risk assessment process becomes indispensable for prioritizing security efforts and ensuring that the most pressing

Table 1
Gaps in Existing Frameworks for SMEs.

Gap	Description
Resource Intensity	Frameworks such as NIST CSF and ISO/IEC 27,005 require significant financial and technical resources, which are often unavailable to SMEs [24,19].
Complexity	The technical complexity of ISO/IEC 27,005 and related standards can be overwhelming for SMEs lacking dedicated cybersecurity teams [23,24].
Lack of IoT-Specific Focus	Frameworks like the OWASP IoT Project address IoT vulnerabilities but do not integrate end-to-end risk assessment and mitigation [15,39].
Scalability Issues	Many existing frameworks assume organizational maturity that SMEs typically do not possess, hindering their applicability [21,24].
Limited Practical Guidance	Most frameworks offer general recommendations but lack detailed, step-by-step guidance tailored to SME operational contexts [23,32,33].

vulnerabilities are addressed efficiently.

Threat modeling offers a complementary lens by systematically identifying potential threats based on a system's architecture, interfaces, and usage patterns [40]. Among the most recognized methodologies are STRIDE [41] and PASTA [42]. STRIDE categorizes threats into six archetypes, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, enabling structured analysis of attack surfaces. In contrast, PASTA adopts a business-aligned, process-driven perspective, aiming to connect technical threats with organizational impact. Both methodologies provide a rigorous basis for uncovering and preemptively addressing IoT-specific threats, including unauthorized access, device manipulation, and data exfiltration.

Vulnerability analysis completes the triad by identifying exploitable weaknesses across the IoT stack from hardware and firmware to communication protocols and cloud services [43]. Given the diversity and scale of IoT deployments, SMEs often struggle to conduct vulnerability assessments systematically. Tools such as Nessus and OpenVAS offer automated scanning capabilities that facilitate the identification and classification of vulnerabilities, often using metrics like CVSS scores to guide remediation priorities [44]. Nevertheless, the effective use of these tools still requires a framework that contextualizes findings within the operational realities of SMEs.

The integration of these three theoretical domains, risk assessment, threat modeling, and vulnerability analysis, forms the analytical core of the proposed framework. Their synergy enables a comprehensive, end-to-end approach that is both methodologically rigorous and practically adaptable. For instance, asset classification, an essential element of risk assessment, provides the input for targeted threat modeling, which, in turn, informs vulnerability scanning strategies. This layered methodology supports SMEs in navigating complex IoT security landscapes with limited expertise and resources, offering a structured yet flexible model for scalable, cost-effective cybersecurity risk management.

2.5. Probabilistic and Bayesian approaches

The incorporation of probabilistic reasoning into cybersecurity decision-making has gained traction in recent years, particularly in the context of dynamic risk estimation and adaptive threat modeling. Among these approaches, Bayesian inference stands out for its ability to systematically update risk assessments based on new evidence, offering a mathematically grounded mechanism for recalibrating threat likelihoods over time [45]. Despite its demonstrated value in broader cybersecurity contexts, the application of Bayesian methods within IoT-specific risk frameworks remains underexplored, particularly in environments characterized by constrained resources and operational variability, such as SMEs.

Existing literature acknowledges the need for dynamic models capable of responding to the fluidity of IoT threat landscapes. Czekster et al. [32] advocate for adaptive risk models but fall short of articulating concrete implementation pathways that are feasible for SMEs. Similarly, Lee [46] underscores the promise of probabilistic techniques in IoT cybersecurity but highlights their limited uptake in practice, citing challenges such as computational overhead, model complexity, and the lack of accessible tooling to support real-time updates.

A critical shortfall in current frameworks is the absence of structured post-control risk reassessment. Once security controls, such as patch deployment or network segmentation, are implemented, most models fail to revise the underlying threat likelihoods accordingly. This omission can lead to persistent overestimation or underestimation of risk, resulting in inefficient allocation of limited security resources. ENISA [21] and empirical investigations such as Younis et al. [2] reinforce the importance of continuous reassessment to maintain alignment between perceived and actual risk postures.

Bayesian models offer a theoretically robust solution to this problem by enabling the integration of prior risk estimates with real-time evidence (e.g., vulnerability scan results, threat intelligence, or behavioral anomalies). This capacity for ongoing refinement makes Bayesian inference especially relevant in IoT ecosystems, where device configurations, exposure profiles, and threat landscapes are in constant flux. However, despite its suitability, Bayesian modeling remains largely absent in SME-oriented IoT security literature, underscoring a significant and timely gap that this study seeks to address through its proposed framework.

2.6. Integrating threat modeling and vulnerability scanning

Structured threat modeling and automated vulnerability assessment represent two foundational components of modern cybersecurity practices. Among threat modeling methodologies, the STRIDE framework has emerged as a widely accepted standard due to its systematic taxonomy, encompassing Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, and its alignment with system-level architectural analysis [40–42]. Despite its conceptual strengths, the operational deployment of STRIDE remains largely limited to organizations with mature secure development lifecycles, rendering it inaccessible to many SMEs that lack formalized security engineering practices.

Parallel to threat modeling, vulnerability scanning tools such as Nessus [43] and OpenVAS [44] provide powerful means for identifying known security flaws, misconfigurations, and software weaknesses. These tools generate Common Vulnerability Scoring System (CVSS)-based severity ratings, offering actionable insights for technical remediation. However, as Neshenko et al. [39] observe, these tools are frequently underutilized in SME contexts, not due to a lack of relevance, but because their outputs are rarely integrated into broader, dynamic risk evaluation frameworks. In SMEs, where security decisions must often be made with minimal human oversight and limited technical capacity, such disconnection diminishes the practical value of vulnerability data.

Case-specific studies by Fernandes et al. [14] and Cherian and Varma [13] illustrate isolated applications of threat analysis in environments such as smart homes and SDN-based IoT networks. While valuable in highlighting device-specific risks, these contributions remain narrowly focused and lack generalizable, system-level integration. More critically, they do not account for the potential of combining threat modeling and vulnerability data with probabilistic risk updating, such as Bayesian inference, to inform risk prioritization and post-control reassessment.

There remains, therefore, a notable gap in current literature and practice: the absence of a unified, SME-oriented framework that systematically links structured threat modeling (e.g., STRIDE), automated vulnerability scanning (e.g., Nessus, OpenVAS), and dynamic risk quantification. This study addresses that gap by proposing an integrated methodology that operationalizes these elements into a cohesive workflow tailored to the constraints and capabilities of SME environments.

3. Methodology

This section outlines the research design used to develop and validate the proposed framework. A sequential mixed-methods approach is adopted, combining theoretical integration with case-based evaluation.

3.1. Research design

The goal of this study is to develop and validate a cybersecurity risk management framework tailored to the needs and constraints of SMEs adopting IoT technologies. To ensure methodological rigor and practical relevance, a sequential mixed-methods design was adopted. This approach combines qualitative and quantitative data collection and analysis in a phased sequence, where the qualitative phase informs the quantitative one, an established design in applied security research [47, 48].

As illustrated in Fig. 1, the study follows a two-phase structure grounded in pragmatic philosophy and a deductive research strategy. The pragmatic stance prioritizes actionable, real-world solutions over rigid adherence to a single philosophical paradigm, allowing for methodological flexibility and contextual adaptation [49]. The deductive approach supports theory-driven framework development, followed by empirical validation.

Phase 1 centers on framework development, which forms the primary contribution of this study. Drawing from ISO/IEC 27005 [19], the NIST Cybersecurity Framework [17], and threat modeling strategies such as STRIDE and PASTA [41,42], this phase involved synthesizing best practices into a lightweight, five-step process appropriate for resource-constrained SMEs. This structured integration offers a novel contribution by operationalizing concepts such as CVSS-based vulnerability scoring and Bayesian risk updating within an accessible, implementation-ready format. The uniqueness of this integration lies in its combination of STRIDE-based threat modeling, CVSS-driven vulnerability scoring, and Bayesian updating into a cohesive workflow that enables SMEs to perform dynamic risk prioritization using lightweight, resource-aware processes.

Phase 2 focuses on framework validation, conducted through a single-case study in a real-world SME. This phase triangulates data from stakeholder interviews, vulnerability scans, and document analysis to assess the framework's usability, scalability, and effectiveness in improving cybersecurity posture. This design ensures that the framework is not only theoretically grounded but also contextually feasible and adaptable for small business environments.

Together, these phases are underpinned by a unified research design grounded in three foundational elements: pragmatism, deductive logic, and a sequential mixed-methods strategy. Pragmatism emphasizes practical, real-world outcomes over strict epistemological adherence, an essential stance when addressing the operational constraints of SMEs. The deductive approach enables theory-driven framework construction, which is then empirically validated through real-world application. Finally, the sequential mixed-methods strategy allows qualitative insights to shape the development of the framework in Phase 1, while quantitative evaluation in Phase 2 ensures measurable impact. These guiding principles shaped both the structure and execution of the study, as illustrated in Fig. 1.

3.1.1. *Phase 1: framework development*

The initial phase of this research focuses on the design of a structured, risk-based cybersecurity framework tailored to the specific constraints and operational realities of SMEs. To inform this development, a systematic review was conducted encompassing existing IoT security frameworks, risk assessment methodologies, and documented SME-specific security challenges [50]. This review served not only to map the current state of practice but also to identify key gaps in applicability, usability, and scalability that constrain existing solutions in SME environments.

The proposed framework does not introduce novel security mechanisms. Instead, it synthesizes established methodologies into an integrated, coherent structure optimized for resource-limited organizations. It draws from recognized standards such as the NIST Cybersecurity Framework (CSF) [17] and ISO/IEC 27005 [19] for risk assessment, while employing threat modeling techniques like STRIDE [40] and PASTA [41] to systematically identify and categorize threats. These components are combined to form a pragmatic, stepwise process that lowers the entry barrier for SMEs seeking to enhance their cybersecurity posture.

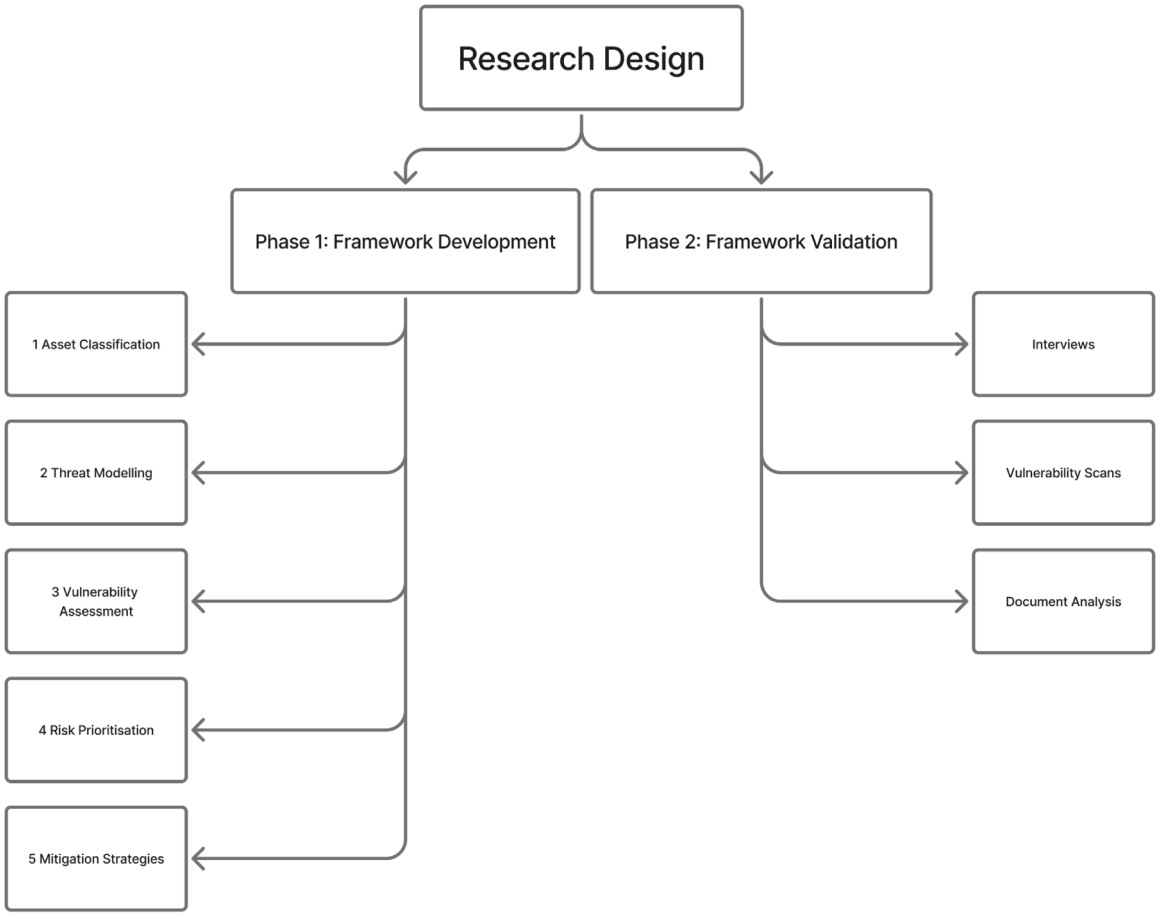


Fig. 1. Research Design.

The resulting framework consists of five interlinked components:

1. **Asset Classification**: Systematic identification and categorization of IoT assets based on business criticality and functional dependencies.
2. **Threat Modeling**: Application of STRIDE and PASTA to analyze potential attack vectors and system vulnerabilities.
3. **Vulnerability Assessment**: Technical analysis of system weaknesses using industry-standard tools such as Nessus and OpenVAS.
4. **Risk Prioritization**: Development of a context-aware risk matrix that accounts for both likelihood and business impact, tailored to SME constraints.
5. **Mitigation Strategies**: Selection of cost-effective and scalable security controls, including technical (e.g., encryption, access control) and procedural (e.g., regular patching) safeguards.

3.1.2. Phase 2: framework validation

The second phase involves empirical validation of the proposed framework through a single-case study conducted in a real-world SME setting. This qualitative-quantitative design enables the evaluation of the framework's practical relevance, scalability, and impact under authentic operational constraints. The case study subject, Lilac Studio, is a Dubai-based SME operating in the retail sector. It was selected using purposive sampling based on three criteria: (1) active use of IoT technologies, (2) resource limitations typical of SMEs, and (3) willingness to participate in comprehensive evaluation procedures [51].

Data collection in this phase employed triangulated methods to enhance reliability and capture multidimensional insights:

- Semi-structured interviews were conducted with six SME stakeholders, including two business owners, two IT personnel, and two operational staff, all based in the United Arab Emirates. While the sample size is small, it reflects key functional roles commonly found in SMEs and provides a representative cross-section of perspectives within the organization. The findings are contextually relevant for other SMEs operating in sectors such as retail, logistics, and hospitality, which share similar IoT adoption patterns and cybersecurity constraints.
- Vulnerability scanning was performed using Nessus and OpenVAS before and after framework implementation, providing objective metrics on system-level improvements.
- Document analysis of internal security policies and historical incident reports was conducted to establish a baseline and track procedural enhancements.

This multi-source approach ensures that the framework's effectiveness is evaluated both technically and operationally, supporting its practical relevance and broader applicability to similarly structured SMEs.

While the single-case design enables deep contextual analysis, it inherently limits the generalizability of the findings to other SME settings or industry domains. The selected case represents a typical example of a digitally enabled SME in a resource-constrained environment, but further validation across multiple organizations and sectors is needed to confirm the framework's broader applicability. This limitation is acknowledged as a trade-off for depth and realism in early-phase framework evaluation.

3.2. Ethical considerations and limitations

This study was conducted in strict accordance with established ethical research protocols, with particular attention to the principles of informed consent, participant confidentiality, and data anonymization [47]. All participants involved in interviews and data collection activities were fully briefed on the study's objectives, procedures, and their rights, including the right to withdraw at any point without consequence. Written informed consent was obtained prior to participation. To protect the integrity and privacy of sensitive organizational data, all collected information was anonymized and securely stored on encrypted systems, with access restricted to the research team.

Despite its contributions, the study is subject to several methodological limitations that warrant consideration. First, the use of a single-case study design, although well-suited to in-depth, context-specific exploration, may limit the generalizability of the findings to other SME contexts or industry sectors. While the selected case is representative of many SME characteristics, broader validation across diverse organizational settings is necessary to strengthen external validity.

Second, a portion of the data collected, particularly through stakeholder interviews, is self-reported, and thus potentially subject to biases such as recall error or social desirability. However, these limitations were mitigated through methodological triangulation, including the integration of quantitative vulnerability scan data and document analysis. This multi-source validation strategy enhances the credibility of the findings and supports a more holistic understanding of the framework's effectiveness.

Overall, while recognizing its constraints, the study is designed with sufficient methodological rigor to ensure reliability and relevance. These limitations also offer pathways for future research, particularly in extending validation efforts to additional SMEs and industry domains.

4. Proposed framework

This section introduces the five-step IoT risk-based framework developed specifically for SMEs. Each component of the framework is discussed in detail, emphasizing practical implementation and scalability.

4.1. Overview

This section introduces the proposed risk-based IoT security framework, which builds on insights from prior research and established industry practices. Designed specifically for SMEs, the framework systematically addresses the unique cybersecurity challenges that arise in managing IoT environments. SMEs are particularly susceptible to IoT-related threats due to constrained budgets, fragmented infrastructure, and limited in-house expertise. To address these realities, the framework provides a structured yet accessible approach that strengthens security without introducing unnecessary complexity or financial burden.

The framework comprises five sequential steps, asset classification, threat modeling, vulnerability assessment, risk prioritization, and mitigation planning. Each step builds on the preceding one, ensuring a logical and scalable progression toward comprehensive risk management. These components are elaborated in detail in Section 4.2, with emphasis on real-world applicability, cost-effectiveness, and compatibility with SME operational models.

By consolidating established cybersecurity practices, such as those found in the NIST Cybersecurity Framework and ISO/IEC 27005, into a streamlined and integrated process, the framework combines theoretical rigor with practical usability. It enables SMEs to identify critical assets, assess threats, quantify risks, and implement appropriate mitigation strategies, all while remaining within realistic operational and resource boundaries. Unlike traditional frameworks that treat these components in isolation, this framework uniquely fuses STRIDE, CVSS, and Bayesian inference into a continuous cycle, supporting iterative risk reassessment as new evidence emerges.

4.2. Process

The operational logic of the proposed framework is realized through five interlinked stages that guide SMEs through the identification, evaluation, and mitigation of IoT security risks. Each step balances methodological precision with operational feasibility, allowing implementation by teams with limited cybersecurity expertise.

Fig. 2 illustrates the five-step IoT security risk framework, presenting each component in a sequential, SME-friendly format. This visual representation supports structured implementation by mapping the flow from asset identification to final mitigation.

Risk prioritization within the framework is further operationalized through Algorithm 1, which presents a lightweight, resource-aware approach for ranking threats based on likelihood, impact, and feasibility of mitigation. The algorithm integrates static scoring and, where applicable, Bayesian inference to support dynamic risk recalibration.

1. **Asset Classification**: The process begins with the identification and categorization of IoT assets based on their criticality to core business operations. This step creates a foundational asset inventory and establishes dependencies, which are essential for contextualizing subsequent risk assessments. The asset classification process follows a structured algorithm designed specifically for SMEs, which accounts for device criticality, functional dependencies, and data sensitivity. The steps are detailed in Algorithm 2 in Appendix A.
2. **Threat Modeling**: Leveraging established methodologies such as STRIDE, organizations systematically map threat categories to identified assets. This process uncovers potential attack vectors and anticipates their business impacts. The application of STRIDE for threat modeling is guided by a structured procedure adapted for SME environments. The detailed steps are outlined in Algorithm 3 in Appendix A.
3. **Vulnerability Assessment**: Automated scanning tools such as Nessus and OpenVAS are employed to detect known vulnerabilities across device, network, and software layers. The results are augmented by CVSS-based exploitability scores, yielding actionable insights for remediation. The vulnerability assessment process is carried out using a three-stage procedure that includes automated scanning and optional penetration testing, tailored to SME capacity. This process is described in Algorithm 4 in Appendix A, while tool-specific configurations are detailed in Appendix B.
4. **Risk Prioritization**: Identified threats and vulnerabilities are evaluated using a custom risk matrix that considers likelihood, business impact, and resource constraints. For SMEs with access to advanced data, Bayesian inference can be used to dynamically update risk levels based on new evidence, providing a more accurate and responsive prioritization model.
5. **Mitigation Planning**: Based on the prioritized risks, SMEs implement cost-effective and scalable controls such as firmware updates, network segmentation, access control mechanisms, or employee training. These mitigation actions are aligned with organizational capacity and regulatory requirements (e.g., GDPR Article 32 and the UAE PDPL), ensuring both compliance and operational fit. Associated cost and effort estimates are provided in Appendix C.

A core strength of the framework lies in its resource-aware risk prioritization mechanism, which enables SMEs to direct limited efforts toward the most critical risks. This process is operationalized through a lightweight algorithm that computes a risk score for each threat using impact and likelihood metrics. Where available, Bayesian scoring replaces subjective estimations to enhance accuracy. The algorithm filters threats through a resource constraint lens, selecting only those for which mitigation is feasible within the SME's available capacity.

This algorithm enables SMEs to focus their limited resources on mitigating the highest-priority threats. The incorporation of Bayesian inference allows for dynamic recalibration of risk scores as new data becomes available, ensuring that the framework remains both adaptive and aligned with the evolving threat landscape.

4.3. Scalability and adaptability

A key strength of the proposed framework lies in its adaptability across a wide range of SME IoT contexts. Recognizing that IoT implementations vary in scale, complexity, and purpose even within the SME segment, the framework is designed to be modular and context-aware. It enables SMEs to tailor adoption based on their existing infrastructure, technical maturity, and regulatory requirements, while maintaining alignment with core risk management principles.

Rather than attempting to generalize across all industry sectors, the framework is explicitly focused on IoT-enabled SMEs, particularly those deploying connected devices for operational monitoring, automation, or service delivery. These include SMEs in retail, logistics, and light industrial settings, domains where IoT adoption is growing and where SMEs remain key stakeholders.

The framework also supports adaptation along two practical dimensions:

- Maturity-Based Adaptations: SMEs with limited technical capacity can adopt a lightweight implementation by prioritizing essential steps such as asset classification and risk assessment using default STRIDE and CVSS templates. More mature SMEs can integrate advanced tools, including Bayesian updating and automated vulnerability scanning, for deeper security insights.
- Regulatory Adaptability: The framework is compatible with jurisdiction-specific compliance mandates. For example, SMEs operating in the European Union can incorporate GDPR-aligned safeguards, while those in the UAE can tailor their implementation to meet the requirements of the Federal Personal Data Protection Law (PDPL).

By focusing on IoT-reliant SMEs and enabling scaling based on operational maturity and legal context, the framework offers a proportionate and sustainable approach to risk management without overextending its intended scope.

The framework is further supported by a practical and reusable toolset tailored to the constraints of IoT-enabled SMEs. It incorporates widely recognized methodologies and tools, including STRIDE for threat modeling, Nessus Essentials and OpenVAS for vulnerability assessment, CVSS v3.1 calculators for risk quantification, and optional Bayesian

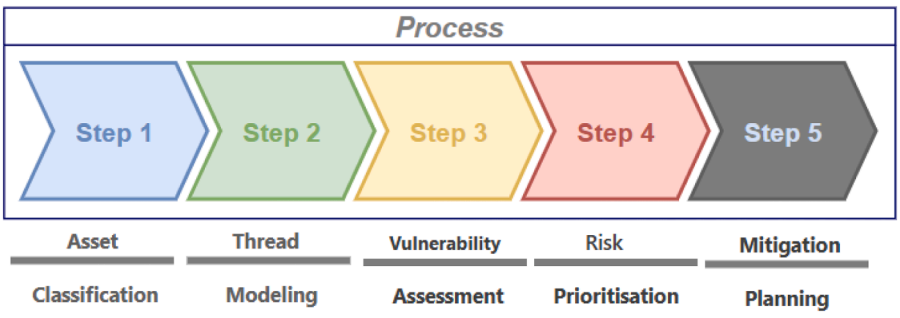


Fig. 2. Five-Step IoT Security Risk Framework for SMEs.

Algorithm 1
Risk Prioritization for IoT Systems in SMEs.

Require: Threat list T, Vulnerability set V, Asset inventory A, Resource constraints R. Optional: Bayesian posterior probabilities P (t |E)
Ensure: Prioritized threat list P
P ←∅
for all threat t ∈T **do**
Retrieve associated asset a ∈A
if Bayesian scoring available then
L(t) ← $P(t|E)$
else
Assign likelihood L(t) ∈{1, 2, 3} ▷ Low, Medium, High
end if
Assign impact I(t) ∈{1, 2, 3}from asset criticality
Compute risk score R(t) ←L(t) × I(t)
end for
Sort T in descending order of R(t)
for all threat t ∈T **do**
Estimate mitigation effort E(t) (cost or hours)
if E(t) ≤R then
Add t to P
R ←R−E(t)
end if
end for
return P

inference scripts for post-mitigation risk updating. All components are either open-source or available under free/community licenses, making them accessible and cost-effective for resource-constrained organizations while ensuring methodological rigor.

4.4. Cost effectiveness

The proposed framework has been intentionally designed with cost efficiency as a core principle, acknowledging the significant financial and technical constraints that characterize many SMEs. In contrast to enterprise-grade security models that often require substantial investments in personnel, infrastructure, and proprietary technologies, this framework offers a practical and economically viable pathway for enhancing IoT cybersecurity in resource-constrained environments.

Several interrelated features contribute to its cost-effectiveness:

- Use of Readily Available and Open-Source Tools: The framework emphasizes reliance on established, freely accessible resources, such as Nessus Essentials, OpenVAS, and CVSS calculators, thereby eliminating the need for costly commercial solutions or vendor lock-in. This approach significantly reduces implementation costs while maintaining analytical rigor.
- Scalability and Incremental Adoption: The framework supports modular deployment, allowing SMEs to implement core components, such as asset classification and basic threat modeling, before gradually expanding to include more sophisticated elements like Bayesian-based risk updating. This progressive rollout aligns with variable budget cycles and evolving security maturity.
- Risk-Based Prioritization: By incorporating a customized risk prioritization algorithm, the framework ensures that security investments are directed toward the most critical threats and vulnerabilities. This targeted approach enhances return on investment by aligning mitigation efforts with business-critical assets and realistic threat likelihoods.
- Operational Simplicity: The framework is designed to be intuitive and accessible, requiring minimal cybersecurity expertise to deploy. SMEs can follow structured processes and algorithmic guidance without needing to hire specialized security consultants or establish dedicated SOC teams.
- Structured Methodology: Its clear, step-by-step architecture reduces ambiguity and streamlines implementation. This structure helps SMEs avoid ad hoc security practices and fosters consistent risk management practices over time.

In sum, the framework offers a cost-effective, scalable, and technically feasible solution for SMEs seeking to secure their IoT ecosystems. By integrating essential components, asset classification, threat modeling, vulnerability assessment, risk prioritization, and mitigation planning, it provides a structured and context-sensitive approach that accommodates the diverse capabilities and constraints of SME environments. Its emphasis on affordability, adaptability, and operational clarity makes it especially valuable in an era of rapidly expanding IoT adoption among smaller organizations.

5. Case study

To evaluate the proposed framework, a case study was conducted in a real-world SME environment. This section details the application process, observed results, and validation methodology.

5.1. SME profile

Lilac Studio is a Dubai-based SME operating in the retail sector, specializing in curated lifestyle products such as celebration robes, personalized accessories, and gift boxes. The company employs a hybrid operational model, combining a physical storefront located in a commercial retail complex with an e-commerce platform that serves regional customers across the United Arab Emirates. To streamline operations and enhance the customer experience, Lilac Studio has adopted several Internet of Things (IoT) technologies, including smart inventory sensors, Wi-Fi-enabled point-of-sale (PoS) systems, and mobile-connected surveillance cameras.

These IoT-enabled systems support real-time inventory tracking, efficient transaction processing, and continuous physical security monitoring, illustrating the increasing digitalization of operational workflows even within small retail environments. However, despite its growing technological footprint, Lilac Studio operates with minimal internal IT staffing and a modest cybersecurity budget, consistent with the broader profile of resource-constrained SMEs.

This juxtaposition of digital dependency and limited cybersecurity maturity renders Lilac Studio an ideal testbed for evaluating the proposed IoT risk management framework. The case study captures the typical challenges faced by SMEs attempting to secure complex, interconnected systems in the absence of dedicated security personnel or advanced infrastructure. As such, it provides a realistic and relevant context for assessing the framework's applicability, usability, and effectiveness in achieving measurable improvements in cybersecurity posture.

5.2. Application of the framework

The proposed risk-based framework was applied to Lilac Studio's IoT environment to evaluate its practicality and impact in a real-world SME context. The implementation followed the framework's five core components: asset classification, threat modeling, vulnerability assessment, risk prioritization, and mitigation planning.

5.2.1. Asset classification

The first step involved identifying and categorizing the organization's IoT assets based on their criticality to business operations, the sensitivity of data processed, and integration with other digital systems. Asset value scores, ranging from 1 (low importance) to 10 (critical, were determined through consultations with the operations manager, sales personnel, and a brief technical audit. These scores provide the foundation for subsequent threat analysis and risk prioritization. The identified IoT assets were categorized based on their business criticality, functional roles, and interdependencies, as shown in Table 2.

5.2.2. Threat modeling

Using the STRIDE methodology, each asset was evaluated to identify potential threat types, enabling a structured assessment of the organization's attack surface. STRIDE threats were mapped to each asset to anticipate likely exploitation scenarios and their associated business impacts. The results of this mapping are presented in Table 3, which aligns each asset with its corresponding threat categories based on architectural vulnerabilities and exposure vectors.

5.2.3. Vulnerability assessment

Comprehensive vulnerability scans were conducted using OpenVAS and Nessus Essentials across all five IoT-enabled assets. The assessment uncovered 19 vulnerabilities, categorized using CVSS v3.1 severity ratings. These included 5 critical vulnerabilities, such as remote code execution flaws in surveillance firmware and exposed default credentials on the IoT gateway, along with additional high, medium, and low severity issues. The distribution and examples of identified vulnerabilities across severity levels are summarized in Table 4.

See Appendix B for the scan setup, plugin families used, and representative CVSS vectors.

5.2.4. Risk prioritization

To determine which threats warranted immediate mitigation, a structured risk scoring model was applied. Each asset's value score was multiplied by the CVSS-based likelihood estimate of exploitation, producing a static risk score. The resulting calculations and classifications are presented in Table 5, which shows the risk levels for the most business-critical assets based on static risk scoring.

$$\textit{Static Risk Score}_{i,j} = V(a_j) - L(t_i) \tag{1}$$

Where:

- $V(a_j)$: Asset value score for asset a_j
- $L(t_i)$: Likelihood of threat t_i, derived from CVSS or other metrics

Table 2
IoT Asset Classification.

IoT Asset	Description	Value Score
Smart Inventory Sensors	Tracks stock levels and updates in real-time	8
Cloud-Connected PoS	Handles transactions and customer payments	9
Surveillance Cameras	Monitors physical store remotely	6
E-Commerce Platform	Customer ordering	10
IoT Gateway/Router	Connects all devices to central network	9

Table 3
Threat Modeling (STRIDE).

Asset	Threats Identified
Smart Inventory Sensors	Spoofing, Information Disclosure
PoS Terminal	Elevation of Privilege, Tampering, Repudiation
Surveillance Cameras	Information Disclosure, Denial of Service
E-Commerce Platform	Spoofing, Tampering, Information Disclosure
IoT Gateway	Denial of Service, Elevation of Privilege

Table 4
Severity Distribution.

CVSS Severity	Vulnerability Examples	Count
Critical	IoT Gateway default credentials, firmware RCE	5
High	SQLi on PoS, weak TLS/SSL ciphers	8
Medium	Input validation flaws	4
Low	Weak password policy, missing headers	2

Table 5
Static Risk Scores.

Asset	Value Score	Likelihood	Static Risk Score
Surveillance Cameras	6	8.5	51.0
PoS Terminal	9	7.2	64.8
IoT Gateway	9	9.0	81.0

Note: The likelihood is CVSS-derived.

Each threat is evaluated using a standard risk scoring formula:

$$R = L \times I \tag{2}$$

where R represents the overall risk score, L denotes the likelihood of threat occurrence (rated as 1 = low, 2 = medium, 3 = high), and I represents the potential business impact (1 = minor, 2 = significant, 3 = critical). This simple but effective method allows SMEs to rank threats based on operational severity, forming the foundation for prioritized mitigation planning.

The resulting calculations and classifications are presented in Table 5, which shows the risk levels for the most business-critical assets based on static risk scoring.

Risks were then categorized using a simple 3-tier model:

- Low (0–15)
- Medium (16–40)
- High (41–100)

The risk categorization thresholds were defined using expert judgment and SME-specific resource constraints. This approach is consistent with ISO/IEC 27005 guidance [19] and ENISA recommendations [21], both of which support context-aware, non-uniform risk boundaries based on operational impact, resource availability, and business risk tolerance. In resource-constrained environments like SMEs, risk prioritization emphasizes operational feasibility over statistical uniformity, allowing high-impact threats to be surfaced more aggressively even if scoring intervals are uneven.

This prioritization ensured that mitigation strategies targeted the most business-critical vulnerabilities, particularly those impacting customer data and payment infrastructure. Lower-risk assets were incorporated into a secondary mitigation schedule based on resource availability.

5.2.5. Mitigation strategies

Based on the risk assessment results, tailored mitigation strategies were developed for each high-risk asset class. These controls address both hardware and software vulnerabilities, including application-level issues such as unpatched content management systems (CMS) and

insecure APIs. The mitigation efforts prioritize technical feasibility, cost-efficiency, and regulatory alignment with data protection requirements such as the GDPR and UAE PDPL.

Table 6 below summarizes the selected mitigation actions, grouped by asset:

These mitigation controls were selected to balance impact severity with implementation complexity, ensuring that the organization could address the most critical vulnerabilities within its operational capacity. Where possible, open-source tools and existing infrastructure were leveraged to minimize cost. All actions were documented to support audit readiness and regulatory compliance.

5.3. Probabilistic risk modeling using probability

To overcome the rigidity of static risk matrices, the framework incorporates Bayesian inference to revise likelihood estimates based on post-control conditions. For example, after firmware updates were applied to the surveillance cameras, the likelihood of successful exploitation dropped significantly. Bayes' Theorem for Posterior Likelihood:

$$P(t_i|E) = \frac{P(E|t_i).P(t_i)}{P(E)} \tag{3}$$

Bayesian-adjusted risk score:

$$Bayesian\ Risk\ Score_{i,j} = V(a_j) \times P(t_i|E) \tag{4}$$

Where:

- $P(t_i)$: Prior probability of threat t_i
- $P(E|t_i)$: Likelihood of observing evidence E given t_i
- $P(t_i|E)$: Updated probability after evidence is collected
- $V(a_j)$: Asset value, same as before

Table 6
Asset-Specific Mitigation Strategies Addressing Hardware and Software Threats.

Asset	Identified Threats/ Vulnerabilities	Mitigation Strategies
Surveillance Cameras	Remote code execution (RCE), default credentials, unencrypted streams	- Apply latest firmware updates to patch RCE flaws - Disable remote admin access - Enable TLS for video feeds
PoS Terminal	SQL injection, lack of input validation, insecure API connections	- Implement server-side input validation and sanitization - Deploy a Web Application Firewall (WAF) - Enforce HTTPS and secure API keys
IoT Gateway	Default login credentials, open ports, weak authentication	- Replace default credentials with unique strong passwords - Enable multi-factor authentication (MFA) - Implement network segmentation
E-Commerce Platform	Unpatched CMS, exposed admin panel, insecure session management	- Regularly update CMS plugins and core - Restrict admin access by IP and enforce MFA - Implement secure cookie settings and session timeout
Smart Inventory Sensors	Lack of authentication, spoofing risk, insecure data transmission	- Enforce mutual authentication between sensors and gateway - Encrypt data in transit (TLS) - Configure MAC address whitelisting

The results of applying Bayesian inference to adjust threat likelihoods based on post-control evidence are presented in Table 7, which illustrates the resulting risk score reductions across key IoT assets.

Full scoring examples and base vector configurations are included in Appendix B.

5.3.1. Integration with the framework

The Bayesian risk model is integrated into the proposed framework as a second-stage enhancement, augmenting the initial static risk matrix with dynamic, evidence-driven recalibration. While the qualitative matrix offers an accessible entry point for SMEs, particularly during early-stage assessments, its static nature limits responsiveness to real-time changes in threat conditions. The Bayesian component addresses this limitation by introducing probabilistic updating, enabling SMEs to refine risk estimates as new evidence becomes available (e.g., via scanner logs, incident reports, or patch records).

Recommended Implementation Flow:

1. Initial Risk Matrix: Risk scores are calculated based on static likelihood-impact assessments, typically using CVSS data and asset value scores.
2. Evidence Collection: SMEs gather new data from system logs, vulnerability scanners, and update records that inform post-control conditions.
3. Bayesian Update: Posterior threat probabilities are computed using Bayes' Theorem, allowing likelihood scores to reflect real-world changes.
4. Reprioritized Mitigation: Updated risk scores guide resource reallocation, shifting focus to residual or emerging risks.

This probabilistic integration enhances cost efficiency, as SMEs avoid overspending on already mitigated threats. It also improves agility, enabling organizations to shift posture without complex reengineering or external consultation. From a usability perspective, the model is designed to function with basic spreadsheet tools or lightweight scripts, making it feasible for SMEs with limited technical resources. Together, the static matrix and Bayesian model offer a scalable, hybrid approach, starting with simplicity and evolving into adaptive precision as operational maturity improves.

5.3.2. Deriving Bayesian parameters in practice

Applying Bayesian inference in the context of an SME, such as Lilac Studio, involves translating observable operational indicators and domain knowledge into probability estimates. The key components of Bayes' Theorem, prior probability, evidence, likelihood, and marginal probability, are derived as follows:

- Prior Probability $P(t_i)$: Represents the baseline likelihood of a specific threat. In this case, Lilac Studio assigns a prior probability of 0.3 to a Denial-of-Service (DoS) attack on its IoT gateway, based on historical latency issues and sector-specific threat intelligence.
- Evidence E: The new observation that may indicate an active threat. Lilac Studio identifies increased traffic volume and repeated port scanning attempts from untrusted IP addresses during business hours.

Table 7
Bayesian-Adjusted Risk Scores.

Asset	Value Score	Posterior Likelihood	Bayesian Risk Score
Surveillance Cameras	6	2.0	12.0
PoS Terminal	9	4.0	36.0
IoT Gateway	9	3.0	27.0

- Likelihood $P(E|t\_i)$: The probability of observing this evidence if the threat (T) is actually occurring. Drawing from industry reports, 80 % of confirmed DoS attacks are preceded by similar traffic anomalies, giving P(E|T) = 0.80.
- Marginal Probability $P(E)$: The overall chance of seeing the observed anomaly, regardless of whether a DoS attack is underway. Historical logs suggest such events occur approximately 40 % of the time, resulting in P(E) = 0.40.

Applying Bayes' Theorem:

$$P(t_i|E) = \frac{P(E|t_i).P(t_i)}{P(E)} = \frac{0.8 \times 0.3}{0.4} = 0.6 \quad (5)$$

- Interpretation: After incorporating real-time evidence, the probability of an active DoS attack increases from 0.30 (prior) to 0.60 (posterior). This represents a substantial escalation in risk perception.
- Use in Framework: The updated posterior probability (0.60) replaces the static likelihood score in the risk calculation formula. For instance, for the IoT gateway, with an asset value of 9:

$$Bayesian\ Risk\ Score_{ij} = V(a_j) \times P(t_i|E) = 9 \times 0.6 = 5.4 \quad (6)$$

This revised score compared to a pre-mitigation score of 81.0 (static risk based on likelihood 9.0), demonstrates a quantifiable reduction in perceived risk due to implemented controls and new contextual evidence. The use of historical cases such as the Mirai botnet [52] further validates the approach, as they illustrate the real-world plausibility of IoT devices being exploited in DoS attacks. Such precedents justify assigning elevated prior probabilities in similar contexts.

5.4. Quantitative and qualitative results

To empirically evaluate the effectiveness of the proposed risk-based framework, two full-spectrum vulnerability scans were conducted, one prior to the implementation of mitigation strategies and another after the controls were applied. Scanning was performed using both Nessus Essentials and OpenVAS, covering the same five IoT-enabled assets. All results were analyzed and categorized in accordance with the Common Vulnerability Scoring System (CVSS) v3.1, ensuring consistency and comparability.

5.4.1. Pre-implementation vulnerability scan

The initial vulnerability scan identified 19 total vulnerabilities across critical IoT assets, with severity levels ranging from low to critical. Notable weaknesses included default administrative credentials, outdated firmware, and SQL injection flaws. These findings are quantified by severity level and summarized in Table 7, which highlights the scope of exposure prior to the implementation of mitigation strategies.

5.4.2. Post-implementation vulnerability scan

Following the mitigation efforts, a second vulnerability scan revealed a marked reduction in total and high-severity vulnerabilities. The comparative results between pre- and post-mitigation periods, including percent change in each category, are detailed in Table 8, illustrating the framework's measurable impact on reducing cybersecurity risk across the SME's IoT environment.

5.4.3. Statistical impact analysis

To further quantify the reduction in overall risk, the mean CVSS score for detected vulnerabilities was calculated for both assessment periods:

Table 8
Vulnerability Comparison by Severity.

Severity	Pre-Mitigation	Post-Mitigation	% Change
Critical	5	1	−80 %
High	8	2	−75 %
Medium	4	5	+25 % (reclassified)
Low	2	3	+50 %
Total	**19**	**11**	**−42.1%**

Note: Certain vulnerabilities were reclassified based on reduced exploitability following partial remediation.

- Pre-Implementation: Mean = 8.1, SD = 1.23
- Post-Implementation: Mean = 5.6, SD = 1.91

This corresponds to a 30.9 % reduction in average vulnerability severity, indicating a substantial improvement in the organization's security posture. The increase in standard deviation is expected, as the remaining vulnerabilities were more dispersed across lower severity categories following mitigation efforts. These quantitative results validate the framework's effectiveness in reducing exposure to critical and high-risk threats in a real-world SME environment. The outcomes also support the suitability of the framework's structured approach for incremental, cost-efficient risk reduction.

5.4.4. Qualitative feedback

In addition to the quantitative findings, qualitative feedback was gathered to assess the perceived usability, effectiveness, and organizational impact of the proposed framework. Informal interviews were conducted with four key stakeholders at Lilac Studio: the business owner, store manager, inventory manager, and a frontline employee. The feedback was analyzed using thematic analysis, following the six-phase methodology outlined by Braun and Clarke [53]. These phases included familiarization with the data, generation of initial codes, identification and refinement of themes, and narrative synthesis.

Three dominant themes emerged from the analysis, reflecting the framework's practical influence across different organizational levels:

- Practicality and Accessibility: Stakeholders consistently emphasized the ease of implementation. The business owner stated, "The framework provided a clear roadmap for securing our IoT systems without overwhelming our small team." Both technical and non-technical staff described the framework's step-by-step structure as intuitive and scalable, suggesting its accessibility even in low-resource environments.
- Operational Continuity: The store manager noted that "the security improvements were seamless and didn't disrupt daily operations." This observation was echoed by the inventory manager, who reported increased system reliability and fewer discrepancies in stock management, suggesting that the framework enhanced security without compromising efficiency.
- Awareness and Confidence: A frontline employee remarked, "The training was really helpful; I understand the risks better now." This feedback reflects a broader organizational shift toward increased security awareness and procedural clarity. Staff members expressed greater confidence in managing and responding to cyber risks.

These insights corroborate the quantitative results presented earlier. Stakeholders reported improved trust in the security of their systems and expressed confidence in the organization's preparedness to address future threats. The framework's non-disruptive and user-centric design appears to have contributed to both technical readiness and organizational alignment.

Overall, the qualitative findings affirm that the framework is not only functionally effective but also culturally adoptable, making it well-suited for replication in similarly structured SMEs. Its ability to foster

staff engagement, procedural clarity, and operational continuity highlights its value as a pragmatic cybersecurity solution for resource-constrained environments.

5.4.5. Key performance indicators (KPIs)

To objectively evaluate the impact of the proposed framework, a set of Key Performance Indicators (KPIs) was defined and tracked before and after implementation. These indicators were selected to reflect critical dimensions of cybersecurity maturity, including technical risk reduction, procedural readiness, and organizational awareness. Together, they provide a holistic view of the framework's effectiveness in a real-world SME setting.

The following five KPIs were used:

- %Critical Vulnerabilities: The proportion of total vulnerabilities classified as *Critical* as CVSS $\geq$9.0 indicating exposure to the most severe threats.
- Mean CVSS Score: The average severity of all detected vulnerabilities, serving as a composite indicator of overall system risk.
- Time to Mitigation (TtM): The average time (in days) required to remediate high and critical vulnerabilities, reflecting operational responsiveness.
- Incident Response Preparedness: The presence or absence of documented and tested incident response (IR) procedures.
- Employee Security Awareness: The percentage of staff who completed foundational security awareness training, reflecting organizational readiness and cultural alignment.

The impact of the framework across key cybersecurity performance dimensions is summarized in Table 9, which tracks changes in technical, procedural, and organizational metrics before and after implementation.

These results demonstrate substantial improvements across all five indicators. The percentage of critical vulnerabilities was reduced by over 65 %, while the average CVSS score declined by 30.9 %. The Time to Mitigation improved significantly, dropping from an unstructured 30-day cycle to a more agile 10-day process. Moreover, the organization moved from having no formal incident response plan to one that was both documented and tested. Perhaps most notably, employee security awareness increased from 0 % to 90 %, indicating a strong cultural shift toward proactive cyber hygiene. Collectively, these KPI trends affirm the framework's capacity to produce measurable, multidimensional improvements in SME cybersecurity posture, spanning technical risk, operational agility, and human factors.

6. Discussion

This section discusses the effectiveness of the proposed framework, synthesizing both the quantitative and qualitative results. It also compares the framework against established models and reflects on broader implications for SME cybersecurity practice.

6.1. Application of the framework

The implementation of the proposed risk-based framework at Lilac Studio offers compelling evidence of its practical value in addressing IoT security challenges within a real-world SME context. The structured methodology, spanning asset classification, threat modeling, vulnerability assessment, risk prioritization, and mitigation planning, enabled the organization to identify and remediate critical risks in a systematic, resource-aware manner.

Table 9
Key Performance Indicators (KPIs).

KPI	Pre-Implementation	Post-Implementation
% Critical Vulnerabilities	26.3 %	9.1 %
Mean CVSS Score	8.1	5.6
Time to Mitigation (TtM)	30 days (ad hoc)	10 days (structured)
IR Preparedness	None	Documented + tested
Employee Security Awareness	0 %	90 %

By categorizing IoT assets based on business impact and integrating these classifications into a multi-layered risk evaluation process, the organization was able to focus its limited cybersecurity resources on the most pressing threats. The application of targeted mitigation strategies, including firmware updates, credential hardening, network segmentation, and the deployment of a Web Application Firewall (WAF), resulted in a substantial reduction in the number and severity of vulnerabilities. Quantitative improvements included a 42.1 % reduction in total vulnerabilities and a 30.9 % decrease in average CVSS scores, demonstrating the framework's capacity to drive measurable security outcomes.

Equally important were the organizational benefits. The inclusion of structured security awareness training increased employee engagement and contributed to a culture of proactive security management, as reflected in the 90 % training participation rate. Positive stakeholder feedback further validated the framework's accessibility, scalability, and minimal disruption to day-to-day operations.

Overall, the Lilac Studio case study illustrates how a cost-effective, modular, and methodologically rigorous framework can empower SMEs to improve their cybersecurity posture without exceeding their operational or financial limits. The results support the framework's broader applicability across similarly structured SMEs, positioning it as a scalable solution for enhancing cybersecurity resilience in the rapidly expanding IoT landscape.

6.2. Framework effectiveness

The effectiveness of the proposed framework is demonstrated not by the invention of new cybersecurity mechanisms, but by its strategic realignment of established practices toward the unique needs of SMEs. At Lilac Studio, the framework enabled a comprehensive and systematic assessment of the organization's IoT ecosystem. By categorizing assets based on business criticality and aligning these with structured risk assessment techniques, the company was able to prioritize its limited cybersecurity resources efficiently.

One of the most impactful elements was the framework's tailored risk prioritization process, which directed attention to the most critical vulnerabilities. This approach ensured that mitigation efforts were not diluted across all identified issues but instead focused on those posing the greatest business risk. The application of controls, such as firmware updates, web application firewalls, and network segmentation, resulted in measurable improvements in vulnerability reduction, operational continuity, and staff awareness. These interventions were specifically selected for their low cost, ease of implementation, and regulatory alignment with standards like the GDPR and UAE PDPL.

Another strength of the framework lies in its accessibility. Its step-by-step design, supported by practical tools and algorithms, allowed non-specialist staff to participate in the security improvement process without requiring advanced expertise. The use of scalable controls and guidance documents made the implementation feasible for an organization with minimal internal IT capacity.

Importantly, the framework enabled Lilac Studio to shift from a reactive to a proactive security posture. Instead of responding to incidents ad hoc, the company began adopting preventive measures based on formalized asset risk profiles and updated threat intelligence. This cultural shift was reinforced by a 90 % employee participation rate in security training and by the introduction of documented incident response protocols, both of which were absent prior to framework adoption.

The inclusion of Bayesian risk scoring in the framework further enhanced its analytical depth and responsiveness. However, to maintain focus in the discussion section, the Bayesian scoring formula and

numerical example have been relocated to Section 5.3.2, where quantitative risk adjustments are explained in detail. This separation preserves the clarity of the narrative while ensuring methodological transparency.

Quantitative outcomes further validate the framework's utility. Over a six-week implementation period, Lilac Studio experienced a 42.1 % reduction in total vulnerabilities and a 30.9 % decrease in mean CVSS scores. These metrics highlight the framework's capacity to deliver both immediate and sustainable security improvements in an SME environment. Collectively, the results confirm that when security strategies are aligned with operational constraints, even small organizations can achieve significant cybersecurity gains.

6.3. Comparison of existing frameworks

Existing frameworks for IoT security, such as the NIST Cybersecurity Framework (CSF), ISO/IEC 27005, and OWASP IoT Project, provide valuable guidance but often fall short in addressing the unique needs of SMEs. The NIST CSF, while comprehensive, requires significant resources and expertise, making it challenging for SMEs with limited budgets and technical capabilities to implement effectively. Similarly, ISO/IEC 27005 offers detailed guidelines for risk management but is often too complex and resource-intensive for smaller organizations. The OWASP IoT Project, though practical, lacks a structured risk assessment process, leaving SMEs without clear prioritization of risks. These frameworks also tend to be generic, lacking tailored guidance for the specific challenges SMEs face, such as limited IT infrastructure and cybersecurity expertise. While recent frameworks target industrial control systems specifically [54], they often assume PLC-centric architectures, limiting applicability to general-purpose IoT infrastructures found in SMEs.

The proposed framework addresses these gaps by offering a cost-effective, scalable, and SME-focused approach to IoT security. It simplifies complex methodologies like risk assessment and threat modeling, making them accessible to non-technical stakeholders. By integrating asset classification, vulnerability analysis, and risk prioritization, the framework provides a structured yet flexible process that SMEs can adapt to their specific contexts. Additionally, it emphasizes practical, actionable steps and leverages readily available tools, reducing the need for specialized expertise or significant financial investment. This tailored approach ensures that SMEs can enhance their IoT security posture without overburdening their resources, bridging the gap left by existing frameworks.

The comparative strengths and limitations of the proposed framework relative to established alternatives such as NIST CSF, ISO/IEC 27005, ENISA, and the OWASP IoT Project are summarized in Table 10, using a set of measurable KPIs to highlight practical applicability for SMEs.

While ISO/IEC 27005 provides a comprehensive methodology for information security risk management, it assumes a level of maturity and resourcing that many SMEs lack. Its abstract treatment of likelihood, impact, and risk response mechanisms often requires consulting expertise to operationalize. OWASP's IoT Top 10 is valuable for threat identification but lacks integrated risk assessment or prioritization mechanisms.

In contrast, the proposed framework explicitly incorporates measurable KPIs such as CVSS severity reduction, time to mitigation, and employee readiness, offering a practical, scalable, and data-driven approach tailored to the operational realities of SMEs.

6.4. Threat modeling results and documentation

This section presents the results of the threat modeling process, which employed the STRIDE methodology to identify, categorize, and evaluate potential threats to Lilac Studio's IoT infrastructure. The methodology was implemented following the structured workflow outlined in Algorithm 3 (Appendix A), which systematically maps threats to asset attributes and system configurations. This approach ensures comprehensive coverage and operational relevance in the SME context.

Using the classified asset inventory developed during the initial assessment phase, each IoT asset was evaluated against the six STRIDE threat categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Specific vulnerabilities were identified based on configuration weaknesses, exposure to external interfaces, and known exploit vectors. These were then linked to corresponding business impacts, ensuring that the threat analysis remained both technically rigorous and business centric.

To improve traceability and practical usability, the threat documentation process recorded the affected asset, observed vulnerability, likely exploitation vector, and anticipated operational consequence. This mapping, carried out in accordance with Steps 2–8 of Algorithm 3, supports both technical remediation and decision-making by non-

Table 11
Validation of Threats Based on STRIDE Utilizing Asset Inventory.

Threat Category	Description	Asset	Identified Vulnerability	Impact
Spoofing	Potential for unauthorized devices to inject false inventory data	Sensors	Lack of authentication	False inventory data
Tampering	Risk of data manipulation	Inventory Server, PoS System	Insecure data handling	Corrupted records, financial loss
Repudiation	Lack of audit trails for transactions	PoS System	Absence of logging mechanisms	Dispute resolution failure
Information Disclosure	Exposure of customer data through unsecured networks	Network Infrastructure	Unencrypted traffic	Privacy breach, legal penalties
Denial of Service	Overloading the IoT network causing service disruptions	Sensors, Network Infrastructure	Lack of traffic filtering or rate limits	Downtime, operational loss

Table 10
KPI-Based Comparative Framework Assessment.

Feature	NIST CSF	ENISA	ISO 270005	OWASP IoT	Proposed Framework
KPI-Driven Evaluation	Not explicit	Limited	Not defined	No	Yes
CVSS Integration	Indirect	No	Indirect	No	Native
Dynamic Risk Scoring	No	Partial	No	No	Bayesian updating
Risk Prioritization Guidance	High-level	Prespective	Detailed	No	Structured, contextual
Resource Constraint Awareness	Low	Medium	Low	Low	High
Usability for SMEs	Low	Medium	Low	Medium	High
Time to Mitigation (TtM)	No	No	No	No	Embedded metric
Employee Readiness	Optional	No	No	No	Yes

technical stakeholders.

Table 11 summarizes the threat-to-asset mapping. It illustrates how identified vulnerabilities, such as lack of authentication on sensors or unencrypted traffic on the network infrastructure, correspond to STRIDE threat categories and lead to concrete business risks such as data integrity failures or service disruption. This actionable mapping provides SMEs with a prioritized and contextualized understanding of IoT security threats, allowing them to implement targeted mitigation strategies without overextending limited resources.

Threat assessment is based on predefined likelihood and impact scores, which are detailed in Section 5.2.4 as part of the risk prioritization methodology.

6.5. Implications for SMEs

The proposed framework offers significant practical benefits for SMEs, addressing their unique challenges and resource constraints while enhancing their IoT security posture. By providing a structured yet flexible approach, the framework enables SMEs to systematically identify, assess, and mitigate IoT security risks without requiring extensive technical expertise or financial investment (See Appendix C for guidance on resource allocation and cost minimization strategies.). Its emphasis on asset classification and risk prioritization ensures that limited resources are allocated efficiently, focusing on the most critical vulnerabilities and threats.

The framework's scalability allows SMEs to start small and expand their efforts as needed, making it adaptable to businesses of varying sizes and industries. Additionally, the inclusion of cost-effective security controls and practical, actionable steps empowers SMEs to implement robust security measures without overburdening their operations. By integrating staff training and clear guidance, the framework also builds internal capacity, fostering a culture of cybersecurity awareness.

Moreover, SME-specific frameworks in smart manufacturing emphasize the importance of operational continuity, real-time monitoring, and layered security [55], all of which align with the goals of this framework. Overall, the framework equips SMEs with the tools and knowledge needed to secure their IoT ecosystems, reducing the risk of disruptions, data breaches, and financial losses, while supporting business continuity and growth.

6.6. Regulatory alignment and compliance implications

While the primary goal of this framework is to enhance IoT cybersecurity posture within SMEs, it also supports alignment with key legal and regulatory obligations. For example, the European General Data Protection Regulation (GDPR), particularly Article 32, mandates data controllers and processors to implement appropriate technical and organizational measures to ensure the security of personal data [56]. The proposed framework operationalizes this requirement through its risk-based approach, which drives the adoption of proportional controls such as data encryption, network segmentation, and access restriction mechanisms [21]. Additionally, recent approaches have demonstrated the feasibility of aligning threat modeling with ISO/IEC 27005 and GDPR Article 32 through structured risk management methods [57]. The proposed framework reflects this alignment by integrating threat identification, CVSS scoring, and mitigation planning within a GDPR-compliant process.

Specifically, the asset classification and threat modeling stages of the framework allow organizations to identify where personal or sensitive data is processed, thus supporting data flow mapping and risk documentation required under Articles 30 and 35 of the GDPR [26]. Similarly, the use of vulnerability scanners and CVSS-based scoring directly supports the principle of "security by design and by default". These technical safeguards help SMEs demonstrate that personal data is adequately protected against unauthorized access or loss, core expectations under GDPR's security provisions.

In the UAE context, the framework aligns with provisions of the Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL) [58], which similarly requires entities to adopt appropriate cybersecurity measures to protect data confidentiality, integrity, and availability. The inclusion of employee training, incident response readiness, and periodic risk reassessment in the framework addresses Article 5 of the PDPL, which emphasizes both technical and organizational security measures [58].

Recent case studies have shown that mapping ISO 27005, NIST CSF, and SP 800–53 to enterprise contexts remains complex [59]; this framework simplifies that mapping by focusing on risk outputs actionable for SMEs. By embedding these legal principles into its structure, the framework not only enhances operational security but also serves as a pragmatic tool to support ongoing regulatory compliance. This is especially beneficial for SMEs that often lack dedicated legal or compliance teams and must rely on integrated approaches to meet both security and legal expectations.

6.7. Limitations

While the proposed framework demonstrates significant potential for enhancing IoT security in SMEs, it is important to acknowledge its limitations. First, the framework's effectiveness is highly dependent on the accuracy of the initial asset classification and risk assessment, which may be challenging for SMEs with limited technical expertise or incomplete knowledge of their IoT ecosystems. Second, the framework's reliance on vulnerability scanning tools and penetration testing may not uncover all potential risks, particularly those related to zero-day vulnerabilities or sophisticated attack vectors. Third, the case study's focus on a single SME, Lilac Studio, limits the generalizability of the findings, as the results may not fully represent the diverse challenges faced by SMEs in different industries or regions. Additionally, the framework's success in other contexts may vary based on factors such as the complexity of the IoT ecosystem, the level of stakeholder engagement, and the availability of resources.

Finally, while the framework emphasizes cost-effectiveness, some SMEs may still face financial or logistical barriers to implementing certain security controls. These limitations highlight the need for further research and validation across a broader range of SMEs to refine the framework and ensure its applicability in diverse settings.

7. Conclusion and future work

In an era of rapid digital transformation, SMEs face a growing need to adopt Internet of Things (IoT) technologies to enhance operational efficiency, customer engagement, and competitive advantage. However, this shift has significantly expanded their cybersecurity risk surface, exposing them to increasingly sophisticated threats while they remain constrained by limited budgets, technical capacity, and regulatory burdens.

In summary, this study contributes a practical, cost-conscious IoT security framework specifically tailored to the operational constraints of SMEs. Drawing upon well-established methodologies, such as STRIDE for threat modeling [41], CVSS for vulnerability scoring [44], and Bayesian inference for dynamic risk reassessment [45], the framework distills complex processes into a five-step model comprising asset classification, threat modeling, vulnerability assessment, risk prioritization, and mitigation planning. This structured yet adaptable approach empowers SMEs to identify and address critical IoT vulnerabilities in a scalable and resource-aware manner.

The framework's value was validated through a real-world case study involving a digitally enabled retail SME, where implementation led to a 42.1 % reduction in total vulnerabilities, a 65 % drop in critical issues, and measurable improvements in response time and employee security awareness. These outcomes underscore the framework's practical effectiveness and its ability to enhance cybersecurity posture

without imposing prohibitive costs or disruption to operations. By embedding regulatory considerations from GDPR [56] and the UAE's PDPL [58], the framework also supports SMEs in fulfilling legal obligations while improving their security maturity.

While the case study provides strong evidence of real-world applicability, it represents a single organizational context. As such, the findings may not fully generalize to SMEs in other sectors or regions. Future work should therefore focus on broadening the generalizability of this approach through multi-case studies across diverse industries and geographical settings. Sector-specific adaptations, for example, in healthcare, manufacturing, and agriculture, may further refine the framework's utility by aligning with domain-specific threat landscapes and regulatory contexts. Additionally, integrating artificial intelligence (AI) and machine learning (ML) for anomaly detection and predictive risk modeling offers promising avenues for enhancing responsiveness and precision in SME cybersecurity. Further research could also explore embedding this framework within modular testbed environments or extending its reach through integration with SIEM tools and automated log parsers. These enhancements would support real-time Bayesian parameter calibration and facilitate continuous, autonomous risk management.

Overall, this study bridges the gap between enterprise-scale cybersecurity models and SME feasibility, offering a robust, implementable pathway for improving IoT security resilience in resource-constrained environments.

CRediT authorship contribution statement

Samer Aoudi: Writing – original draft, Validation, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Hussain Al-Aqrabi:** Writing – review & editing, Visualization, Methodology, Investigation, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Framework Algorithms

Algorithm 2 provides a structured approach to classifying IoT assets within SME environments. Accurate asset classification is essential for understanding business-critical dependencies and for ensuring that security resources are focused where they matter most. This algorithm supports SMEs in developing a comprehensive asset inventory, capturing key metadata such as location, function, ownership, and criticality. It serves as the foundational input for subsequent threat modeling and risk prioritization processes within the proposed framework.

Algorithm 2
IoT Asset Classification for SMEs.

Require: IoT environment E with devices, networks, and applications
Ensure: Structured asset inventory I with criticality levels
I ←∅
for all asset a ∈ E **do**
Identify asset type: device, network, or software
Record metadata: location, function, dependencies, owner
Assign criticality level C(a) based on:
Impact on core operations
Data sensitivity
Service continuity dependencies
Add entry {a, type, metadata, C(a)}to I
end for
return I

Algorithm 3 outlines a systematic method for applying the STRIDE threat modeling framework to classified IoT assets. By assessing each asset against the six STRIDE categories, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, the algorithm helps identify specific threat scenarios that are relevant in the context of SME operations. This targeted threat mapping ensures that the risk assessment process is grounded in the actual exposure and function of each asset, rather than relying on generic threat assumptions.

Algorithm 3
STRIDE-Based Threat Modeling for IoT Assets.

Require: Asset inventory I with criticality scores and configurations
Ensure: Threat list T mapped to assets and threat categories
T ←∅
for all asset a ∈ *I* **do**
Retrieve asset characteristics: access interfaces, communication protocols
for all STRIDE category s ∈{Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege} **do**
Assess applicability of s to a using:
Known vulnerabilities
Exposure to external actors
Past incidents or threat intelligence
if s applicable **then**
Record threat t ←{a, s, impact level, justification}
Add t to T
end if
end for
end for
return T

Algorithm 4 describes a three-stage vulnerability assessment process suitable for SMEs. It combines automated scanning using tools like Nessus or OpenVAS with optional penetration testing for high-value or high-risk assets. The algorithm also supports structured documentation and categorization of vulnerabilities based on CVSS scores and exploitability levels. This ensures that the vulnerability data feeding into the risk prioritization step is both comprehensive and context-sensitive, enabling more informed and defensible security decisions.

Algorithm 4
Vulnerability Assessment for IoT Systems.

Require: IoT assets E, security tools (e.g., Nessus, OpenVAS)
Ensure: Consolidated vulnerability report V with CVSS scores
1: V ←∅
2: **for all** asset a ∈ E **do**
3: Perform vulnerability scan using automated tools
4: Extract raw findings: CVE identifiers, descriptions, CVSS base scores
5: **if** critical service or internet-facing **then**
6: Conduct targeted penetration testing for a
7: **end if**
8: **for all** vulnerability v found on a **do**
9: Classify v by:
10: Severity: CVSS ∈{Low, M edium, High, Critical}
11: Exploitability: ∈{Low, M edium, High}
12: Add {a, v, CVSS, exploitability, description}to V
13: **end for**
14: **end for**
15: **return** V

Appendix B. Vulnerability Scanning Configuration and Use Case Details

To enhance reproducibility and provide implementation-level detail, this appendix outlines the configuration parameters and specific use cases employed during the vulnerability assessment phase described in Sections 4.2 and 5.2.3.

B.1 Tools Used

- Nessus Essentials v10.5.1
- OpenVAS via Greenbone Security Assistant v22.4

B.2 Target Scope

- Devices scanned included IoT gateways, IP surveillance cameras, PoS terminals, and connected web-based interfaces.
- Internal scans were conducted over a segmented test VLAN with static IPs assigned for each IoT node.

B.3 Key Nessus Configuration

- Scan Template: “Advanced Scan”
- Plugin Families Enabled:
  - IoT Protocol Detection
  - Web Servers
  - General Plugins
  - SCADA
- Port Scanning:
  - TCP Full Connect Scan: Enabled
  - UDP Scan: Enabled (restricted to ports 53, 123, 161)
- Authentication: SSH credential-based scanning on PoS terminal
- Performance Settings:
  - Max simultaneous checks: 4
  - Max hosts per scan: 5

B.4 Key OpenVAS Configuration

- Scan Profile: “Full and fast”
- Timeouts: Increased to 120 s for embedded camera systems
- Log Level: Verbose
- Credentialed checks: Disabled (due to vendor restrictions on camera firmware)

B.5 CVSS Use Cases
Vulnerabilities were scored using CVSS v3.1 base scores from scan outputs. Example vectors:

- CVE-2022–22954 (PoS terminal input validation flaw):

- Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- CVSS Score: 9.8 (Critical)

- CVE-2021–36260 (Surveillance camera RCE):
  - Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - CVSS Score: 10.0 (Critical)
- Default credentials on IoT Gateway:
  - Vector: AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
  - CVSS Estimate: 7.4 (High), no CVE assigned; based on vendor advisory

These scores were directly used in the risk prioritization algorithm (Section 4.2) and in calculating static and Bayesian-adjusted risk scores (Section 5.3).

Appendix C. Estimated Effort and Budget for Framework Implementation in SMEs

This appendix outlines the estimated resource requirements for implementing the proposed IoT risk-based security framework in a typical SME environment. Estimates are based on a single-site deployment with fewer than 50 IoT-enabled assets and no dedicated cybersecurity team. Figures assume internal staff carry out most tasks, with optional external support for tool configuration or training.

C.1 Effort Estimate by Framework Component

- Asset Classification: 6–10 staff hours

  (IT administrator or operations manager maps devices and dependencies)

- Threat Modeling (STRIDE): 8–12 hours

  (Basic STRIDE mapping across 3–5 asset categories using checklists or templates)

- Vulnerability Assessment: 10–15 hours

  (Tool setup, scan execution, review of Nessus/OpenVAS output; includes re-scanning)

- Risk Prioritization: 6–8 hours

  (Matrix creation, CVSS lookup, optional Bayesian update for top 3 risks)

- Mitigation Planning and Implementation: 15–25 hours

  (Patch application, credential changes, segmentation, training delivery, testing)

Total Staff Effort Estimate: *45–70 hours*

C.2 Budget Estimate by Activity Category

- Open-Source Tools (OpenVAS, CVSS calculators): $0
- Commercial Tool (Optional: Nessus Pro license): $2990/year
- Training Resources (Basic awareness kit): $200–$500
- External Consultant Support (Optional): $1500–$3000 for tailored threat modeling or scan review

Estimated Budget Range: *$200 – $6500* depending on tool/license choices and external assistance.

C.3 SME Cost Optimization Notes

Most SMEs can minimize costs by:

- Using free versions of scanning tools (e.g., Nessus Essentials)
- Relying on publicly available STRIDE and CVSS documentation
- Delivering internal security awareness training using open resources (e.g., OWASP guides)
- Prioritizing mitigation actions with minimal operational disruption (e.g., disabling unused ports)

These estimates provide a practical benchmark to help SMEs plan framework adoption incrementally while staying within budget.

Data availability

The data that has been used is confidential.

References

[1] Transforma Insights, Global IoT Forecast Report, 2023-2033. https://tinyurl.com/549jrpsv, May 2024.

[2] H. Younis, N. Shbikat, O.M. Bwaliez, I. Hazaimeh, B. Sundarakani, An overarching framework for the successful adoption of IoT in supply chains, Benchmark. Int. J. (2025).

[3] L. Atzori, A. Iera, G. Morabito, Understanding the internet of things: definition, potentials, and societal role of a fast-evolving paradigm, Ad. Hoc. Netw. 56 (2017) 122–140, https://doi.org/10.1016/j.adhoc.2016.12.004.

[4] S. Jayadatta, A study on latest developments in artificial intelligence (AI) and internet of things (IoT) in current context, J. Appl. Inf. Sci. 11 (2) (2023) 21–28.

[5] M. Satyanarayanan, The emergence of edge computing, Computer (Long. Beach. Calif.) 50 (1) (2017) 30–39, https://doi.org/10.1109/MC.2017.9.

[6] H. Al-Aqrabi, L. Liu, R. Hill, N. Antonopoulos, A multi-layer hierarchical inter-cloud connectivity model for sequential packet inspection of tenant sessions accessing BI as a service, in: Proc. 2014 IEEE Int. Conf. High Perform. Comput. Commun. (HPCC), 2014 IEEE 6th Int. Symp. Cyberspace Safety Security (CSS), 2014 IEEE 11th Int. Conf. Embedded Softw. Syst. (ICESS), 2014, pp. 498–505.

[7] H. Al-Aqrabi, R. Hill, P. Lane, H. Aagela, Securing manufacturing intelligence for the industrial internet of things, in: Proc. 4th Int. Congr. Inf. Commun. Technol. (ICICT), London, U.K. 2, 2019, pp. 267–282.

[8] M. Wazid, A.K. Das, S. Shetty, P. Gope, J. Rodrigues, Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap, IEEE Access, 2020, https://doi.org/10.1109/ACCESS.2020.3047895, 1-1.

[9] L.A. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider, IoT Privacy and security: challenges and solutions, Appl. Sci. 10 (12) (2020) 4102.

[10] M. Azrour, J. Mabrouki, A. Guezzaz, A. Kanwal, Internet of things security: challenges and key issues, Secur. Commun. Netw. 2021 (1) (2021) 5533843.

[11] B.K. Mohanta, D. Jena, U. Satapathy, S. Patnaik, Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet of Things 11 (2020) 100227.

[12] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Netw. 76 (2015) 146–164, https://doi.org/10.1016/j.comnet.2014.11.008.

[13] M.M. Cherian, S.L. Varma, Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks, Int. J. Comp. Netw. Inf. Secur. 14 (1) (2022) 52.

[14] E. Fernandes, J. Jung, A. Prakash, Security analysis of emerging smart home applications, in: IEEE Symposium on Security and Privacy, 2016, pp. 636–654, https://doi.org/10.1109/SP.2016.44.

[15] OWASP, OWASP IoT Top Ten 2018, Open Web Application Security Project. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10, 2018.

[16] I. Kuzminykh, B. Ghita, J.M. Such, The challenges with Internet of Things security for business, in: International Conference on Next Generation Wired/Wireless Networking, Springer International Publishing, Cham, August 2021, pp. 46–58.

[17] N.I.S.T. NIST, Special Publication 800-183: Networks of 'Things, National Institute of Standards and Technology, 2016, https://doi.org/10.6028/NIST.SP.800-183. https://csrc.nist.gov/pubs/sp/800/183/final.

[18] C.I. Cybersecurity, Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, 2018.

[19] ISO/IEC, ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks, 4th edition. https://www.iso.org/standard/80585.html, October 2022.

[20] ENISA, Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot, 2017.

[21] ENISA, Guidelines for Securing the Internet of Things. https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things, 2020.

[22] OWASP Foundation, OWASP Internet of Things Project, Retrieved June 8, 2025, from, https://owasp.org/www-project-internet-of-things/, 2018.

[23] A. Chidukwani, S. Zander, P. Koutsakis, A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations, IEEE Access 10 (2022) 85701–85719.

[24] F. Almeida, J.D. Santos, J.A. Monteiro, Challenges in cybersecurity: lessons from the ISO/IEC 27001 and ISO/IEC 27005 standards, J. Glob. Inf. Manage. 27 (4) (2019) 1–15.

[25] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.

[26] European Union, General Data Protection Regulation (EU) 2016/679, Official Journal of the European Union, 2016, p. L119. http://data.europa.eu/eli/reg/2016/679/oj.

[27] M. Saleh, T. Kdour, A. Ferrah, H. Ahmed, S. AP, R. Azzawi, A. Ali, Health wearable IoT (WIoT) technology devices security and privacy vulnerability analysis, in: 2022 8th International Conference on Information Technology Trends (ITT), IEEE, 2022, pp. 16–20.

[28] M. Aqeel, F. Ali, M.W. Iqbal, T.A. Rana, M. Arif, M.R. Auwul, A review of security and privacy concerns in the internet of things (IoT), J. Sens. (1) (2022) 5724168, 2022.

[29] P. Zheng, H. Wang, Z. Sang, R.Y. Zhong, Y. Liu, C. Liu, X. Xu, Smart manufacturing systems for Industry 4.0: conceptual framework, scenarios, and future perspectives, J. Manuf. Syst. 56 (2020) 1–12.

[30] M.M. Queiroz, S.C.F. Pereira, R. Telles, M.C. Machado, Industry 4.0 and digital supply chain capabilities: a framework for understanding digitalisation challenges and opportunities, Benchmark. Int. J. 28 (5) (2019) 1761–1782.

[31] E. Lee, Y.D. Seo, S.R. Oh, Y.G. Kim, A survey on standards for interoperability and security in the internet of things, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1020–1047.

[32] R.M. Czekster, P. Grace, C. Marcon, F. Hessel, S.C. Cazella, Challenges and opportunities for conducting dynamic risk assessments in medical IoT, Appl. Sci. 13 (13) (2023) 7406.

[33] H. Taherdoost, Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview, Electronics (Basel) 11 (14) (2022) 2181.

[34] M. Alauthman, A. Almomani, S. Aoudi, A. al-Qerem, A. Aldweesh, Automated vulnerability discovery generative AI in offensive security, in: A. Almomani, M. Alauthman (Eds.), Examining Cybersecurity Risks Produced by Generative AI, IGI Global Scientific Publishing, 2025, pp. 309–328, https://doi.org/10.4018/979-8-3373-0832-6.ch013.

[35] L. Kong, J. Tan, J. Huang, G. Chen, S. Wang, X. Jin, P. Zeng, M. Khan, S. Das, Edge-computing-driven Internet of Things: a Survey, ACM Comput. Surv. 55 (8) (August 2023) 41, https://doi.org/10.1145/3555308. Article 174pages.

[36] O. Aouedi, T.H. Vu, A. Sacco, D.C. Nguyen, K. Piamrat, G. Marchetto, Q.V. Pham, A survey on intelligent Internet of Things: applications, security, privacy, and future directions, IEEE Commun. Surv. Tutor. (2024).

[37] I. Brass, L. Tanczer, M. Carr, M. Elsden, J. Blackstock, Standardising a moving target: the development and evolution of IoT security standards. Living in the Internet of Things: Cybersecurity of the IoT-2018, IET, Stevenage, UK, 2018, p. 24.

[38] J. Webb, D. Hume, Campus IoT collaboration and governance using the NIST cybersecurity framework. Living in the Internet of Things: Cybersecurity of the IoT-2018, IET, March 2018, pp. 1–7.

[39] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2702–2733.

[40] A. Shostack, Threat modeling: Designing for Security, John Wiley & Sons, 2014.

[41] Microsoft, The STRIDE Threat Model, Microsoft Security Development Lifecycle, 2005.

[42] T. UcedaVelez, M.M. Morana, Risk Centric Threat modeling: Process for Attack Simulation and Threat Analysis, Wiley, 2015.

[43] Tenable, Nessus vulnerability scanner, Tenable Network Security (2021).

[44] OpenVAS, Open Vulnerability Assessment System, Greenbone Networks, 2021.

[45] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, K. Stoddart, A review of cyber security risk assessment methods for SCADA systems, Comput. Secur. 56 (2016) 1–27.

[46] I. Lee, Internet of Things (IoT) cybersecurity: literature review and IoT cyber risk management, Future Internet 12 (9) (2020) 157.

[47] E. Bell, B. Harley, A. Bryman, Business Research Methods, Oxford University Press, 2022.

[48] J.W. Creswell, J.D. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, Sage Publications, 2017.

[49] Keele, S., Guidelines for performing systematic literature reviews in software engineering (Vol. 5), Technical report, ver. 2.3, EBSE Technical Report, 2007.

[50] M. Casula, N. Rangarajan, P. Shields, The potential of working hypotheses for deductive exploratory research, Qual. Quant. 55 (5) (2021) 1703–1725.

[51] R.K. Yin, Case Study Research and applications: Design and Methods, Sage Publications, 2017.

[52] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and other botnets, Computer (Long. Beach. Calif.) 50 (7) (2017) 80–84.

[53] V. Braun, V. Clarke, Using thematic analysis in psychology, Qual. Res. Psychol. 3 (2) (2006) 77–101.

[54] Manubolu, G.S., A comprehensive security testing framework for PLC-based industrial automation, 2024.

[55] Ramya, G., & Srinivasagan, K.G., Integrating cybersecurity threats into smart manufacturing: best practices and frameworks, In Artificial Intelligence Solutions For Cyber-Physical Systems, pp. 120–138, Auerbach Publications.

[56] P. Voigt, A. Von dem Bussche, The EU General Data Protection Regulation (gdpr), A practical Guide, 1st ed., 10, Springer International Publishing, Cham, 2017, pp. 10–5555.

[57] Flores, D.A., & Perugachi, R., A GDPR-compliant risk management approach based on threat modelling and ISO 27005, arXiv preprint arXiv:2306.04783, 2023.

[58] United Arab Emirates Government, Federal decree-law no. 45 of 2021 on the protection of personal data (PDPL). https://u.ae/en/about-the-uae/digital-uae/data/data-protection-law, 2021.

[59] E.H.N. Safitri, H. Kabetta, Cyber-risk management planning using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization), in: 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), IEEE, August 2023, pp. 332–338.