**Title**

"Exploring IoT Device Vulnerabilities in Small and Medium-Sized Enterprises: Challenges and Mitigation Strategies"

# Abstract

(200 words)

# Introduction

Internet of Things or IoT devices are widely available and used in settings from the home to the large enterprise. Small and medium sized enterprises are no exception to enhancing their business by using IoT devices. This can come in the form of integrating:

* Smart speakers (Amazon Alexa, Google Nest)
* Smart lighting (Philips Hue)
* Smart thermostats (Nest, Philips Hue)
* IoT security camera systems (Ring, Hikvision)
* Smart door locks and buzzer systems (August Smart Lock, Butterfly MX Smart Intercom)
* Smart security alarms (SimpliSafe, ADT Smart sensors)
* Pay terminals (Square terminals, Clover POS)
* Smart signage (Samsung smart signage, LG WebOS)

However, the integration of these technologies brings its own set of challenges, particularly when maintaining network security. IoT devices while extremely useful can also be viewed as a weak point within a network. This problem is amplified through the fact that small to medium sized enterprises do not have the resources at hand to have an IT professional integrating and monitoring their deployment and use. IoT devices are inherently vulnerable due to their reliance on legacy protocols, weak authentication mechanisms, and limited computational resources (Liao et al., 2020, p. 120331) This leaves SMEs exposed to cyber threats such as Distributed Denial of Service (DDoS) attacks, data breaches, and ransomware. For instance, Liao et al. (2020) highlighted that many IoT systems lack robust security frameworks, making them attractive targets for attackers. Adding to this issue, SMEs often fail to implement basic cybersecurity practices like firmware updates, network segmentation, or secure authentication measures, which are essential to reduce these risks.

The lack of interest for IoT security in SMEs stems from a gap in current research. While IoT vulnerabilities have been extensively studied in residential and large enterprise settings, SMEs remain underexplored (Masyhur et al., 2022, p. 17)​ Existing frameworks are either too generalized or tailored the home or for large enterprises this leaves SMEs without practical guidance to safeguard their networks. This research aims to address this critical gap by developing a practical, SME-specific guide to safely integrate IoT devices into business networks. Building off of existing literature, this proposal aims to show the importance and lack of research into this particular niche of IoT enabled systems without proper security.

**Literature review**

# The Internet of Things or iot refers to a network of interconnected devices that communicate data through the Internet. Due to the ease of use affordability and the growing range of products available, iot devices have been adopted into more and more small and medium sized enterprises. These devices provide businesses with professional grade solutions such as automated lighting, smart security systems, Intercom systems, pay terminals. These systems that may be designed for a residential setting come with user friendly installation. According to (Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations, 2019) “ The negligence of security considerations in IOT design leads to vulnerabilities such as unauthorised access, unprotected data transmission, and malicious manipulation of device firmware.” This paired with a standard network configuration provided by an ISP that doesn’t employ best practices such as network segmentation or have changed default passwords can create a sizeable attack surface. According to a survey 55% of small and medium sized enterprises lac and up to date cyber risk strategy or a defined strategy for cyber security at all (Sukumar, Mahdiraji and Jafari‐Sadeghi, 2023). One reason this occurs Is that SMEs Can usually make do with off-the-shelf solutions for their it needs. They do not have the resources or feel the need to hire in IT professionals to create a secure network for business operations. This creates an environment where you have targets with enough money to steal but these targets are ignorant to the fact that they are vulnerable.

Many affordable IOT devices marketed towards consumers sacrifice security to reduce costs and improve usability for the user. Lack of know-how, together with the hectic approach to the design of new products and the need to compress costs and time-to-market have led to the commercialization of IoT products where security is either neglected or treated as an afterthought (Meneghello *et al.*, 2019). One of the most common attacks done to home IoT devices is unauthorized access. Devices with unchanged default credentials are particularly vulnerable, allowing attackers to infiltrate networks or monitor device activity remotely (Meneghello et al., 2019). Privacy risks are also a big worry, as shown by smart speakers and voice assistants inadvertently recording sensitive conversations without user consent (Davis, Mason & Anwar, 2020). These risks show the lack of adequate security practices in consumer devices. Home networks with IoT devices face challenges that are similar those encountered by small and medium-sized enterprises (SMEs). Both rely heavily on plug-and-play solutions for their ease of use, this leaves them exposed to cyber threats (Davis, Mason & Anwar, 2020). The customers who buy these devices do not want to hire external IT professionals to set up a home network that has these devices implemented correctly. This can be due to not wanting to spend the money or not realising the way they are exposing themselves. To address these vulnerabilities, manufacturers and users alike must adopt stronger security measures to ensure devices are equipped with secure configurations by default, providing regular firmware updates, and educating users on basic cybersecurity practices (Neshenko et al., 2019).

Large IOT ecosystems bring with them a unique set of security challenges. These organisations often have a range of iot devices built into the production line such as sensors and automated manufacturing systems, this creates a large attack surface (Puche Rondon et al., 2022). The fact that in an enterprise setting these devices are likely interconnected if one is breached then there is a strong possibility that a breach can spread throughout the network (Puche Rondon et al., 2022). Some of the threats that enterprise IoT devices have to deal with are Distributed Denial of Service (DDoS) attacks and insider threats. These attacks often exploit supply chain vulnerabilities, where compromised devices from third-party vendors can introduce risks to the broader network (Meneghello et al., 2019). . DDos attacks occur when the Internet of things device has been incorporated into a botnet, this hiders the performance of the device An example of this is the Mirai botnet attack, which used insecure IoT devices to launch a DDoS attack on the DNS provider Dyn. This attack disrupted major online services around the world, it highlights how weak credentials and poor device security can have devastating consequences for enterprises (Neshenko et al., 2019). Large enterprises are better funded and more aware of these issues than smaller organizations. This leads the larger enterprises to invest in adequate security measures as they often have dedicated IT departments who are aware of the risks. Larger enterprises often have the funding integrate enterprise-grade solutions like network segmentation and endpoint monitoring to reduces risks. With that being said these measures do not guarantee enterprises will not experience a breach, which carries financial and operational losses while also hurting the reputation of the company(Rajendran et al., 2019).

Home IoT systems and enterprise IoT environments have a number of vulnerabilities in common, especially concerning authentication and firmware management. Both are vulnerable to problems like weak default passwords, outdated firmware, and poor network segmentation, which makes them ideal targets for cyberattacks. The vulnerabilities we've seen point to a clear need for better security measures in IoT ecosystems, no matter their size (Meneghello et al., 2019). However, the types of threats and the resources at hand to address them differ between the two situations. In home IoT settings, the absence of specialised IT support and dependence on easy-to-use devices often lead to security being neglected or inadequately addressed. Devices designed for everyday consumers often trade off strong security for affordability and simplicity, making them susceptible to breaches. In the same way, small and medium-sized enterprises frequently use consumer-level IoT devices to save money, putting themselves at risk just like regular home users (Davis, Mason & Anwar, 2020). For instance, small and medium-sized enterprises might unintentionally use devices that come with default settings, which often do not include encryption or access control, increasing their vulnerability to threats. In contrast, enterprise IoT systems gain advantages from dedicated IT teams and bigger budgets, allowing them to adopt sophisticated security measures like network segmentation and endpoint monitoring. Enterprises encounter distinct challenges, such as the complexity of securing different and large IoT ecosystems, along with the risks tied to supply chain vulnerabilities (Puche Rondon et al., 2022). Small and medium-sized enterprises often don't have the necessary resources, which makes them more susceptible, even though many risks are common among businesses. Studies on IoT vulnerabilities have typically concentrated on home and enterprise systems, yet SMEs are often overlooked even though they face distinct challenges. They depend on everyday devices and have tight budgets, which means they need customised security solutions that fit their unique challenges, helping to fill the gaps in current IoT security frameworks (Meneghello et al., 2019).

Small and medium-sized enterprises (SMEs) are ideal targets for cyberattacks. This is because they rely on IOT devices Designed for use in the home do not have the required network security for an enterprise, another reason is that they do not employ IT professionals as the quick and easy nature of these devices means that they feel they do not require any further security measures. One of the most common types of breaches is unauthorised access to IoT devices. Many SMEs fail to update default credentials or implement strong authentication mechanisms, this leaves devices vulnerable to attackers who can use these flaws to gain access sensitive data or disrupt operations (Neshenko et al., 2019). This lack of basic security highlights the need for SMEs to implement appropriate security measures. Malware, including ransomware, is another significant vulnerability for IoT breaches in SMEs, as it targets unpatched or outdated devices. This is particularly relevant to SMEs who rarely have a dedicated IT department to ensure all devices are up to date and secure. These attacks can lock SMEs out of critical systems and demand large payouts to restore access, crippling business operations (Rajendran et al., 2019). These breaches cause financial losses and damage to a business’s reputation customers and partners lose trust in the affected company's ability to protect their data. The Mirai botnet attack, which targeted IoT devices with weak passwords, demonstrated how vulnerable devices could be co-opted into massive Distributed Denial of Service (DDoS) attacks. While this attack primarily targeted larger networks, SMEs with compromised IoT devices frequently serve as entry points, allowing attackers to expand their operations (Meneghello et al., 2019). The consequences of IoT breaches for SMEs include downtime and financial costs. The cost of recovery, which includes system restoration and legal fees, can be expensive for resource-constrained SMEs (Rajendran et al. 2019). These factors highlight the importance of SMEs implementing security measures as they integrate these devices.

Even though IoT security is a growing area of research, the specific needs of Small and Medium-sized Enterprises (SMEs) are still not being given enough attention. Most studies tend to focus on larger companies or consumer IoT setups. For example, frameworks like those from NIST or ENISA are designed for big companies with lots of resources and often don’t take into account the financial and technical constraints SMEs face (Sukumar, Mahdiraji & Jafari-Sadeghi, 2023). This is a serious issue because SMEs are often an easy target. Hackers know they have fewer defenses, making them an easy target and a stepping stone to attack bigger organizations. To add to that many SMEs rely on consumer-grade IoT devices, which are designed for convenience rather than security. (Khan et al., 2022). This specific challenge is rarely explored in the existing literature.

Another big problem is the lack of affordable security options for SMEs. Most tools on the market are either too expensive or too complicated for small businesses to use. This leaves them relying on basic security measures that just don’t cut it against more advanced threats (Rajendran et al., 2019).

Human error is a massive issue that often gets overlooked. A lot of breaches come down to employees not knowing how to use the technology securely. But despite this, there’s hardly any research on how proper training could help SMEs tackle this problem (Davis, Mason & Anwar, 2020). Addressing this would go a long way toward giving smaller businesses a fighting chance against the growing wave of IoT-related threats.

The research approach for this project is designed to investigate the vulnerabilities posed by Internet of Things (IoT) devices in Small and Medium-Sized Enterprises (SMEs). The focus is on identifying specific risks, comparing these vulnerabilities to those in home and in large enterprises, and proposing user friendly security solutions for SMEs. This section outlines the research questions, methodology, tools, and expected outcomes in detail.

**Research Approach**

**Research Questions**

The study aims to address the following research questions:

1. **What are the key IoT vulnerabilities in SMEs?**  
   This question seeks to identify the most common security risks associated with IoT devices in SMEs are.
2. **How do these vulnerabilities differ from those in home and enterprise IoT systems?**  
   This question compares the challenges faced by SMEs with other environments to highlight their unique position.
3. **What practical measures can SMEs adopt to mitigate these vulnerabilities?**  
   This question aims to develops a plug and play, cost-effective, and robust solution for SMEs to secure their IoT devices.

**Methodology**

The research employs a mixed-methods approach, integrating qualitative and quantitative methods to provide a comprehensive understanding of IoT vulnerabilities in SMEs. This is essential in order to prototype a solution.

1. **Systematic Review of Existing Literature**
   * **Objective**: To establish a foundation of knowledge on IoT vulnerabilities across home, enterprise, and SME contexts.
   * **Process**:
     + Conduct database searches (e.g., IEEE Xplore, ACM Digital Library, SpringerLink) for peer-reviewed journal articles and industry reports published in the last 5–7 years.
     + Use keywords such as "IoT vulnerabilities," "SME cybersecurity," and "IoT device security."
     + Categorize findings into themes, such as common vulnerabilities, mitigation strategies, and SME-specific gaps.
2. **Case Studies of SMEs**
   * **Objective**: To analyze real-world IoT deployments in SMEs and identify vulnerabilities and security practices.
   * **Process**:
     + Identify 3–5 SMEs using IoT devices in different industries (e.g., retail, healthcare, manufacturing).
     + Conduct semi-structured interviews with SME stakeholders to gather qualitative data on their IoT implementations and perceived challenges.
     + Use tools like Wireshark and Metasploit (with consent) to perform non-invasive network vulnerability scans and analyze risks.
3. **Survey of SMEs**
   * **Objective**: To quantify the state of IoT security in SMEs and validate findings from case studies.
   * **Process**:
     + Design a survey with structured questions addressing:
       - Types of IoT devices used.
       - Existing security practices (e.g., firewalls, network segmentation).
       - Experiences with IoT-related breaches.
       - Budget allocation for IoT security.
     + Distribute the survey via SME networks, industry associations, and LinkedIn groups.
     + Analyze responses using statistical tools to identify trends and gaps.
4. **Prototype Testing and Validation**
   * **Objective**: To develop and test a "security box" prototype tailored for SMEs.
   * **Process**:
     + Design a multi-functional device combining firewall, intrusion detection/prevention systems (IDS/IPS), network monitoring, and secure Wi-Fi access.
     + Simulate an SME network environment with common IoT devices such as smart locks, cameras, and payment terminals.
     + Test the prototype against simulated attacks (e.g., unauthorized access, malware injection) and measure its effectiveness.

**Materials and Tools**

To conduct the research effectively, the following resources will be utilized:

1. **IoT Devices for Testing**
   * Examples include smart cameras (e.g., Ring), locks (e.g., August Smart Lock), and payment terminals (e.g., Square).
   * These devices represent typical IoT implementations in SMEs.
2. **Vulnerability Assessment Tools**
   * **Wireshark**: For packet analysis and detecting abnormal traffic patterns.
   * **Nmap**: For identifying open ports and vulnerable devices.
   * **Metasploit**: For simulating attacks to evaluate the resilience of IoT networks.
   * **ESP32 marauder/ Flipper zero combination**: to showcase portability, subtlety of attacks
3. **Survey and Interview Platforms**
   * Tools like Google Forms and Typeform will be used to collect survey responses.
   * Zoom or in-person interviews will be conducted for case studies.
4. **Prototyping Hardware and Software**
   * Raspberry Pi or similar devices to create a "security box" prototype.
   * Open-source software like pfSense or OPNSense for firewall and IDS/IPS functionality.
5. **Analytical Tools**
   * **Excel or SPSS**: For survey data analysis.
   * **Tableau**: For creating visualizations of survey and case study results.

# Conceptual Model

# Potential Outcomes

The research outlined aims to produce tangible outcomes that address IoT vulnerabilities faced by Small and Medium-sized Enterprises (SMEs). The expected deliverables are categorized into practical tools, actionable insights, and contributions to research, which collectively aim to bridge the gap between existing IoT security frameworks and the specific needs of SMEs.

1. A Practical Guide for SMEs

One of the primary outputs will be a detailed guide to help SMEs integrate IoT devices securely into their operations. This guide will include step-by-step instructions on implementing affordable and effective security measures tailored to resource-constrained organizations. Specific recommendations will focus on:

Device Configuration: Ensuring default credentials are changed, and encryption is enabled.

Network Security: Implementing basic segmentation through VLANs and using firewalls for better traffic control.

Firmware Management: Establishing protocols for regular updates to minimize vulnerabilities.

Employee Training: Addressing human error through targeted awareness programs to improve security hygiene.

The guide will be easy to understand, even for non-technical users, and adaptable across different SME industries.

2. Survey and Case Study Insights

The survey and case studies will generate a comprehensive understanding of how SMEs adopt and manage IoT technologies. Insights will include:

IoT Adoption Trends: Identifying the most commonly used devices and how SMEs incorporate them into their workflows.

Security Gaps: Highlighting vulnerabilities such as weak authentication, lack of encryption, and minimal network segmentation.

Challenges Faced: Documenting the resource limitations, knowledge gaps, and reliance on consumer-grade IoT devices.

Industry Comparisons: Comparing practices across sectors like retail, healthcare, and manufacturing to identify industry-specific risks.

These insights will serve as a critical reference for SMEs and researchers, providing real-world examples of both effective and ineffective IoT security practices.

3. Validated Prototype

The security box prototype will be a central outcome of the project, showcasing a practical, cost-effective solution for SMEs. Designed with affordability and usability in mind, the prototype will:

Combine multiple security functions such as a firewall, intrusion detection/prevention system (IDS/IPS), and secure Wi-Fi.

Support customizable features like VLANs for network segmentation and WPA3 encryption for better wireless security.

Be tested in a simulated SME network environment with common IoT devices, measuring its performance against attacks like malware injection and unauthorized access.

The prototype's performance will be evaluated using metrics such as detection rates, response times, and usability. Its validation will demonstrate that SMEs can deploy effective security solutions without significant financial or technical overhead.

4. Contributions to Research

This research will address critical gaps in existing IoT security literature by focusing on the specific needs of SMEs. Contributions will include:

Identification of Gaps: Highlighting why current security frameworks designed for enterprises or home environments are not suitable for SMEs.

Tailored Solutions: Proposing practical and scalable measures that align with SMEs' budgetary and technical constraints.

Future Research Foundations: Providing a baseline for further studies into SME-specific IoT security challenges and solutions.

The research will also establish an empirical understanding of the risks SMEs face, encouraging policymakers and industry leaders to develop more inclusive standards.

5. Long-Term Impact

The outcomes of this project aim to create a meaningful, long-term impact by equipping SMEs with the knowledge and tools needed to safeguard their IoT systems. In doing so, the research not only strengthens individual businesses but also enhances the overall security of supply chains and ecosystems where SMEs operate. By addressing the vulnerabilities in SMEs, the project contributes to a more resilient digital economy, ensuring that smaller organizations are not left behind in the race to secure IoT deployments.

# References

​ Davis, B.D., Mason, J.C. and Anwar, M. (2020) 'Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study,' *IEEE Internet of Things Journal*, 7(10), pp. 10102–10110. https://doi.org/10.1109/jiot.2020.2983983.

*Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations* (2019) *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*. journal-article, pp. 2702–2703. https://doi.org/10.1109/COMST.2019.2910750.

Feng, X. *et al.* (2023) *Detecting Vulnerability on IoT Device Firmware: A Survey*, *IEEE/CAA J. Autom. Sinica*, pp. 25–41. https://doi.org/10.1109/JAS.2022.105860.

Khan, A. *et al.* (2022) 'Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends,' *Complex & Intelligent Systems*, 8, pp. 3919–3941. https://doi.org/10.1007/s40747-022-00765-y.

Liao, B. *et al.* (2020) 'Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review,' *IEEE Access*, 8, pp. 120331–120350. https://doi.org/10.1109/access.2020.3006358.

Masyhur, Z. *et al.* (2022) *Internet of Things (IoT): Security, Threats and Countermeasures*, *JOURNAL SHIFT*. journal-article, pp. 15–17.

Meneghello, F. *et al.* (2019) *IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices*, *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2019.2935189.

Rajendran, G. *et al.* (2019) *Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures*.

Rondon, L.P. *et al.* (2021) 'Survey on Enterprise Internet-of-Things systems (E-IoT): A security perspective,' *Ad Hoc Networks*, 125, p. 102728. https://doi.org/10.1016/j.adhoc.2021.102728.

Sukumar, A., Mahdiraji, H.A. and Jafari‐Sadeghi, V. (2023) 'Cyber risk assessment in small and medium‐sized enterprises: A multilevel decision‐making approach for small e‐tailors,' *Risk Analysis*, 43(10), pp. 2082–2098. https://doi.org/10.1111/risa.14092.