Title

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

Abstract

Small and Medium-Sized Enterprises (SMEs) are increasingly turning to Internet of Things (IoT) devices to enhance their operations; however, this shift brings about considerable cybersecurity challenges. IoT devices, created to prioritise user convenience and cost-effectiveness, frequently fall short in terms of strong security protocols. The combination of these vulnerabilities and the limited resources of SMEs, along with the lack of dedicated IT professionals, positions them as attractive targets for cyberattacks, including unauthorised access, ransomware, and Distributed Denial of Service (DDoS) attacks. In contrast to large enterprises that have comprehensive cybersecurity systems in place, small and medium-sized enterprises face budgetary and technical challenges. As a result, they often depend on consumer-grade devices that come with default credentials and outdated firmware. This study highlights a significant gap in IoT security frameworks that are specifically designed for small and medium-sized enterprises, which are frequently neglected in comparison to residential or large enterprise settings. This project seeks to identify the unique vulnerabilities that SMEs encounter by conducting systematic literature reviews, case studies, and surveys, while also proposing practical and cost-effective solutions. This project will involve the development and testing of a prototype for a "security box" utilising open-source tools, aimed at offering small and medium-sized enterprises (SMEs) accessible and scalable security solutions.

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 questions we chose were decided on as they were able to identify the vulnerabilities within SMEs in relation to IoT, compare them to larger enterprise and home vulnerabilities and provide a solution to these problems. The first research question is “What are the key IoT vulnerabilities in SMEs?” This question will help us identify what are the most common vulnerabilities that face SMEs that use IoT devices. The second question is “How do these vulnerabilities differ from those in home and enterprise IoT systems?” By comparing the vulnerabilities of all the spectrums of IoT devices we are able to identify similarities and differences between the systems with regards to design, implementation and security practices. This is essential in order to produce a practical countermeasure. The last question is “What practical measures can SMEs adopt to mitigate these vulnerabilities?” By developing a practical countermeasure that is secure, easy to use and cost effective. This question aims to produce a solution to the bulk of SME network security.

Methodology

The research will consist of a systematic review of existing literature, Case studies of SMEs, Surveys of SMEs and the design and testing of a practical solution. This will employ a mixed-methods approach, integrating qualitative and quantitative methods to provide a well-rounded understanding of IoT vulnerabilities in SMEs. With this approach there will be sufficient data to answer all the research questions. The Systematic Review of Existing Literature objective is to establish a database of IoT vulnerabilities across home, enterprise, and SME contexts. We will do this by conducting database searches for peer revied journal articles and industry reports that were published in the last 5-7 years. Refining our search by using Google scholar and compiling these results in a web-based tool called Research Rabit to organise and suggest similar work. When searching for sources using keywords such as IoT vulnerabilities, SME cybersecurity and IoT device security helps to categorize the findings into specific groups. When conducting the Case Studies of SMEs our objective is to analyse real-world IoT deployments in SMEs and identify vulnerabilities and security practices. We aim to do this by identifying 3–5 SMEs using IoT devices in different industries that we can conduct a case study on. When we have established the subjects for study we will conduct semi-structured interviews with SME operators to gather qualitative data on their IoT implementations and perceived challenges. Tools like Wireshark and Metasploit will be used with consent to perform non-invasive network vulnerability scans and analyse risks. Secondary devices such as the Flipper Zero and a ESP32 marauder device will be used to preform the actions of Wireshark and Metasploit in a similar manner to prove the ease, portability and low barrier to entry of an attack. With the survey of SMEs our objective is to confirm the state of IoT security in SMEs and validate findings from case studies. We will conduct this by designing a survey that identifies how many use IoT device, do they have any network security implemented, do they have a budget for cyber security. This survey will be distributed through online emails and in person questions to local businesses. Prototype Testing and Validation is done in order to to develop and test a "security box" prototype tailored for SMEs. Developing a custom network security box for small and medium-sized enterprises (SMEs) can be done by using single-board computers like the Raspberry Pi or more powerful alternatives such as the ZimaBoard. These devices offer the flexibility to integrate essential security functions including firewall protection, intrusion detection systems (IDS), and virtual private network (VPN) capabilities into a compact, cost-effective solution. This is done by using open-source software tailored for these platforms, SMEs can deploy a customizable security box that addresses their specific network protection needs without the expense associated with commercial all-in-one systems.

Materials and Tools

To conduct the research effectively, we will need to use Iot Devices for testing, vulnerability testing tools, survey services and interview platforms for case studies, hardware to build prototype and analytical tools to analyse data collected. The IoT devices that will be tested will include a Ring doorbell, smart locks, and a payment terminal. These devices will represent typical IoT implementations in SMEs. Vulnerability assessment tools will include 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. In order to conduct a large enough survey we will need services such as Google Forms and Type form that will be used to collect survey responses. Zoom or in-person interviews will be conducted for case studies. To design a counter measure prototyping hardware and software will consist of Raspberry Pi or similar devices to create a "security box" prototype. We will use open-source software like pfSense or OPNSense for firewall and IDS/IPS functionality. In order to properly analyse the collected data we will use Excel or SPSS for statistical analysis of survey data and tableau for creating visualizations of survey and case study results.

Conceptual Model

Potential Outcomes

The outcomes of this research will help identify the most common IoT vulnerabilities in SMEs and offer practical solutions specifically designed for their needs. We expect to find that SMEs face critical issues like weak authentication, outdated firmware, and poor network segmentation, which make them easy targets for cyberattacks. Since SMEs often rely on consumer-grade IoT devices and lack the resources for enterprise-level security, they are more exposed to threats. By comparing vulnerabilities in SMEs with those in home and enterprise IoT systems, we will identify similarities, like reliance on default settings and poor management practices, and key differences, such as the absence of dedicated IT teams or budgets in SMEs. This will give a clear picture of how SME challenges fit into the wider IoT security problem and why targeted solutions are so necessary. The surveys and case studies will confirm just how insecure IoT setups are in SMEs. Trends we expect to see include unchanged default passwords, devices running without firmware updates, and very little awareness of IoT security risks. Many SMEs probably use off-the-shelf IoT devices with no extra security measures, leaving huge gaps in their defenses. By collecting this kind of real-world data, we can back up the idea that SMEs need simple and affordable tools to secure their networks. As part of this research, we will also create and test a "security box" prototype to address these issues. Using devices like the Raspberry Pi or ZimaBoard, we can build a practical, low-cost solution that SMEs can use to protect their IoT systems. The prototype will likely include features like network segmentation, intrusion detection, and secure Wi-Fi, all designed to work effectively in SME environments without requiring IT expertise. In addition, this research will create clear, step-by-step security guidelines for SMEs. These will cover basic actions like changing default passwords, updating firmware regularly, segmenting networks, and providing staff with basic training on cybersecurity. These guidelines will give SMEs simple and effective ways to improve their IoT security without needing a lot of time or money. Beyond the practical tools and recommendations, this research will also contribute to the academic field by pointing out gaps in current IoT security frameworks, especially how they overlook the specific needs of SMEs. It will suggest new areas for research, such as looking into how staff training can reduce IoT risks in small businesses. This study will ultimately help

SMEs use IoT technology without constantly worrying about cybersecurity threats. It will show how they can protect their networks in a way that's both affordable and easy to manage. The results will also have broader implications, raising awareness among SME owners about the importance of IoT security and encouraging them to take action.

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.