Section 1

Timothy Udumula

Department of Information Technology, University of Maryland Baltimore County

CYBR 624 (Spring 2025): Cybersecurity Project

Dr. Behnam Shariati

March 14, 2025

Introduction

The usage of the internet has transformed compared to its conception. The users of the internet are impacted by the widespread of the internet because it provides pathways for newer technologies to be utilized, thus making it more efficient. The capabilities of technology that can be mentioned as highly preferred are usability and flexibility, which have been pivotal issues regarding the reliance on technology. Now, focusing on the newer technologies, the Internet of Things technology has emerged and evolved. Since the users are focused on usability and flexibility, as mentioned previously, it is notable to mention that Internet of Things devices have become a part of daily life (Szymoniak et al., 2025). According to Okereke et al. (2024), the integration of Internet of Things devices is observed in different areas, such as industry, environmental care, medicine, and urban development. However, it is notable that dependency, integration, and reliance have problems associated with the Internet of Things devices. Szymoniak et al. (2025) mention the advantages of integrating the Internet of Things devices, which assess the environment, gather information, and implement specific tasks depending on specific instances.

However, there are certain disadvantages to using the Internet of Things devices. The authors Okereke et al. (2024) argue that the challenges associated with the Internet of Things are multifaceted and related to the security of the devices. The key identifier of the challenges is the security problems. Identical to several technologies, IoT devices are not immune to security risks and vulnerabilities. The common issues with integrating and implementing IoT devices include the design of the devices themselves (Kabir et al., 2023). The commercial IoT devices that are designed are not usually built upon security principles. For instance, one challenge with manufactured IoT devices is that they come with default passwords that are not complex enough to be protected. IoT devices primarily do not offer high computing power for advanced security features. Hence, understanding the limitations of the devices is essential to focus on the solution, granted the problem statement is evident.

As this paper in the following sections discusses the problems associated with the devices and the plausible solutions to the problem, it is necessary to mention the obvious of the technological world, which is the problem of securing devices. The Internet of Things devices, like any other devices, are prone to risks and vulnerabilities due to their extensive usage and network-sharing capabilities. These vulnerabilities and risks can be exploited and give rise to a breach, unavailability, system, or network compromise (Okereke et al., 2024). Hence, this paper will aim to solve the necessary problems associated with the Internet of Things; specifically, this paper will cover the aspects of the security problems associated with the implementation of IoT devices, updates, segmentation of the IoT network in a small office home office environment, and access control. Also, it will focus on resolving by proposing a framework that includes policy and technical solutions that would help streamline the security and privacy in IoT systems.

1.1 Overview

The Internet of Things is being implemented faster into residential or enterprise network structures. The devices are designed to function swiftly. As mentioned in the introduction, these devices do not possess high processing power and are limited in performance due to their processing constraints. The typical Internet of Things device design denotes that the security of the device is not considered seriously compared to processing and profitability (El Jourhari, 2022). Due to this, there may be several issues regarding implementing the Internet of Things devices in residential or enterprise networks. The Internet of Things devices are a combination of multiple technologies such as Machine-to-Machine (M2M), Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), and Supervisory Control and Data Acquisition (SCADA) (Kokila & Reddy, 2025); by utilizing the Internet of Things machine-to-machine, human-to-machine, and machine-to-human interactions are plausible.

The Internet of Things is utilized in various sectors, such as health, information technology, agriculture, transportation, and supply chains (Magara & Zhou, 2024), with the primary goal of creating a platform for humans to interact with technology seamlessly. However, there are specific challenges to utilizing Internet of Things devices in different sectors. The risks and vulnerabilities that surround the Internet of Things technology are multifaceted: improper access control, network architecture, and update mechanisms are a few of many problems that are common among the Internet of Things technologies. As mentioned previously, the architecture of the Internet of Things devices is a combination of multiple technologies, which means that the complexity of the technology will substantially increase the vulnerability and risk perimeter, in other words, the complexity of the Internet of Things technology is directly proportional to the risks and vulnerabilities. Hence, it is necessary to discuss the challenges and drawbacks of the Internet of Things devices and technologies to understand their current situation and implement a solution. The primary protocols utilized by IoT technology, such as IP, HTTP, SMTP, and FTP, do not have the necessary security functions. For instance, data such as sensor readings, commands, and messages transmitted using these protocols are sent in plaintext and can be a security risk (Kabir et al., 2023); moreover, the authors describe the layers of the IoT architecture, and they are perception layer which is the lowest layer, network layer which is responsible to data transmission, processing which is between network and application layer, and application layer which is the top layer responsible for interaction. Comprehending the layers is necessary to segment the problems associated with IoT technologies. The IoT technologies, due to sophisticated design, increase the surface area for exploits. The authors explain several examples of exploits in each layer, for instance, the network layer is susceptible to severe attacks such as forming botnets where the attacker may gain access and poison the IoT devices in the network, and these devices may be utilized for a bigger attack as bots, denial of services attacks by flooding packets where the attacker may cause obstruction of availability of the system resources by overwhelming the capabilities of the computing power, and address resolution spoofing and poisoning attacks where the devices would broadcast the ARP request and the attacker may appear to respond to a genuine address message, the mentioned attacks are a few of the several attacks and exploits that may be executed by overriding the risks and vulnerabilities existing in each layer of the current IoT devices and technologies. Since the surface area of IoT technologies is actively increasing, so is the complexity of the architecture, the related risks, and vulnerabilities that may be prone to exploits. Hence, the necessity to implement plausible solutions to the sophisticated IoT technologies, which are primarily deprived of security practices and design, is significant.

The paper will actively aim to illustrate the significance of the research conducted in the following sections. As we conclude the overview, it is necessary to discuss the problem statement, which is security and privacy in systems with strong, secure communication and networking elements. As mentioned previously regarding the risks and vulnerabilities in the Internet of Things devices, this paper will be based on the problem mentioned, which covers the topic of the Internet of Things. The problems discussed apply to the problem statement. Moreover, this paper will aim to solve the plausible problems and propose a framework that includes a policy and technical aspect to solve the research problem in the research question.

1.2 Research Question

Deriving from the problem statement, the research question, security, and privacy in systems with strong, secure communication and networking elements, we analyze the Internet of Things devices, and the foundational area to discuss the research question is the networking element in modern technology. Networks are essential to modern networks. The basis for sharing resources is made available because of the foundational layer called networking. The IoT devices or nodes in a network constantly share resources with each other and require high availability to function. As discussed in 1.1, the network layer, along with the rest of the IoT layers, is prone to exploitation; for instance, the network layer is prone to address resolution protocol poisoning attacks. According to Bakhshi et al. (2024), IoT firmware vulnerabilities are often overlooked aspects of IoT system architecture. Moreover, the authors detail the problems related to firmware vulnerabilities, which can be damaging to the overall security of the IoT device, also, the device vulnerabilities are discovered upon their release. However, some IoT devices may have limitations and cannot be updated; this is a serious problem for IoT device implementation because the risk is actively propagated through known and unknown vulnerabilities, which is the following aspect of IoT devices and technologies. Zero-day attacks are well-known in the information technology environment, where the patch is unavailable to the known vulnerability, according to Zhao et al. (2021), the manufacturers may tend to mitigate the security problems associated with IoT devices with regard to software, the serious issue of Number of Days vulnerability persists where the system patch available for a known vulnerability however the patching for the device was not conducted due to misconfiguration or automatic-update mechanism issues.

Hence, in this paper, we will focus on solving the issues discussed above, which play an integral part in the security of IoT devices and technologies. We are actively trying to bridge the gap for a policy-driven technical solution for the issues related to zero-day, number of days attacks, continual updates mechanism, and network segmentation, which may be a primitive solution to the proposed problems, however, it is essential to layout comprehensible and easy to understand policy-driven technical solution for the discussed problem because just as complexity of technical devices increases due to sophistication, the comprehension of any complex problem becomes a hurdle unless there exists a comprehensible, concise, and communicable policy-driven and technical solution which is comprehensible and readable (Alkhurayyif & Weir, 2017). Hence, this paper is actively trying to solve the necessary problems detailed previously.

1.3 Significance

Security is a significant part of the proper function of technology. The purpose of this research is to provide a policy-driven technical framework for the Internet of Things technological devices usage in a small office home office environment because of the persisting issue that surrounds the IoT technology, which is the security aspect because security is not often taken seriously in the robust design. A common phrase that explains the security conditions regarding IoT technology within the world of information technology is that the ‘s’ in IoT stands for security. However, this research is not to comment on or demean the robust technology involved in IoT technology. However, as specified, it is to serve research and will pursue to provide a policy-driven technical framework. The paper will discuss zero trust, the number of days of vulnerability (Zhao et al., 2021), and the mechanism for the trivial problems pertaining to continual updates such as over-the-air updates (El Jourhari, 2022), and configuring network segmentation principles, which are driven by zero trust principles (Naik et al., 2025), and involving or inducing access control parameters upon the existing network segmentation (Kokila & Reddy, 2025), moreover, this paper will serve the purpose to formulate a policy-driven technical framework, the framework consideration principles will be derived from the National Institute of Standards and Technology Cyber Security Framework for a small office home office environment (NIST, 2023).

1.4 Research Contributions

This current research study will aim to discuss the numerous gaps in the study of the IoT environment, and this research study will also strive to make suitable contributions. Firstly, this paper recognizes that the approach to the IoT technology is layered in structure, such as the network layer, which is integral to devices establishing communication with each other, and aims to signify network segmentation where practices, in many cases, are implemented with zero-trust principles. However, this paper considers the number of days of vulnerability parameters to ensure security. Secondly, the paper draws attention to the comprehensive IoT framework and introduces a comprehensive policy-driven technical framework for small office home office environments. The complexity of the policy and sophisticated technical parameters may hinder comprehension and implementation in small office home office environments due to the users being in various technical levels and positions. Finally, this paper will provide a framework that is in line with industry regulations such as NIST CSF in an SOHO environment.

References

Szymoniak, S., Piątkowski, J., & Kurkowski, M. (2025). Defense and Security Mechanisms in the Internet of Things: A review. *Applied Sciences*, *15*(2), 499. https://doi.org/10.3390/app15020499

Okereke, G. E., Mathew, D. E., Ukeoma, P. E., Uzo, B. C., Umaru, A. A., & Dibiaezue, N. F. (2024). IoT device security and network protocols: A survey on the current challenges, vulnerabilities, and countermeasures. *International Advanced Research Journal in Science, Engineering, and Technology*, 11(7). https://doi.org/10.17148/IARJSET.2024.11701

Kabir, M. a. A., Elmedany, W., & Sharif, M. S. (2023b). Securing IoT devices against emerging security threats: challenges and mitigation techniques. *Journal of Cyber Security Technology*, *7*(4), 199–223. https://doi.org/10.1080/23742917.2023.2228053

Toward a Secure Firmware OTA Updates for constrained IoT devices. (2022, September 26). IEEE Conference Publication | *IEEE Xplore*. https://ieeexplore.ieee.org/document/9922087

Kokila, M., & K, S. R. (2024). Authentication, access control and scalability models in Internet of Things Security–A review. *Cyber Security and Applications*, *3*, 100057. https://doi.org/10.1016/j.csa.2024.100057

Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, *2024*, 1–17. https://doi.org/10.1155/2024/7716956

Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. *Sensors*, *24*(2), 708. https://doi.org/10.3390/s24020708

A Large-Scale empirical study on the vulnerability of deployed IoT devices. (2022, June 1). *IEEE Journals & Magazine* | *IEEE Xplore*. https://ieeexplore.ieee.org/document/9259111

Readability as a basis for information security policy assessment. (2017, September 1). IEEE Conference Publication | *IEEE Xplore*. https://ieeexplore.ieee.org/document/8090409

Naik, A. C., Awasthi, L. K., Priyanka, R., Sharma, T. P., & Verma, A. (2025). Enhancing IoT security: A comprehensive exploration of privacy, security measures, and advanced routing solutions. *Computer Networks, 237, 110841. https://doi.org/10.1016/j.comnet.2025.110841*

The NIST Cybersecurity Framework (CSF) *2.0. (2023). https://doi.org/10.6028/nist.cswp.29*