Section 2

Timothy Udumula

Department of Information Technology, University of Maryland Baltimore County

CYBR 624 (Spring 2025): Cybersecurity Project

Dr. Behnam Shariati

April 11, 2025

2. Literature Review

2.1 Overview

The implementation of the Internet of Things in small residential and commercial network perimeters is rampant at the present time. The usage of the Internet of Devices has increased due to ease of deployment and utilization. This implementation and security risks are associated with the Internet of Things, as mentioned in the introduction; since the manufacturing of IoT devices is not security-centric, certain risks are persistent in the Small Office Home Office networks. The security aspect is significantly undermined in SOHO networks because of resource constraints and limited technical approach. This survey of literature will review present sources on the Internet of Things associated problems such as network layer segmentation issues, policy-driven technical solutions, and steps for a comprehensive approach. Moreover, these findings will provide a pathway to identify the existing obstacles to the existing approaches or solutions, thus helping in providing a comprehensive solution aligned with the NIST CSF approach.

2.2 Summary of all Journals

The authors Szymoniak, Piątkowski, and Kurkowski (2025) discuss and synthesize several existing IoT security mechanisms, which include the current standards of access control, intrusion detection, and security protocols. The authors critically evaluate the need for more research and identify the roadmap for IoT security enhancement. Moreover, the authors emphasize the confrontation of security and defense obstacles in the IoT environment. However, this paper is limited due to its limitations in practical approach. The paper lacks empirical testing, which directly reduces its practical applicability in production network environments. The authors stressed the limitations of IoT device processing. However, this paper provides invaluable insight into the drawbacks of IoT devices in the network perimeter and the significance of security architecture in IoT-implemented networks within the SOHO context.

Okereke et al. (2024) present information of the major problems related with the network protocols and the IoT devices. They highlight the massive implementation of IoT devices in various sectors ranging from healthcare to industrial automation and emphasize the significant need for security. The authors stressed that the current unsecure protocols used in the IoT networks are less secure, which means that there is a lack of better encryption methods within the protocols, which makes the network extremely susceptible to various network attacks, such

as on-path attacks. Moreover, the paper highlights the obstacles surrounding IoT devices due to their constrained computing power. However, they provide various countermeasures that can be implemented, such as firmware updates, secure protocols, and proper utilization of access controls in the IoT network. This work aids in shaping solutions for the segmentation of the network and access controls, which are critical to SOHO IoT networks.

The authors Kabir, Elmedany, and Sharif (2023) signify the security challenges brought by IoT devices. They critically show the design aspect of the IoT architecture being designed for easy implementation and a smaller footprint, making the design of the IoT design not security-centric. However, the paper discusses the massive number of IoT devices in existence, and the risks and vulnerability footprint have also increased. The malicious actors can target the IoT devices and may use them in larger botnet attacks. This paper provides insight into several mitigation techniques and standards w]such as proper segmentation of network controls and protocols, which is critical in the SOHO IoT network security approach.

The author El Jourhari (2022) highlights the importance of over-the-air updates in the IoT environment. Many devices in the information technology world may be prone to vulnerabilities and risks due to insufficient patch management. The process of indulging in detailed examination to verify, analyze, and validate all the systems in the network and manually update them can be a rigorous task for network administrators. The paper makes valuable contributions by discussing the efficient measures and steps that pertain to the implementation of OTA updates which enhances the security posture by eliminating the device vulnerability, which is critical in the SOHO IoT network environment where efficient OTA updates are necessary for enhanced security posture.

The authors Kokila and K (2024) discuss the role of access controls, authentication, and scalability in the IoT network environment. The paper highlights the limitations of access controls, which are a hindrance in larger network environments. The paper accounts for the computing resource restraints in the current IoT devices and offers a comprehensive authentication and access control mechanism. Though the authors provide insight into the existing challenges, empirical studies in the IoT network structures are not provided, which is a limiting factor since it is the major focus of the research question. However, their insight is significant to decentralized systems such as IoT SOHO networks.

The authors Magara and Zhou (2024) primarily discuss the segment of smart home IoT network environment. The paper highlights several IoT-related security issues, for instance, insecure encryption, concerns of privacy, inadequate authentication, patch management issues, insecure interfaces, and the risk of IoT devices being susceptible to denial of service attacks. Though the paper argues for enhanced IoT security measures and strategies while focusing on a theoretical framework., it lacks practical implementation approaches that are essential for IoT SOHO network environments.

The authors Bakhshi, Ghita, and Kuzminykh (2024) review the significant vulnerabilities in IoT firmware and focus on auditing IoT systems present in the network. The IoT devices are often designed by overlooking the security measures during design and deployment. The authors mention the usage of outdated firmware installed on the devices when they are shipped, and may contain hardcoded credentials which can be a risk parameter for the security of the network as they can be brute forced easily. This paper aids in the technical approach for the SOHO IoT network; however, it lacks a policy-driven framework.

Zhao et al. (2022) conducted an audit through a tool called Firmsec on thousands of IoT device networks, and the authors found a significant number of vulnerabilities in the IoT systems that are induced by third-party components. This analysis is alarming because of the fundamental fact that the IoT device surface area is directly proportional to the increase in risk and vulnerabilities. Their findings are significant as they highlight the importance of the number-of-days vulnerabilities that are persistent in SOHO IoT device networks. The paper is focused on surfacing the vulnerabilities. However, the paper is limited in mitigation approaches, which are significant in the SOHO IoT networks, stressing the need for future research.

Alkhurayyif and Weir (2017) highlight the importance of the role of effectiveness of readability in the implementation of security policy. The authors point out the importance of readability because many security policies are written at a professional level, and readability drastically decreases. This is significant in the SOHO IoT network since readability ensures the SOHO environment users may comprehend the security policies effectively. However, this paper investigates the current policies rather than implements a mitigation solution, which signifies future research using a comprehensive policy-driven technical approach to the research problem.

The authors Naik et al. (2025) show the specific challenges in IoT networks. They examined the vulnerabilities in the networks and proposed advanced routing protocols and

encryption standards for the IoT environment where data transmission security is essential. The paper discussed a novel approach that combines mesh routing with cryptography, which can reduce the attack surface in an IoT environment. However, although the paper signifies the necessary implementation, it lacks a practical approach to the SOHO IoT network where the device computing restraints are significant.

The NIST Cybersecurity Framework 2.0 (2023) is an enhanced guidance compared to its previous revision. The CSF framework permits the organizations to tailor the security functions to suit their needs and necessities, which is significant in the SOHO IoT environments. It is notable that the CSF does not provide a step-by-step implementation of the framework in the SOHO IoT environment. Hence, enhanced research is required to present a comprehensive policy-driven technical solution that suits the needs of the SOHO IOT 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*