Security and Privacy Challenges in Smart Connected Homes: Addressing Insider Threats and Technology-Facilitated Abuse

Fazeleh Dehghani Ashkezari[1,*], Andreas Jacobsson[1], Martin Höst[1], and Klara Svalin[2]
[1]Department of Computer Science, Malmö University, Malmö, Sweden
[2]Department of Criminology, Malmö University, Malmö, Sweden
[*]fazeleh.dehghaniashkezari@mau.se

Abstract. Smart connected homes use Internet of Things (IoT) systems to connect devices such as smart locks, cameras, voice assistants, and home automation systems, enabling remote access, monitoring, and control of domestic environments. While these devices improve convenience and automation and the general quality of life, they also introduce important security and privacy challenges. Existing smart home security research has primarily focused on external cyber threats and technical vulnerabilities, often overlooking insider threats arising from individuals with legitimate access to shared devices.

In our research, we investigate security and privacy risks in smart connected homes from the perspective of insider threats and technology-facilitated abuse, particularly interpersonal violence and abuse enabled through connected devices. In our work, we examine how smart home systems can be misused for surveillance, coercive control, monitoring, and psychological abuse in home. These scenarios challenge traditional cybersecurity assumptions that typically separate authorized users from malicious actors. In this research, we adopt an interdisciplinary socio-technical perspective that combines cybersecurity, software engineering, and criminology. As part of the research, we have conducted a large-scale systematic mapping study of smart home security research involving more than 6,000 publications to identify major research communities and trends in the field. We also carried out a systematic mapping review on interpersonal violence and abuse in smart homes, examining how smart home systems can facilitate abuse as well as support prevention, detection, and victim support. In parallel, we have explored a hybrid deep learning-based approach to detect early signs of domestic violence through speech emotion recognition in smart connected homes. Together, these studies highlight the need for human-centered and context-aware approaches that integrate interpersonal safety considerations into smart home security and system design.

As next step, we have planned to investigate how practitioners, including IoT developers, security professionals, social workers, and police, perceive and address interpersonal violence and abuse in smart homes. The findings of this study are expected to support the development of practical guidelines and design considerations for developers and organizations working with smart home systems.

The overall goal of this research is to contribute to the design of security-enhanced, privacy-aware, and abuse-resistant smart connected homes by addressing both technical vulnerabilities and relational forms of misuse within smart homes.

References

Dehghani Ashkezari, F., Jacobsson, A., Adewole, K. S., Svalin, K., & Höst, M. (2026). Research Communities in Smart Homes Security: A Systematic Mapping Study. *IoT*, *7*(1), 19. https://doi.org/10.3390/iot7010019

Adewole, K. S., Ashkezari, F. D., & Jacobsson, A. (2025, November). Combating Intimate Partner Violence Through Emotion Detection in Smart Connected Homes. In *International Conference on Ubiquitous Computing and Ambient Intelligence* (pp. 57-68). Cham: Springer Nature Switzerland.

Dehghani Ashkezari, F., Höst, M., Adewole, K. S., Svalin, K., & Jacobsson, A.. (2026). Interpersonal Violence and Abuse in Smart Homes: A Systematic Mapping Study. In *Euromicro Conference Series on Software Engineering and Advanced Applications (SEAA) Cham:* Springer Lecture Notes in Computer Science (LNCS)
(Submitted, waiting for acceptance)