University of Pittsburgh | School of Computing and Information

Dissertation Defense

Doctor of Philosophy in Computer Science

"**Privacy in Smart Spaces**" by **Pratik Musale**

Date: July 15, 2026
Time: 10 a.m. to 12:30 p.m.
Place: Room 538-539, 130 N Bellfield Ave, Pittsburgh, PA 15260

Committee:

- Dr. Adam Lee, Professor, Department of Computer Science, School of Computing and Information
- Dr. Jacob Biehl, Associate Professor, Department of Computer Science, School of Computing and Information
- Dr. Stephen Lee, Assistant Professor, Department of Computer Science, School of Computing and Information
- Dr. Balaji Palanisamy, Associate Professor, Department of Informatics and Networked Systems, School of Computing and Information

Abstract:

IoT devices are increasingly deployed in smart spaces, potentially raising significant privacy concerns for the individuals who use and occupy them. These spaces can be used by multiple users with different privacy preferences, and existing mechanisms, such as role-based access control and majority voting, treat privacy as an administrative problem rather than a social one, failing to account for the social, contextual, and dynamic nature of privacy in smart spaces.

In this dissertation, we examine privacy in IoT-enabled smart spaces through the lens of Contextual Integrity (CI) theory across four studies. These studies examine the role of secure technologies (e.g., Trusted Execution Environments (TEEs)) in shaping users' privacy perceptions and their privacy information and interface requirements in a given space. We further examine the negotiation of IoT device configurations among peers and users' preferences for default IoT device configurations in smart spaces. We first examine how incorporating TEEs into IoT data flows shifts users' privacy perceptions regarding data type, device vendor, and notification requirements. However, concerns around consent, data retention, and bystander sensing remain unchanged. To address users' privacy concerns more precisely in smart spaces, we examine privacy awareness information and interface requirements. We find that data type and purpose of sharing are consistently prioritized, that interface preferences adapt to the social and activity context of the space, and that users expect controls within the same interface.

Smart spaces are inherently dynamic and multiuser, requiring the study of IoT device configurations for multi-user groups. We therefore examine IoT device configuration negotiations within a group of peers in smart spaces. We find that peers negotiate symmetric and asymmetric configurations, driven by activity within the space. These conditional agreements cannot be encoded by existing mechanisms, indicating that workplace configuration is a social problem rather than an administrative one. Finally, we examine

suggested default IoT device configurations based on users' individual preferences to help groups of users navigate configuration negotiations more efficiently. We find that users socially moderate their preferences when transitioning from individual to group settings, informing approaches for more efficient privacy negotiations.

These four studies support our thesis that privacy in smart spaces is dynamic and that understanding the interplay among individual privacy preferences, privacy awareness, group privacy preferences, and secure technologies is essential for empowering informed, meaningful privacy decision-making.