IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, November 2025
Impact Factor: 7.67

'Over Time Everyone's Gonna Be Open to It': User Attitudes Towards Security and Privacy in Continuous Authentication for Smart Homes

Sandesh Nat[1], Adesh Nat[2], Omkar Maindad[3], Prof.S.A.Wanave[4]
Student, Department of Computer Engineering[123]
Professor, Dept, of Computer Engineering[4]
Adsul Technical Campus, Chas, Ahilyanagar, Maharashtra, India

Abstract: *Continuous authentication (CA), a user authentication approach that continuously verifies a person's identity without requiring explicit input, is increasingly being deployed in smart homes to maintain security posture throughout user sessions. However, prior research has overlooked user attitudes toward the increased data collection and surveillance associated with CA in smart homes. To bridge this gap, we conducted a focus group study with 33 participants, using a design probe video to simulate various CA implementation scenarios in smart homes. We explored participants' current authentication methods (e.g., passwords and physiological biometrics) and examined their perceptions of CA. Through affinity diagram- ming, we found that participants perceive smart-home CA as presenting privacy and security challenges yet possessing great potential for enhanced usability. Participants also envisioned CA systems that offer more granular permission controls over personal data. Our findings indicate the contextual dependencies in balancing usability with privacy and security concerns. Our contributions include a comprehensive empirical dataset featuring the design probe video, participant transcripts, and a conceptual model of users' nuanced understanding. We provide design recommendations for smart-home CA systems, emphasizing transparency as a crucial factor in building user trust and improving adoption rates.*

Keywords: Document Forgery Detection, Optical Character Recognition (OCR), Deep Learning, Convolution Neural Network (CNN), Text Extraction, Image Processing, Computer Vision

DOI: 10.48175/IJARSCT-30068