Enhancing Privacy Awareness in Buildings through Augmented Reality Technology

LIRU CHEN, School of Cyber Science and Engineering, Southeast University, China
ZIYI ZHANG, School of Computer Science and Engineering, Southeast University, China
XIN YI, Institute for Network Sciences and Cyberspace, Tsinghua University, China
XIAOMENG SHI, School of Transportation , Southeast University, China
HANTAO ZHAO*, School of Cyber Science and Engineering, Southeast University; Purple Mountain Laboratories, China

Occupants of multi-occupancy buildings often face privacy concerns due to the sharing of common areas and the proliferation of smart devices. Augmented reality (AR) has emerged as a potential solution to address these challenges by creating virtual protective barriers and increasing privacy awareness. In this paper, we explore the application of AR for privacy protection in multi-occupancy buildings. We propose the use of privacy information visualization to enhance privacy protection and reduce the risk of privacy violations. Additionally, we implement a multi-information visualization AR system and invite users to experience and evaluate it. With the advancement of hardware technology, augmented reality-based privacy protection is expected to be widely used to provide better privacy protection solutions for occupants in multi-occupancy buildings.

Additional Key Words and Phrases: augmented reality, smart home, privacy awareness, information visualization

ACM Reference Format:
Liru Chen, Ziyi Zhang, Xin Yi, Xiaomeng Shi, and Hantao Zhao. 2024. Enhancing Privacy Awareness in Buildings through Augmented Reality Techology. In *Proceedings of Make sure to enter the correct conference title from your rights confirmation emai (Conference acronym 'XX)*. ACM, New York, NY, USA, 6 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Occupants often share common areas such as lobbies, elevators, and hallways; however, these common areas can be observed and recorded by others, thus invading the privacy of the occupants [2]. With the proliferation of smart devices and sensors, occupants' personal information and habits become more easily collected and utilized. For example, smart meters can leak the use of electricity by owners [5], and smart language assistants can spy on user conversations [12]. In addition to the user, IoT devices may violate the privacy of visitors and strangers since they can access the personal information of anyone in the environment [13].

Augmented reality is increasingly acknowledged as a promising tool for mitigating privacy concerns in multi-occupancy buildings. The technology combines virtual worlds with real-world scenarios to provide users with immersive experiences [14]. The potential of AR technology lies in its ability to create virtual protective barriers in the real world

*Corresponding author

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.
Manuscript submitted to ACM

to prevent others from directly observing or invading the privacy of the occupants. In addition, AR technology can alert users and visitors to smart devices using markers to increase respect and awareness of privacy protection.

In this paper, we explore the application of augmented reality for privacy protection in multi-occupancy buildings. By employing privacy information visualization and related decision-making facilitation functions, we aim to enhance the level of privacy protection for occupants and reduce the risk of privacy invasion. With the continued development and implementation of augmented reality, we anticipate offering superior privacy protection solutions for occupants in multi-occupancy buildings.

2 AUGMENTED REALITY SOLUTIONS FOR PRIVACY AWARENESS CHALLENGES

2.1 Privacy Awareness Challenges

As urbanization accelerates and population density increases, multi-occupancy buildings (MOBs) have become the dominant form of housing for urban dwellers [19]. However, this type of living also brings many privacy challenges. In MOBs, public spaces such as elevators, corridors, and courtyards are unavoidable places for communication. However, these public spaces are often the hardest hit by privacy violations [17]. In particular, the lack of privacy in public spaces is a personal concern when it comes to digital screens that display sensitive personal information [6]. Additionally, with the development of the Internet of Things (IoT), facilities such as communication networks and smart home systems in MOBs, while providing convenience to occupants, also pose a risk of information leakage [20]. For example, smart door locks, smart home appliances, and other devices in the networked state, once hacked, may lead to the theft of occupants' personal information and living habits. Currently, privacy protection regulations for MOBs are imperfect and supervision is insufficient. This allows some lawbreakers to take advantage of public space to carry out illegal surveillance and other activities. The challenge of privacy in MOBs is exacerbated by the lack of awareness of privacy protection among some occupants, who freely disclose personal information or violate the privacy of others.

Traditional solutions mainly involve the government, manufacturers, or legal constraints, such as strengthening building design specifications, clarifying security standards for communication networks, and improving the regulatory system while increasing penalties for illegal monitoring and other behaviors. However, from a user psychology perspective, these aspects do not fully capture users' attention. Occupants find it difficult to notice potential privacy risks in their neighborhoods and may not even be aware of the devices that collect their information and how it is used. Therefore, we need to enhance occupants' concern and awareness of privacy protection from a user-centered approach and improve their understanding of privacy risks.

2.2 Augmented Reality for Privacy Enhancement

Augmented reality has the potential to address these challenges by providing innovative solutions to improve privacy in buildings. Augmented reality can create interfaces that protect personal information by masking or anonymizing data that others may see. For example, privacy is increased in publicly visible areas by showing a portion of the information in a publicly visible area, while another portion can be viewed using smart glasses in augmented reality [6]. In addition, AR apps can alert users when they enter areas with high privacy risks, such as surveillance areas or areas where sensitive conversations may take place. This can remind users to be more cautious about their behavior and take steps to protect privacy.

Appropriate visualization is an effective strategy for informing users of device threats [4], for example, AR can provide users with a real-time information overlay that highlights the presence and location of surveillance devices

(e.g., cameras or microphones). Visualization has been shown to help users notice the presence of privacy devices [16], which can increase users' awareness of potential privacy risks and help them make informed decisions about their actions and movements. PARA is a system solution that utilizes interactive AR visualizations to inform users of privacy threats from their first-person perspective [3]. Furthermore, increased transparency through AR visualization can help users make privacy decisions and fix potential privacy breaches [8].

3 ENHANCING USER PRIVACY RELATED DECISIONS: AN AR APPLICATION SCENARIOS

3.1 Analysis of Smart Home Users' Privacy Decision Making Needs

To explore the extension of augmented reality technology into the realm of privacy, we have selected smart home environments as a representative and significant scenario. Smart homes are becoming increasingly popular, and with them, a large number of devices continue to collect and process personal data, and there is growing concern about their impact on privacy. An emerging but less researched privacy-preserving technology context is how people manage privacy in smart home environments [1]. Smart homes support residents in improving their quality of life in their personal living environments by integrating a network of sensors and devices that enable wireless communication-based data collection and task execution [18]. Users enjoy the various smart features offered by smart homes, including remote control and multitasking, and are willing to share devices [10]. However, security and privacy can pose new challenges to the user experience for applications related to the Internet of Things [15]. The proliferation of IoT devices in the home has raised concerns about user privacy, and many studies have launched investigations into users' smart home privacy perceptions [11]. Past studies have revealed users' smart home privacy protection needs. Users were found to want transparency in data collection and processing [7]. And, what makes protecting user privacy particularly difficult is that users are rarely aware of the surrounding sensors or the privacy risks associated with them [3].

3.2 Augmented Reality-based Visualization Scheme for Smart Home Privacy Protection

With the increasing popularity of smart homes, users are demanding privacy protection. Augmented reality technology provides a new solution for protecting privacy. The solution aims to provide users with an intuitive and easy-to-use visualization interface through augmented reality technology to assist in decision making for the protection of personal privacy in smart homes. Based on this, we implemented an AR prototype system, HoloLens glasses, which enables features such as visualization of the state of the smart device (shown in Figure 1(a)), visualization of the sensor range (shown in Figure 1(b)) and visualization of cross-device communication (shown in Figure 1(c)).

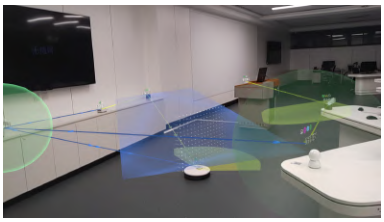
Smart home device status visualization refers to presenting the status and operation of smart home devices to users in real-time and intuitively. It enables users to understand the operating status of devices more conveniently and quickly locate them. For smart home devices that involve private data, device state visualization can ensure that users have a clear understanding of and access to control the device. Additionally, for public or unfamiliar areas, it provides a way to understand the current situation of a smart device. Sensor range visualization allows users to more easily understand the performance and limitations of a device by visualizing the operating range of a sensor. Sensor distance visualization helps to increase users' privacy awareness, reduce the risk of misuse, make them more cautious and attentive to protecting their personal privacy when using the device, and reduce incidents of privacy leakage due to inappropriate use. In a smart home system, devices can collect and share usage data, and data connection visualization enables users to see the flow and processing of this data. This allows users to better control their data, stop unnecessary data sharing, and ensure that data is only used for necessary and authorized purposes, increasing user control over



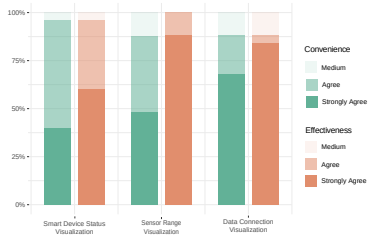
(a) Projections of privacy information on each device.



(b) Visualization of sensor range.



(c) Cross-device communication visualization.



(d) User evaluation of the convenience and effectiveness of the AR system.

Fig. 1. AR System Overview and User Evaluation. (1-2 were very strongly disagree, 3-4 were disagree, 5-6 were medium, 7-8 were agree, and 9-10 were strongly agree.)

their data. Additionally, cross-device communication visualization promotes transparency in the system, and users can clearly see how the system works, which can lead to more trust in the smart home system.

To assess the system's utility, participants were invited to interact with it and rate the convenience and effectiveness of its features on a scale from 1 to 10. Figure 1(d) illustrates the results, indicating overall satisfaction among users with the system's functionalities. Notably, effectiveness received higher ratings than convenience, possibly attributed to many users' initial experience with AR glasses. Augmented reality technology facilitates the direct overlay of virtual information onto the real world, enabling users to comprehend environmental cues and operational instructions more intuitively. This offers personalized decision support in a more intuitive manner. As smart home and AR technologies advance, the system can further expand its functionalities and application scenarios to cater to evolving user needs.

4 CONCLUSION AND FUTURE OUTLOOK

This paper investigates the application of AR for architectural privacy protection and proposes an AR visualization decision aid for common smart home privacy issues. Although AR currently has some challenges, such as user experience, it provides better privacy protection solutions for occupants in multi-occupancy buildings and can optimize user privacy decisions in smart homes. Future AR applications must prioritize user experience and acceptability [9]. Over the past few years, AR systems and related devices, such as head-mounted displays, have become more affordable, mobile, and accessible. This suggests that AR is likely to be widely used in public environments in the future. Another issue is the privacy threat posed by AR itself. Researchers have explored methods to protect the privacy of AR users, including authentication, fine-grained sharing control options, and the removal of sensitive objects through AI techniques. In the future, AR will present more advanced hardware technologies, diverse interactions, and a wider range of application

areas. This will provide users with a more realistic and immersive AR experience and opportunities for innovation and development.

REFERENCES

[1] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering Smart Home Internet of Things Privacy Norms Using Contextual Integrity. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 59 (jul 2018), 23 pages. https://doi.org/10.1145/3214262

[2] Babak Rahimi Ardabili, Armin Danesh Pazho, Ghazal Alinezhad Noghre, Christopher Neff, Arun K. Ravindran, and Hamed Tabkhi. 2022. Understanding Ethics, Privacy, and Regulations in Smart Video Surveillance for Public Safety. *ArXiv* abs/2212.12936 (2022), 83–95. https://api.semanticscholar.org/CorpusID:255125295

[3] Carlos Bermejo Fernandez, Lik Hang Lee, Petteri Nurmi, and Pan Hui. 2021. PARA: Privacy Management and Control in Emerging IoT Ecosystems using Augmented Reality. In *Proceedings of the 2021 International Conference on Multimodal Interaction* (Montréal, QC, Canada) *(ICMI '21)*. Association for Computing Machinery, New York, NY, USA, 478–486. https://doi.org/10.1145/3462244.3479885

[4] Carlos Bermejo Fernandez, Petteri Nurmi, and Pan Hui. 2021. Seeing is Believing? Effects of Visualization on Smart Device Privacy Perceptions. In *Proceedings of the 29th ACM International Conference on Multimedia* (Virtual Event, China) *(MM '21)*. Association for Computing Machinery, New York, NY, USA, 4183–4192. https://doi.org/10.1145/3474085.3475552

[5] Saba Rebecca Brause and Grant Blank. 2024. 'There are some things that I would never ask Alexa' – privacy work, contextual integrity, and smart speaker assistants. *Information, Communication & Society* 27, 1 (2024), 182–197. https://doi.org/10.1080/1369118X.2023.2193241 arXiv:https://doi.org/10.1080/1369118X.2023.2193241

[6] Alejandro Cabrera, Austin Rider, Jennifer Xiong, and Hayssam El-Razouk. 2023. Implementing Privacy on Public Digital Displays Using Smart Glasses. In *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. 274–279. https://doi.org/10.1109/CCWC57344.2023.10099103

[7] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (, Yokohama, Japan,) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 555, 16 pages. https://doi.org/10.1145/3411764.3445691

[8] Stefany Cruz, Logan Danek, Shinan Liu, Christopher Kraemer, Zixin Wang, Nick Feamster, Danny Huang, Yaxing Yao, and Josiah Hester. 2023. Augmented Reality's Potential for Identifying and Mitigating Home Privacy Leaks. https://doi.org/10.14722/usec.2023.238930

[9] Pouya Eghbali, Kaisa Väänänen, and Tero Jokela. 2019. Social acceptability of virtual reality in public spaces: experiential factors and design recommendations. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia* (Pisa, Italy) *(MUM '19)*. Association for Computing Machinery, New York, NY, USA, Article 28, 11 pages. https://doi.org/10.1145/3365610.3365647

[10] Erik M. Fredericks, Kate M. Bowers, Katey A. Price, and Reihaneh H. Hariri. 2018. CAL: A Smart Home Environment for Monitoring Cognitive Decline. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. 1500–1506. https://doi.org/10.1109/ICDCS.2018.00155

[11] Haojian Jin, Hong Shen, Mayank Jain, Swarun Kumar, and Jason I. Hong. 2021. Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost. *ACM Trans. Comput.-Hum. Interact.* 28, 5, Article 34 (aug 2021), 55 pages. https://doi.org/10.1145/3463910

[12] Dasom Lee and David J. Hess. 2021. Data privacy and residential smart meters: Comparative analysis and harmonization potential. *Utilities Policy* 70 (2021), 101188. https://doi.org/10.1016/j.jup.2021.101188

[13] Karola Marky, Sarah Prange, Florian Krell, Max Mühlhäuser, and Florian Alt. 2020. "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In *Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia* (Essen, Germany) *(MUM '20)*. Association for Computing Machinery, New York, NY, USA, 83–95. https://doi.org/10.1145/3428361.3428464

[14] Carlos E. Mendoza-Ramírez, Juan C. Tudon-Martinez, Luis C. Félix-Herrán, Jorge de J. Lozoya-Santos, and Adriana Vargas-Martínez. 2023. Augmented Reality: Survey. *Applied Sciences* 13, 18 (2023). https://doi.org/10.3390/app131810491

[15] Sarah Prange and Florian Alt. 2020. I Wish You Were Smart(er): Investigating Users' Desires and Needs Towards Home Appliances. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (, Honolulu, HI, USA,) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3382910

[16] Sarah Prange, Ahmed Shams, Robin Piening, Yomna Abdelrahman, and Florian Alt. 2021. PriView– Exploring Visualisations to Support Users' Privacy Awareness. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (, Yokohama, Japan,) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 69, 18 pages. https://doi.org/10.1145/3411764.3445067

[17] Titus Stahl. 2020. Privacy in Public: A Democratic Defense. *Moral Philosophy and Politics* 7, 1 (2020), 73–96. https://doi.org/doi:10.1515/mopp-2019-0031

[18] Yi Sun and Shihui Li. 2021. A systematic review of the research framework and evolution of smart homes based on the internet of things. *Telecommun. Syst.* 77, 3 (jul 2021), 597–623. https://doi.org/10.1007/s11235-021-00787-w

[19] Fatih Topak, Gregory S. Pavlak, Mehmet Koray Pekeriçli, Julian Wang, and Farrokh Jazizadeh. 2023. Collective comfort optimization in multi-occupancy environments by leveraging personal comfort models and thermal distribution patterns. *Building and Environment* 239 (2023), 110401.

https://doi.org/10.1016/j.buildenv.2023.110401

[20] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security & privacy concerns with smart homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 65–80.