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

I. INTRODUCTION

Smart homes offer a level of convenience that has transformed how users interact with their living spaces. One such con- venient technology is the Internet of Things (IoT), where interconnected devices and sensors share data over the net- work to deliver services [1]. However, a connected network also introduces substantial security and privacy challenges. For instance, IoT devices and sensors are vulnerable to cy- berattacks and unauthorized access, leading to the theft of personal information or even compromising users' physical safety [1]. Additionally, these devices often collect sensitive data that may be exploited, including users' physiological and behavioral biometric information [2]. Moreover, although users rely on the seamless usability of smart home devices, many remain unaware of the potential risks associated with the devices.

Consequently, they may not take essential steps to protect their devices or personal information, such as fre- quently updating passwords, configuring firewalls and intru- sion detection systems, or enabling automatic device updates for timely security patches [3]. These challenges require ad- vanced authentication methods with robust security measures and privacy protection while maintaining usability in smart homes.

Continuous authentication (CA) is a security mechanism that involves the ongoing verification of a user's identity throughout a session, thereby ensuring protection beyond the initial login. Unlike identification, which determines a person's identity by comparing their data with that of all known individuals in a database (a one-to-many comparison), authentication validates the claimed identity by comparing new data to previously registered data for that specific indi-

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

vidual (a one-to-one comparison) [4]. CA systems maintain continuous assurance of user identity during active sessions, providing an additional layer of security by repeatedly verify- ing identity over time instead of relying exclusively on initial login credentials [5].

This paper examines users' perceptions of CA, with a particular emphasis on the collection of diverse behavioral modalities, such as gait [6], body behaviors [7], and voice [8], to enable persistent identity verification. Such behav- ioral modalities can be monitored invisibly and unobtrusively, facilitating data collection compared to physical modalities, like face and fingerprints, which typically require explicit user engagement with a sensor, such as a camera [9], [10]. Previous research has identified several factors shaping user perceptions of CA, including security and privacy [9], [11], usability [9], [12], and explainability [13]. However, these studies have primarily focused on CA practices in mobile devices, resulting in a gap in understanding user attitudes toward CA within IoT environments. Our study extends pre- vious work by investigating users' mental models of CA in the emerging context of smart homes.

The use of behavioral biometrics for CA in smart homes enables users to seamlessly interact with their environment without the need to repeatedly authenticate across multiple devices or services [14]. This approach can also substantially mitigate the risk of unauthorized access to smart devices, potentially making CA more user-friendly than traditional methods [15]. However, the implementation of CA in smart homes necessitates careful consideration of privacy, as real- time data processing involves the frequent collection of sensi- tive data [16]. Therefore, understanding user attitudes toward CA is essential for evaluating its adoption potential [17], [18]. In this paper, we collected data on participants' past experiences with traditional authentication methods, their au- thentication behaviors, and their perceptions regarding the potential deployment of CA in smart homes. This study not only synthesizes user needs, expectations, and current chal- lenges related to CA in smart homes, but also informs the development of a prototype, which we intend to design and evaluate in future research.

The contributions of this paper include a dataset featuring a design probe video that illustrates potential use cases for CA in smart homes, alongside interview transcripts capturing participants' perceptions of CA. Through qualitative analysis, we propose a conceptual model that elucidates participants' nuanced understanding of authentication, encompassing both traditional and CA-based methods. Building on this model, we examine the interplay of factors that collectively shape participants' attitudes and behaviors toward various authenti- cation techniques. We identified three principal design impli- cations for developing smart-home CA that align with users' mental models. First, authentication adoption is influenced by user experiences, contexts, and individual attitudes. Second, transparency is critical to bridging the gap between users and systems, enhancing comprehension of usability, security, and privacy. Third, context-aware and customizable systems can empower users to make informed trade-offs between usability and security or privacy, thereby affording them greater agency and control.

II. RELATED WORK

This section reviews the privacy and security risks associated with smart home devices, evaluates current authentication methods, and synthesizes existing literature on CA use cases within smart homes.

A. PRIVACY AND SECURITY RISKS IN SMART HOME DEVICES

The rising popularity of smart home devices is largely at- tributable to their potential to improve users' quality of life. Devices like smart speakers enhance the convenience of daily domestic activities while remaining cost-effective [19]. How- ever, these devices also introduce privacy and security risks due to their interconnectedness within IoT networks and the collection of personal data [1]. For example, Ferraris et al. scrutinized smart home devices that collect various forms of sensitive information (e.g., personal calendars and names), emphasizing the susceptibility of this data to security threats [20]. The 2016 Mirai Botnet attack compromised around 600,000 devices, including baby monitors, home routers, and personal surveillance cameras, disrupting services such as Amazon for several hours [21].

Prior research has demonstrated a significant relationship between user acceptance of smart home systems and users' perceptions of privacy [22], [23], security [24], and usability [25]. For example, Abdi et al. examined how privacy norms influence user acceptance of information flows in smart per- sonal assistants [22]. Their findings indicate that users per- ceive data access as more acceptable when recipients are trusted or familiar, when the data involved is less

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

sensitive, and when the purpose of data sharing is transparent. However, few participants actively configured access control mecha- nisms within these systems. Their results showed that users do not take actions with the same level of security as their perceived privacy.

Moreover, the actual security and privacy implications of smart home devices often fall short of users' expectations. Abdi et al. identified limitations in smart home technologies that require precise privacy configurations to enable more granular access control [22]. Kaaz et al. highlighted both the lack of configuration options and the gap between users' expectations of secure systems and the reality that devices such as Amazon Echo can accept voice commands from unau- thorized individuals [3]. These system shortcomings may lead to user frustration and increase the risk of compromised personal data.

Additionally, users' desire to safeguard privacy often clashes with their preference for convenience and connec- tivity provided by technology [26], leading them to make trade-offs despite acknowledged privacy issues [23], [25] and security risks [24]. For example, users apply social norms when utilizing smart home features (e.g., access control and notifications) to mitigate security and privacy issues [24]. Townsend et al. found that users were willing to compromise privacy if unobtrusive sensors provided increased autonomy [23]. Similarly, elderly users were willing to compromise on privacy and usability in exchange for continuous monitoring of their health conditions [25].

B. AUTHENTICATION METHODS IN SMART HOMES

Authentication serves as the primary defense to ensure the security and integrity of digital resources [27]. To mitigate the aforementioned risks, prior studies have assessed conven- tional authentication methods in smart environments [28]– [31]. For example, Dahl presented multiple domestic scenar- ios for token-based and location-based authentication, offer- ing various interactive features [29]. Sudharsan et al. reported the cybersecurity risks faced by smart speaker users due to the lack of an authentication scheme [30]. They proposed a smart speaker that uses biometric authentication to address these risks. However, each method poses its challenges. Passwords require user memorization and do not adapt to the needs of visually impaired users [28]. Token-based authentication is impractical if the authenticating object is not in the user's possession [29]. Biometric authentication is vulnerable to cy- bersecurity attacks, and existing schemes may be insufficient [30]. Two-factor authentication (2FA) presents challenges to users during the registration phase [31].

Additionally, these conventional methods lack contextual awareness and fail to dynamically adjust security levels based on user needs. They authenticate users only at the point of entry, thereby failing to provide constant protection for user data. Prior research explored user perspectives on security and privacy, finding that users anticipated advanced authentica- tion methods capable of overcoming the challenges posed by traditional methods. Ponticello et al. conducted interviews to investigate user opinions on the privacy and security of voice authentication in smart speakers [32]. Their participants per- ceived voice assistants as convenient and trustworthy. How- ever, participants expressed a desire to test novel biometric authentication schemes first. They also felt conspicuous when performing security-sensitive tasks in front of others in social situations. The authors suggested providing a sandbox mode for users to experiment with the authentication process, help- ing them build trust in the system. They advocated designing systems that could sense the social situation and adapt the authentication process to the context. The authors concluded that participants envisioned low-effort authentication, which CA could provide.

In this regard, CA emerges as a solution to implicitly authenticate multiple users in a household and seamlessly accommodate changes in context, such as authentication time and location [33], thereby moving beyond traditional point- of-entry logins.

C. CONTINUOUS AUTHENTICATION IN SMART HOMES

Considering the multifaceted nature of the smart home con- text, the design of CA systems necessitates the integration of various factors. Al-Naji and Zagrouba reviewed CA for IoT- based smart home devices and outlined the successive steps of CA design, including user factors, the selection of scenarios, devices, features, authentication enforcement, and evaluation [34]. However, current CA designs are insufficient in address- ing all aspects comprehensively. Gonzalez-

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

Manzano et al. highlighted the prevalence of portable devices and behavioral biometrics in current CA practices, emphasizing the lack of scenario-based research and consensus on evaluation metrics [16].

Evaluation of CA prototypes in smart homes is spread across various aspects such as privacy [33], security [35], accuracy [36]–[39], and usability [14]. For example, Sabbah et al. employed CA to verify examinees' identities using fingerprints, keystroke dynamics, and a video comparison algorithm throughout a remote session [35]. The authors reported that their scheme was fully automated and secure, effectively minimizing cheating. Amraoui et al. constructed a model based on user behaviors for smart speaker access control [36]. The model achieved a true positive rate of at least 95.29% and a false positive rate of no more than 4.12%. Sooriyaarachchi et al. developed an IoT-based system that used music-induced brainwave patterns for CA [38]. The system achieved over 97% accuracy in authenticating 20 participants wearing commercial headsets. Kong et al. developed CA based on users' finger gestures using WiFi signals [5]. Their classifiers accurately authenticated about 90% of users' finger gestures with a false acceptance rate of 3%. Additionally, Hayashi and Ruggiero conducted user activity recognition for smart speakers in real-world settings over two months and obtained 97% accuracy and 81% recall [39]. They reported that their system helped bridge the gap in implementing granular access control in a smart home testbed.

However, prior work examines smart-home CA from the designer's perspective and lacks investigation into the user's attitude toward the system [16], [34], which is a crucial factor for designing context-aware or scenario-based CA. Previous findings are limited by prototype specifics or study contexts [40]–[42]. For instance, Feng et al. proposed CA for voice assistants that detects the user's body surface vibrations and matches them with voice commands [40]. They reported that CA was reliable against various attack scenarios, demonstrat- ing high accuracy and a low error rate. However, the authors mentioned that their prototype could not treat commands differently based on task sensitivity levels. Kong et al. [5] only reported results from a usability study with seven participants, indicating a need to explore the generalizability of CA with a larger user group. Stylios et al. conducted a study similar to ours, surveying participants about the factors influencing user adoption of behavior-based CA [41]. Their factors included trust in the technology, compatibility, perceived usefulness, and innovation. Participants reported being less willing to compromise on security for CA usability. The authors noted that their research specifically targeted CA on mobile devices and suggested that future work could extend the application of CA to IoT devices.

Our work contributes to the existing body of research by qualitatively exploring users' attitudes toward CA in vari- ous smart home contexts. These contexts are grounded in users' everyday domestic activities and deliberately exclude unnecessary technological details to allow users to naturally articulate their opinions on CA. Our study addresses the gap in prior literature regarding the missing piece of user attitude towards smart-home CA [12], [41]. We emphasize that privacy and security challenges persist, yet CA has the potential to provide granular control for enhanced security and user experience by incorporating context and user needs. By uncovering the relationships among various factors that influence user perceptions, our work supports previous re- search advocating for a shift from a device-centric model to a capability- and relationship-centric model [43].

III. METHOD

This section details the study design, research questions, par- ticipant demographics, procedures, and design probe video content.

A. STUDY DESIGN

We chose focus groups to explore users' attitudes toward au- thentication collectively. Focus groups enable the qualitative identification of themes in users' comments and help syn- thesize the similarities and differences in their attitudes. This approach facilitates organic conversation among participants, yielding insights less accessible in individual interviews [44]. Five independent focus groups were conducted, each with

6 to 8 participants (minimum = 6, maximum = 8, average = 7). Each session lasted between 60 and 80 minutes. To begin, we asked participants about the devices they currently use as a warm-up (see Appendix A for the full script). We also showed participants a design probe video before discussing CA (see Appendix B).

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

B. RESEARCH QUESTIONS

We designed focus group questions based on prior research [41], [45], [46]. Aloba et al. surveyed 117 MTurk workers and 43 computer science students regarding their attitudes toward active authentication systems, finding lower trust in natural authentication methods (e.g., gestures) compared to traditional methods (e.g., passwords) due to concerns about visibility and social exposure. Their participants reported feeling awkward when using natural methods in the presence of people they did not trust. Their results highlighted concerns about privacy, security, and social risks with explicit device logins [45]. Similarly, Crawford and Renaud conducted a survey with 30 participants on CA and traditional smartphone authentication methods, finding that 90% were willing to adopt CA on smartphones [46]. However, existing studies do not explore user attitudes toward CA in smart homes, where biometric recognition shifts to implicit or passive forms for a more seamless user experience.

To complement previous research, we identified the fol- lowing research questions (RQs):

RQ1: How do users utilize and perceive existing (active) au- thentication methods in home environments?

RQ2: How do users' mental models of these methods affect their authentication behaviors on shared devices?

RQ3: What are users' perceptions and concerns about the po- tential implementation of (passive) CA in home settings?

RQ4: How do users view various natural modalities (i.e., be- havioral and physiological data) monitored by CA, par- ticularly when sharing devices among household mem- bers?

These RQs inform ten focus group questions (see Ap- pendix A) focused on four overarching goals: 1) participants' current authentication devices, methods, and data protec- tion mindset [RQ1]; 2) encountered authentication challenges [RQ1]; 3) strategies for shared device authentication [RQ2]; and 4) attitudes toward CA and its monitored modalities [RQ3, RQ4].

C. PARTICIPANTS

Participants were 33 adults aged 18 to 35 years (mean = 22, SD = 3.85 years) who were recruited from a local uni- versity. Multiple gender options were available, including trans and/or gender non-conforming and 'prefer not to say'. Twenty-two participants self-identified as male, eleven as female. Participants had diverse races: White (14), Asian (13), Black or African American (3), American Indian or Alaska Native (1), and Prefer not to say (2). Participants reported having different levels of experience with technology related to smart homes, including workstations/personal computers, cellphones and tablets, wearable devices (e.g., smartwatches), Amazon Alexa/Google Home, Microsoft Kinect, health mon- itoring sensors (e.g., heart rate sensors), video game consoles, and smart TVs. During the focus group, none of the partici- pants reported having used CA before.

Prior to participating in the focus group, we assigned a unique 3-digit random ID to each participant and asked them to complete a consent form and a demographic questionnaire. To express our appreciation, we offered each participant extra course credit in a course of their choosing as compensation.

D. PROCEDURE

This study was conducted during the COVID-19 pandemic, which hindered the feasibility of organizing in-person focus groups. We ran the focus group sessions remotely over Zoom in a semi-structured format. A researcher acted as the facilita- tor, and two others served as notetakers. One of the notetakers recorded every question asked by the facilitator in the chat to aid participants in recalling them.

Participants were encouraged to freely express their thoughts with the reassurance that sharing was voluntary. To facilitate organic conversation, the facilitator allowed partic- ipants to respond in any order and employed active listening cues (e.g., nodding), managing each participant's speech dy- namically.

The facilitator encouraged participants to share their opin- ions by asking them to recall recent experiences and share stories with as much detail as they desired. Subsequently, we showed participants a design probe video introducing CA (described below) and asked for their opinions of CA. The facilitator clarified that the use cases of CA were not limited to the examples shown in the video and encouraged participants to envision other at-home scenarios. After confirming that participants had no further comments, researchers expressed their appreciation and granted participants extra course credit. The study was approved by the university's Institutional Review Board (IRB).

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

E. DESIGN PROBE VIDEO

To elicit discussion among participants regarding their atti- tudes towards CA, we utilized a design probe video following scenario-based design [47]. We employed the envisioning ap- proach, which is commonly used to understand user opinions towards novel technologies in ubiquitous computing and HCI [48]–[50]. The video was a digital storytelling presentation with vignettes of a family using CA at home. We chose cartoon-style vignettes as they are easier to create than real- istic representations, and realistic rendering would not match any participant's home scenarios, as outlined in prior work [51]. We showcased potential use cases of CA for current smart home technologies such as a smart TV [32], alongside future scenarios of recognizing various modalities (e.g., voice and behaviors). We omitted overly technical details that might be challenging for a general audience to understand.

The video included the following scenes: The Smith family is cooking dinner together. After tasting their food, the parents discover they are out of butter. Mr. Smith instructs the fridge to add butter to his shopping list (Fig. 1(a)). Right after that, Johnny mimics his father's behavior and asks the fridge, ''Can we add candy to the list as well?''. However, the fridge recognizes his voice and responds, ''Sorry, you need to ask your parents for permission,'' denying his request. (Fig. 1(b)). Later that night, both Mr. and Mrs. Smith are resting in their room while their child is playing in the living room. Johnny wanders into the bathroom and attempts to open the medicine cabinet, but the bathroom is equipped with smart devices that detect who is in the bathroom. If Johnny tries to open the medicine cabinet, the smart home locks it (Fig. 1(c)). However, the door will automatically unlock whenever Mr. or Mrs. Smith walks by. The next day, Mr. Smith and Johnny want to watch something together during breakfast. The TV recognizes their behavior and already displays Johnny's fa- vorite TV show (Fig. 1(d)). Later that afternoon, Johnny invites his friend Nick over to the house. Nick has visited the house previously, and the smart floor recognizes him by his gait, activating the TV to launch their preferred video game (Fig. 1(e)).

In these scenarios, CA occurs passively, without requiring the user to actively engage with an authentication service. Smart devices, such as the fridge or bathroom systems, con- tinuously monitor and authenticate users based on behav- iors or biometric cues like voice or presence. For instance, Johnny's voice is automatically recognized by the fridge with- out him needing to provide a password or other explicit au- thentication. Similarly, the smart bathroom devices recognize who is in the room and adjust access to the medicine cabinet without requiring Johnny or the parents to perform any active authentication actions. This seamless, ongoing authentication happens in the background as part of the natural interaction within the smart home.

IV. DATA ANALYSIS

All focus groups were audio and video recorded using Zoom's screen recording feature, yielding a total of four hours and 50 minutes of video from five focus group sessions. Following the study sessions, we transcribed the videos using an auto- matic transcription software [53]. Four researchers then man- ually corrected the transcripts. We analyzed the transcripts us- ing affinity diagramming [54], a bottom-up inductive method for identifying common themes and patterns in qualitative data.

Four researchers iterated over the affinity diagram in three phases. We used an online whiteboard tool [55] to transfer participants' responses from transcripts to sticky notes. Ini- tially, we accumulated 697 sticky notes organized by focus group question. As a team, we reviewed the sticky notes one by one, grouping those referring to similar concepts or themes inductively. If a sticky note encompassed multiple themes, we divided it into separate notes or duplicated it, allowing it to ap- pear under each relevant theme. Next, we reviewed all themes and categorized them into 23 broader, higher-order groupings. We continued to refine and reorganize these categories until clear distinctions emerged.

Finally, we iterated again to or- ganize the categories into seven major themes, resulting in 954 sticky notes. From these, we disregarded 237 sticky notes deemed irrelevant to our research questions. This included responses to warm-up questions: ''I use my smartphone and my laptop mostly every day'' (P008). The entire research team then discussed the themes and analyzed the relationships between groups to create a conceptual model diagram. We combined the resulting sticky notes from all questions into the diagram, integrating participants' thoughts about everyday authentication alongside their speculative views about CA.

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

V. FINDINGS

We identified seven overarching themes: during the focus groups, participants discussed specific contexts and experiences using existing authentication methods (User Context of Use and User Experience). These factors influenced partici- pants' attitudes towards current technologies, including Trust towards technologies, Perceived Security, Data Privacy, and Perceived Usability. Based on these themes, we created a conceptual model shown in Figure 2. Using Transparency as the mediating factor between user and system design, we present three main findings:

FIGURE 1: Screenshots from the design probe video: (a) The smart fridge recognizes Mr. Smith's voice and adds butter to his shopping list. (b) When it recognizes Johnny's voice, it prompts Johnny to ask for permission first. (c) The medicine cabinet recognizes Johnny's behavior and locks itself to prevent his access. (d) The smart TV recognizes Mr. Smith's and Johnny's body behaviors and starts their favorite TV show. (e) The smart floor recognizes Johnny's friend Nick based on his gait and launches their favorite video game. Images were created with Storyboard That [52].

1) The acceptance of authentication systems is influenced by factors including user experience, contexts of use, and user attitude.

2) Transparency is the pivot between users and systems. The system should consider factors from the user, striv- ing for transparency to enhance users' understanding of system usability, security, and privacy.

3) The system should convey transparency in its technical design, implementation flexibility, and user interface design, so that users can make better trade-offs based on their perceptions.

These findings inform the development of human-centered CA for smart homes, and contribute to the broader discussion about adopting any authentication technology. Next, we illus- trate each theme and the interrelationships of factors within themes.

A. USER CONTEXT OF USE

During the focus group, participants elaborated on differ- ent contexts of using authentication technologies: Device-sharing, Tasks with varying degrees of sensitivity, and Ur- gency of use.

Device-sharing is common among our participants who live with others in the same household. For example, partic-ipants shared authentication methods with family members who were less familiar with these technologies. In P085's words, ''I know my parents' passwords because I usually help them with issues they have with certain websites or get-ting information that they need''. Our participants considered tasks with varying degrees of sensitivity; thus, they restricted content on the shared device. Specifically, they employed guided access for children to limited usage. P166 explained, ''I share it [TV] with him [my little brother] and I restrict him to his age level. Usually, they have parental control. And I have to give a pin to allow him to watch certain things that are outside of that range''. We also found that

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

participants inten- tionally circumvented traditional authentication methods in urgent situations. P187 thought that, ‘‘When my friend needed to call someone and his phone was dead, I let him use my phone. I unlocked it, and then he just used it’’.

Participants considered the implications of CA by reflect- ing on the scenarios in our video and relating them to their personal use cases. For example, P818 expressed enthusiasm for CA on shared devices, stating, ‘‘I think that [CA] is cool. Also the constant authentication is nice. Preventing the kid from adding stuff to the grocery list seems really usable. My cousins are older now, but when they were younger, having them have access to unfiltered access to smart devices used to freak me out because there were creeps on the internet’’. P300 exemplified this perspective, commenting, ‘‘For example, personal drawers or belongings, maybe just for the handle or something.’’ However, P004 did not see the potential of

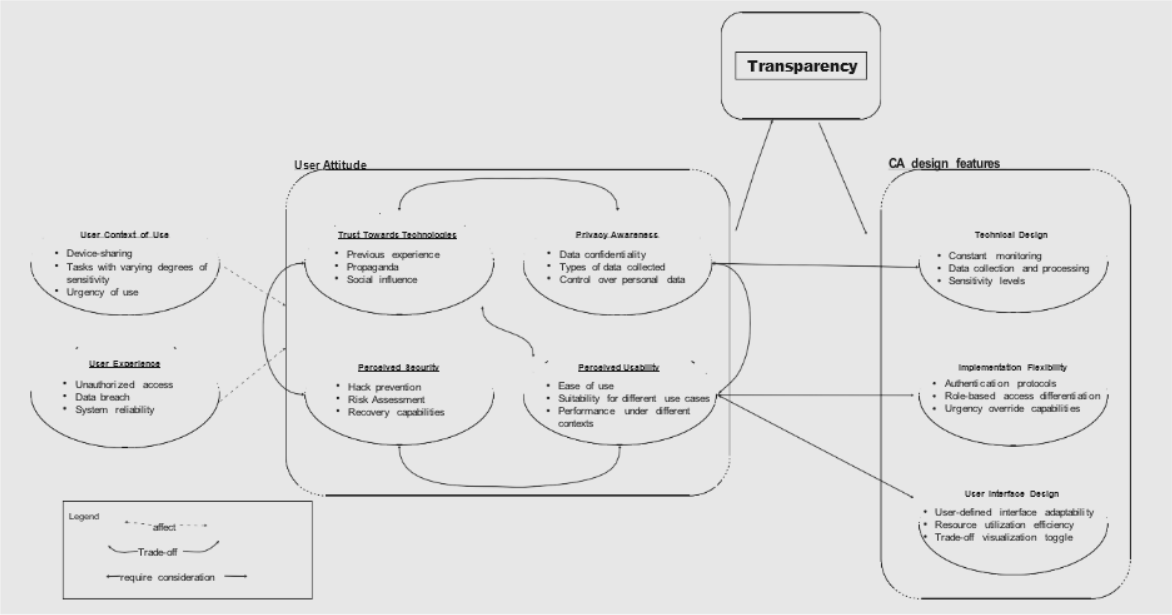

FIGURE 2: The conceptual model of users’ understanding of authentication systems.

CA to adapt to urgent tasks, ‘‘What if someone needs their insulin [from the medicine cabinet], like you need to get to the medicine cabinet quick’’. P464 also perceived CA as less flexible compared to traditional methods, ‘‘If it’s something that can be done using conventional means like a combination lock or regular lock, I maybe don’t see the true point in having it because a combination lock, somebody can open it. If a child needs to get the insulin for their parent, they can open it’’.

B. USER EXPERIENCE

Participants had experienced Unauthorized access, Data breach, and System reliability incidents with traditional au- thentication technologies. These included face ID, finger- print, password, voice recognition, and 2FA. No participant had used CA before.

Traditional authentication systems only verified partici- pants at the point of entry, leaving their data vulnerable to unauthorized access, as P534 stated, ‘‘I remember one time I was away, it was during the time when I was working with the firm and I went away from my desktop and I forgot to lock my device. So as a prank, my colleagues mailed my manager and set up a meeting’’. Participants reported encountering password leaks. For example, P919 shared, ‘‘I used to use the same set of passwords for a lot of things, but then I stopped when I started getting all these warnings about password leaks and forced me to change the passwords. And then I started using those generated ones’’.

They also shared their opinions on the reliability of bio- metric authentication based on their personal experiences.

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

For example, P981 found face ID frustrating, explaining, ‘‘I was outside wearing sunglasses and I tried to use face ID on my phone and it did not work. And I was pretty frustrated’’. In contrast, P710 had a positive experience, ‘‘I like the face ID because even if I’m wearing a mask, I know it will still work’’. Additionally, 2FA received negative comments due to its reliance on the presence of the device and cumbersome reset procedures. Conversely, passwords were perceived by numerous participants as the most reliable of the current technologies and were used as a backup when biometric authentication failed. As P008 stated, ‘‘I would like to concur with the password, as being so far, the most reliable’’.

C. USER ATTITUDE

We found that participants expressed varying degrees of Trust Towards Technologies, Privacy Awareness, Perceived Secu- rity, and Perceived Usability.

1) Trust Towards Technologies

Participants’ trust in technology is influenced by their previ- ous experiences or media propaganda. P286 stated, ‘‘although I don’t want those information to be like other things (to be accessed), the company will still have access to that. Actually it looks like we can’t really do much things about that’’. We observed a dichotomy among participants regarding CA, with some exhibiting unconditional trust while others expressed a lack of trust. A significant concern that emerged was about companies exploiting user data while constantly surveilling them. P464 stated, ‘‘I do not trust these technologies and in our current situation of rampant, unregulated data collection.

We see headlines every day [about] our personal data being collected and sold. I would not trust my home to know where I was and what I was doing at all times’’. P633 initially said, ‘‘I would prefer that nothing really gets shared but if it was just used for training AI, I don’t think I would mind that most of it is shared’’. However, P633 later added comments expressing a lack of trust:

I’ve seen a few articles about how Amazon, Google, they’ve had Google Homes or Amazon Echos record conversations. And I just don’t really trust big tech that much. If someway, somehow, they got their hands on it. I would kind of tolerate it. I’d always prefer that they have less information about me. So I probably wouldn’t use any of this [CA].

Similarly to their adoption of existing technologies due to so- cial influence, other participants envisioned the inevitability of CA adoption over time. P017 said:

When they first made the car, everyone was like, ‘I’m not getting the car, that doesn’t look safe’. And then came passwords on your phone, everyone’s like, ‘I’m not doing that. It’s not safe.’ I’m sure over time everyone’s gonna be open to it and it’ll be normal. So I’m sure it’s not a big deal. It’s just the public state of mind. You have to ease that stuff in one thing at a time.

2) Privacy Awareness

Regarding the data they wanted to protect, participants were concerned about Data confidentiality, Types of data collected, and Control over personal data.

Participants expressed various levels of privacy awareness. Many took steps beyond traditional authentication methods to safeguard their data on shared devices. One participant verified the identity of individuals accessing shared accounts to ensure their data was not accessed by unauthorized parties. Another participant chose not to share personal devices at all to minimize potential risks.

In contrast, a few participants were less concerned about their data being collected. In P818’s words, ‘‘As long as it’s not incriminating, you can collect any data you want from me. Cause I absolutely love that. My browsing history knows what I like. I get great ads. I think the one thing I wish is, I could tell it when I’ve already bought something, so it can stop giving me that ad’’. When asked about the types of data to be col- lected, some participants were comfortable with having their heart rate, facial features, or voice tracked. Others emphasized the need for their conversations, habits, activities, and other biometric data to remain confidential. P633 commented, ‘‘It would really bother me if my conversations between friends or any images I have saved on my phone get shared’’.

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

Regarding CA, participants worried about data confiden- tiality as well, which led to hesitations in adopting the tech- nology in the first place. For example, P008 said, ‘‘I think even though this technology [CA] has the potential to make life easier, but also keep in mind if it receives a signal, it can also send a signal. So it’s a two-way communication and you never know who’s on the other side and collecting that data and never will they tell you ‘we are using that data’’’. This apprehension stemmed from the constant monitoring of CA, which participants feared would encroach on their privacy.

Participants’ opinions also varied depending on the type of data that CA would collect:

If you have a medicine cabinet that’s not connected to the internet or wifi, but it could detect there’s a little kid trying to open it. I think that’s not a bad idea. But at the end of the video I saw the dude playing around with his computer and the camera was taking data points [for recognition] from his face. I don’t really like that idea. (P004)

Similarly, P028 said, ‘‘I think tracking voice and stuff is okay but tracking my movements and what I usually do is not ok’’. Participants acknowledged the convenience of CA but stated they would not compromise their privacy unless they had complete control over their data:

I think it depends on how the data is being [pro- cessed], if it was insulated from the internet en- tirely, I would feel more comfortable with it. But if there was any connection to the outside world and it wasn’t running on some internal machinery, then I would not use it if it was connected that way. But I think the functionality sounds great. I just wouldn’t be comfortable unless I was in complete control of all the data that was being processed in it. (P669)

3) Perceived Security

Participants discussed perceived security in terms of Hack prevention, Risk assessment, and Recovery capabilities.

We found that although participants thought passwords were secure, they still asked their browsers to remember passwords, which sometimes led to hacks. Additionally, P534 raised concerns about biometric spoofing and said, ‘‘[Voice prediction] can be replicated’’. In contrast, P710 felt that biometrics were secure due to the rigorous verification of facial characteristics at the point of entry:

I have not had any problems with face ID. I found it’s performed really well in situations where, let’s say someone has my phone and they’re trying to unlock it and they try to put it in front of my face to get it to unlock. If I just close my eyes, I know the face ID won’t unlock it all, even though it can see my face.

Participants felt that CA could introduce more risks be- cause it collects more data than traditional methods:

We’re becoming a little dependent on technology and the amount of information that this technol- ogy is gathering is unsafe or weird. You’re get- ting tracked all over your house with your daily movements and everything you’re doing. If for some reason someone else got that information, it would be they know everything you do on a day-to-day basis. That would be a safety risk. It’s weird to me. The phone tracks your information obviously, but like CA, with the fridge and the floor, that’s a lot more information being tracked and more than just your location of where your phone is. (P852)

Despite these concerns, P629 suggested that hacking issues in CA can be addressed based on their experiences with existing technologies, ‘‘I would say if your fridge gets hacked, they can buy whatever, but then you can contact your bank and say I didn’t buy this. Someone hacking my thing.’’

4) Perceived Usability

Participants perceived system usability in terms of Ease of use, Suitability for different use cases, and Performance under different contexts.

We found that participants made trade-offs based on their trust, perceived privacy and security, and usability in the tech- nology when selecting authentication methods, which influ- enced their adoption of biometrics.

For example, P779 said, ‘‘For me it has to be fingerprints [being the most convenient]. I somehow think that passwords are the safest, but still, I think fingerprints are much easier than face recognition. It [face recognition] does not work sometimes when you’re wearing glasses or masks. So fingerprint is very easy and I think it’s more secure’’. Similarly, P591 considered biometrics more reliable and convenient than passwords, stating that ‘‘I’d say my favorite is the fingerprint. I find that it almost never fails me and I don’t have to take off a mask to use it. And I have password

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

backups if it [fingerprint] does fail, I think those just get annoying most of the time. I'm so used to the convenience of fingerprint or facial ID''.

However, biometric recognition was found to perform poorly in some contexts. For example, P633 noted, ''My phone's five years old. Fingerprint sensors are worn away. So typically it takes me a few attempts for the fingerprint to work. And if I'm busy, I'll just use the PIN to get in rather than the fingerprint''. Although participants considered passwords to provide a reliable user experience, they criticized them for being difficult to recall and causing frustration. Similar sentiments were expressed about 2FA due to its cumbersome setup process.

When asked about CA, participants highlighted its implicit authentication that requires no user input. P320 mentioned, ''I like how it [the fridge] is easy and you can just deal with that and not have to think when you're getting groceries''. Par- ticipants expressed a desire to customize CA for different use cases and even to enable proactive interventions. For example, one participant preferred that CA continuously monitor their activities and provide reminders. CA was perceived as a one- size-fits-all solution; in P017's words, ''I'm sure it's super convenient to have just everything autonomous for you''. P818 noted that CA could simplify user experience while providing secure and safer parental control, ''Kids will do terrible stuff with given full access. So I'm interested. I think it sounds somewhat secure and safer. I think I would love it more if like you said it was on a local network versus the internet. I'm into it. This is what I'm saying''. On the other hand, one participant voiced concern that CA could supplant the security and privacy awareness traditionally taught by par- ents, potentially leading future generations to become overly dependent on it.

Due to a lack of understanding about CA, participants tended to conflate its limitations with those of traditional technologies and, as a result, felt that the convenience offered by CA came at the expense of security and privacy risks:

If all of this does work and you can apply it to a real- life thing, then it definitely will make things way easier. Like opening your computer, you could do it really fast and you have to make a compromise, it's like, you can have an authentication method that's really easy [CA], or you can have something a little more old school and secure, but less easy. (P004)

P028 also acknowledged the trade-off between privacy, security, and usability, ''This new technology that tracks your behavior and stuff, watching the video, I don't want some device tracking my behavior. It feels weird. I think though it'll become convenient in a way. Almost like we give up some of our privacy for the sake of convenience or security''.

Participants felt that unreliable biometric recognition could compromise the convenience of CA as well. P028 com- mented, ''I think this system might be frustrating if in my own home I'm trying to do something and it's just not working. I don't need those additional minor stresses in my life and frustrations. Maybe sometimes it's really convenient. I feel like it could just get frustrating, no system's gonna be perfect. So it just depends on how well the system works''.

They also raised practical concerns regarding CA's cost and power consumption, indicating these as additional factors in their decision-making.

D. TRANSPARENCY

A central concern that emerged from our participants' opin- ions was Transparency. It is worth noting that in some prior work, the term ''transparent" means authenticating a user's identity invisibly-without interrupting the user with oper- ational details [15]. To avoid confusion, we define trans- parency here as the system's ability to remain invisible when identifying users at entry points. However, we argue that incorporating explicit authentication at specific points during continuous verification can help users better appreciate the protection provided by CA. Previous findings suggest that en- countering occasional barriers to data access on smartphones can assist users in forming a mental model of the security CA offers [46]. Moreover, participants' concerns about obtaining consent from guests further underline the importance of ex- plicit authentication, as discussed later in this section.

Throughout the focus group, participants commented on system security based largely on their perceptions, without investigating different systems in detail. Furthermore, their visions of CA were influenced by limitations of current technologies—particularly when CA lacks transparency. For example, compared to concerns about constant monitoring, many participants were more worried about having little knowledge regarding how CA manages their data and feeling a lack of control over it:

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

I think there are some concerns. How does it [CA] learn this behavior? How does it learn these things about me? And I think based on who's making it, which I think given our current world is probably gonna be meta or Google.

So I guess you decide how you feel about those two entities. And how they're getting that initial baseline data. I'm not too concerned about the constant monitoring because I think a realistic portion of this is where you store all of that data. You can't necessarily hold onto all of it. So that is not an issue with the constant monitoring. (P818)

Participants also expressed a desire for CA to let them adjust sensitivity levels, seeking more control over how responsive CA would be to their inputs.

Additionally, we found that context plays a crucial role when users trade security and privacy for usability. Participants were intrigued by the nuanced protection CA could offer for tasks with varying degrees of sensitivity and anticipated the ability to customize settings:

But it might be nice for a wake-up routine or having security in your home. If your house could detect a stranger in it, that might be a very useful thing. And then when you're at home, it's a security system and you can detect how sensitive you need it to be, like do you just need monitoring on these important aspects, and then you turn off the TV monitoring. I think there's like a granularity to it that might make this more acceptable for some people. For some people it might be, 'take over my whole house, that's great.' But for others it might be, 'keep an eye on that medicine cabinet, but leave the TV alone.' So I think that might be an interesting space to examine. (P818)

Our participants also sought transparency regarding CA's inherent mechanisms and its capability to handle multiple users within the same household. For example, one partici- pant asked whether CA obtains visitor consent before tracking their information in the smart home–a clear indication of the need for informed, explicit authorization when user roles differ.

Last but not least, participants expressed concerns about how well CA could handle urgent situations that might require altered authentication policies. They also wanted information about CA's cost and power consumption.

VI. DISCUSSION

We focus our discussion on 1) our conceptual model, 2) design recommendations and social implications for future CA systems, and 3) limitations.

A. OUR CONCEPTUAL MODEL

Throughout the focus group sessions, we gathered partici- pants' opinions about traditional authentication and CA. We presented a conceptual model with transparency as a mediat- ing factor to bridge the gap between participants' perceptions and the design of smart-home CA.

Participants elaborated on contexts in which they used conventional authentication systems and showed varying degrees of privacy and security awareness, leading to differ- ent authentication strategies developed around device-sharing needs (addressing RQ1). These strategies reflected that users made trade-offs based on perceived security, privacy, and usability when choosing between methods in different con- texts (addressing RQ2). When questioned about CA, despite expressing interest, participants pointed to the limitations of traditional methods, and their attitudes toward CA were influenced by their interactions with biometric authentication (addressing RQ3). Consequently, participants were hesitant to compromise their privacy and security for the sake of us- ability, especially when CA lacked transparency in collecting substantial amounts of data in smart homes. Nevertheless, participants acknowledged the benefits of CA in a smart home context. Participants sought automated authentication with- out explicit input while moving around the house (addressing RQ4). For example, they liked the constant monitoring of the medicine cabinet, especially since CA facilitates parenting by preventing children from accessing hazardous objects such as medicine and guns. This emphasizes the advantages of CA over traditional methods, extending beyond the point of entry to enable seamless user verification and a positive user experience.

We found that a significant limitation of conventional au- thentication methods is that they only provide entry-point logins and thus do not satisfy users' sharing needs. Throughout the focus group sessions, these methods were cited as incon- venient because they required explicit user input. Users had to authenticate frequently, remember additional authentication procedures, or prepare multiple backups. As a result, numer- ous participants chose to bypass traditional authentication. In addition, participants adopted biometric methods due to their perceived usability and a sense of

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

enhanced security. Our findings align with previous research indicating users' pref- erence for biometric CA over passwords on mobile devices due to its convenience [12]. However, there were concurrent concerns about the potential for device unlocking through spoofing. Similarly, concerns about the potential exposure of user biometrics to third parties led to low trust in the adoption of CA [9]. Our results suggest that while biometric CA holds the potential to enhance user experience, users expect it to be robust and secure. Prior work found that users' privacy aware- ness is related to the perceived vulnerability of behavioral biometrics [11]. These user concerns and behaviors reflect the challenges in data collection and management in future smart-home CA.

While embracing the convenience offered by CA, partici- pants expected CA to be able to adapt to different contexts. In the medicine cabinet example, participants discussed whether CA could detect urgent situations, such as when a child needs to fetch medicine for an ill or incapacitated parent from a locked cabinet. Prior researchers have argued that a context- aware CA system holds the potential to address emerging privacy and security concerns within the IoT environment [37].

It has been suggested that context-aware CA demon- strates enhanced security compared to conventional methods, as evaluated by real-world data [33]. Nevertheless, these discussions are grounded in the researchers' interpretation and selection of contextual factors, lacking the valuable input of user opinions that we collected. Our work shows that participants expressed a desire for control over CA and the data it collects, with the ability to customize it based on the context. This aligns with previous research indicating that users prefer systems offering granular security levels and user access control [46]. Baig and Eskeland [56] pointed out the challenges of CA in a survey paper, including maintaining data privacy, enhancing security (reliability and hack preven- tion), and improving the usability of biometrics. Our work adds to such prior research by qualitatively analyzing authen- tication schemes from the participants' perspective, and our interpretation bridges the gap between user attitudes and the design space of CA in a complex and integrated scenario–a smart home. Our findings reinforce those of previous studies while also introducing new insights into various use cases of CA.

B. DESIGN RECOMMENDATIONS AND SOCIAL IMPLICATIONS

We propose design recommendations for enhancing system transparency in terms of Technical Design, Implementation Flexibility, and User Interface Design.

Our study revealed that, despite CA being expected as a solution to offer fine-grained authentication in smart homes, participants' trust in CA was influenced by their unsatisfac- tory experiences with existing techniques. Participants ex- pected explanations regarding how CA systems would collect and utilize their data. Our findings align with the conclu- sions drawn by Ponticello et al., who highlighted system transparency and user control as key factors in establish- ing trust when introducing novel authentication technolo- gies [32]. Therefore, we provide design recommendations to improve the transparency of the technical design: CA should provide users with accessible, clear, and detailed information about its continuous monitoring, data collec- tion/processing, and sensitivity levels. The system should communicate how it secures, stores, and shares user data while highlighting potential risks or vulnerabilities. For ex- ample, prior research suggests enhancing transparency in IoT environments by sharing device communication through semantic behaviors like heartbeat signals, firmware checks, and motion detection [57]. Additionally, the system should communicate its consistent protections beyond entry-point authentication methods, ensuring that sharing user data with third parties or online services only occurs when necessary (e.g., to increase recognition accuracy). These technical de- signs could help users build trust in CA's privacy and security, especially those prone to hacks or data breaches (e.g., younger individuals and elderly people). Finally, CA should query users regarding the biometric modality they are comfortable being tracked with as authentication protocols, assigning dif- ferent modalities for tasks with different sensitivity levels to enhance security and reliability while maintaining usability.

When the technical design conveys transparency, con- text becomes crucial as participants weigh privacy/security against usability. We recommend that CA incorporates flexi- bility in its design: The system should execute flexible au- thentication protocols leveraging multi-modalities based on the context, communicate contextual factors to users, and provide granular customization options that allow users to make informed decisions. Contextual information (e.g., location and nature of the task) was used as input to CA in previous research and demonstrated improved security [33].

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

For smart homes, CA should adapt to user strategies of sharing devices and provide immediate, understandable feedback on specific processes (e.g., initial logins and context changes). For instance, when the system detects that multiple users are accessing a shared device, it should inform them of the authentication mode being used, such as a many-to-many matching system, and clarify that each user's data will remain private. Users have different roles and security levels even in the same household; therefore, higher-level roles (e.g., hosts) should be granted more access than guests. However, specific role assignment should be delegated to users by informing them of their control levels and offering a space for discus- sion and adjustment. In addition, the system should allow users to customize the levels of protection and monitoring based on specific contexts. For example, users should be able to set strict access controls on sensitive home areas while having more relaxed settings for shared devices. Last but not least, the system should recognize and adapt to urgency, providing immediate access when necessary without com- promising overall security by using override authentication protocols/modalities. Notably, greater contextual awareness comes with increased surveillance. The system should strive to balance contextual adaptation with user privacy.

Because our participants value context-awareness and sys- tem customization, we argue that providing a user-defined interface is crucial to helping them develop trust and control. CA designers need to take greater responsibility in interface design to facilitate acceptance: The system should provide a user-defined interface with visualizations of resource uti- lization efficiency and toggles explaining potential trade- offs. For example, an economic mode of CA could be de- signed for users who prioritize cost and power consumption in smart home environments, satisfying the needs of diverse user groups. The system could emphasize how it facilitates seam- less user interactions and improves overall user experience, helping users make informed trade-offs based on the benefits. The feature toggle could provide real-time visualization of associated trade-offs and impacts on risks and security for each user action.

Interestingly, our participants expressed that the adoption of CA may become inevitable in the future. They noted that CA may become normative over time, similar to current authentication technologies. This supports previous research showing that most existing technologies experienced initial pushback, especially recognition systems that encroached on user privacy while performing their services [58].

If CA becomes widely adopted, initially reluctant users may be influenced by early adopters, conforming to social norms and leveraging available resources to avoid falling behind. By im- proving technical design, implementation flexibility, and user interface design, the perceived security, privacy, and usability of this novel technology can be enhanced, facilitating CA's acceptance process.

VII. LIMITATIONS AND CONCLUSION

We conducted focus groups to uncover participants' authenti- cation strategies and decision-making processes. Our guided discussions range from traditional authentication methods to CA, collecting valuable perceptions grounded in real user experiences. However, our study has several limitations that should be considered when generalizing the findings. First, our participants were students from a local university. Future research involving a broader range of ages and backgrounds may provide a more representative sample. Nevertheless, we exerted every effort to recruit from the general population, recognizing our options were limited because we conducted the study in a college town. Despite this relatively narrow de- mographic, our results reinforce previous findings regarding key factors in CA design [41]. Second, our design probe video did not cover all possible use cases of CA in smart homes. However, the envisioning approach (i.e., using vignettes to prompt discussion) has been employed in numerous studies for designing technologies [47]–[50]. Our video scenarios draw on present-day user activities within the home, illustrat- ing multiple modalities and environments while anticipating future developments [45]. We designed open-ended, non- leading questions to facilitate discussion of generalizable CA use cases. As shown in Section V, participants expanded beyond the scenarios presented in the video by elaborating on their own preferred use cases.

While existing smart-home CA systems demonstrate com- mendable usability, there is a notable gap in evaluation stan- dards and consideration of privacy and security from the user's standpoint. Prior research, particularly in domains like mobile phones, has highlighted challenges related to user trust in CA security and usability, advocating for further exploration in the smart home context [12], [41]. Our study helps bridge the gap between users' attitudes toward CA in smart homes and current CA prototypes.

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

Our focus groups presented participants with various smart home-based CA use cases, prompting them to discuss their current authentication methods and device-sharing strategies. Our findings indicate that participants' attitudes toward CA are significantly shaped by past experiences and contextual factors, leading to diverse user needs and concerns. We con- cluded that conventional methods are insufficient to address the nuanced needs of smart home users, who expect CA to offer granular data control coupled with a seamless user experience. However, privacy and security concerns emerged prominently, with participants expressing apprehension about data breaches and hacks. These concerns create trade-offs between usability and privacy/security that vary based on specific contexts. Drawing from user perceptions of CA sys- tems, we present a conceptual model diagram and offer design recommendations emphasizing the importance of CA trans- parency as a mediating factor to improve technical design, implementation flexibility, and user interface.

Our work contributes to the ongoing efforts in designing CA systems that align with users' fine-grained understanding of authentication mechanisms, thereby enhancing their adop- tion in smart homes. Future work should adopt a holistic so- ciotechnical approach to explore the varying perceptions and interactions of users across different age demographics within the same household. This research should also rigorously examine the ethical implications and user consent dynamics, particularly focusing on the challenges and solutions related to differential permissions within these systems. Such stud- ies are crucial for developing inclusive and ethically sound technologies that resonate with diverse user experiences and values.

ACKNOWLEDGMENT

Heting Wang thanks previous reviewers for their insightful feedback on earlier drafts of this manuscript. Additionally, we utilized ChatGPT [59] for editing and grammar improve- ments.

REFERENCES

[1] H. Touqeer et al. ''Smart home security: challenges, issues and solutions at different IoT layers''. J. Supercomput., 77:14053–14089, 2021.

[2] T. K. Ghazali and N. H. Zakaria. ''Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment''. Journal of Computers (Taiwan), 29:189–208, Feb 2018.

[3] K. J. Kaaz et al. ''Understanding user perceptions of privacy, and con- figuration challenges in home automation''. In 2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), pages 297– 301, 2017.

[4] A. K. Jain, A. Ross, and S. Prabhakar. ''An introduction to biometric recognition''. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4–20, Jan 2004.

[5] H. Kong et al. ''Continuous authentication through finger gesture in- teraction for smart homes using WiFi''. IEEE Transactions on Mobile Computing, 20(11):3148–3162, Nov 2021.

[6] S. Rasnayaka and T. Sim. ''Action invariant IMU-Gait for continuous au- thentication''. In 2022 IEEE International Joint Conference on Biometrics (IJCB), pages 1–10, 2022.

[7] P. Bours and S. Mondal. ''Continuous authentication with keystroke dynamics''. Gate to Computer Science & Research, 2, 2015.

[8] G. Peng et al. ''Continuous authentication with touch behavioral bio- metrics and voice on wearable glasses''. IEEE Transactions on Human- Machine Systems, 47(3):404–416, Jun 2017.

[9] V. M. Patel et al. ''Continuous user authentication on mobile devices: Recent progress and remaining challenges''. IEEE Signal Processing Magazine, 33(4):49–61, Jul 2016.

[10] T. Neal and D. Woodard. ''Surveying biometric authentication for mobile device security''. Journal of Pattern Recognition Research, 11:74–110, 2016.