

Received 18 October 2022, accepted 13 November 2022, date of publication 23 November 2022, date of current version 30 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3224236

RESEARCH ARTICLE

How Perceptions of Trust and Intrusiveness Affect the Adoption of Voice Activated Personal Assistants

DEBAJYOTI PAL¹, MOHAMMAD DAWOOD BABAKERHELL²,
AND PRANAB ROY³, (Senior Member, IEEE)

¹School of Information Technology, Innovative Cognitive Computing Research Center (IC2), King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand

²Department of Information Technology, Shaikh Zayed University Khost, Khost 2501, Afghanistan

³Department of Computer Science and Engineering, Institute of Engineering and Technology, J. K. Laxmipat University, Jaipur, Rajasthan 302026, India

Corresponding authors: Mohammad Dawood Babakerhell (dawood.csf@gmail.com) and Debajyoti Pal (debajyoti.pal@mail.kmutt.ac.th)

This work was supported in part by the Asahi Glass Foundation.

ABSTRACT Voice Activated Personal Assistants (VAPA) are unique and different from other Information Systems (IS) due to their personalized, intelligent, and human-like behavior. Given the unique characteristics of these VAPA's, current technology adoption models are not comprehensive enough for explaining the usage of these systems. While trust and privacy have been identified as relevant issues affecting adoption of VAPA's, both these have been treated in a simplistic fashion that is not effective keeping in mind the complex nature of these factors. Moreover, being "always on", VAPA's are intrusive by nature: another aspect that current research has overlooked. Drawing on current findings in IS and artificial intelligence, we propose two different types of trust (cognitive and emotional) together with their antecedents (anthropomorphism, intelligence, VAPA privacy concern, household privacy concern, vendor & third-party privacy concern, and government privacy concern). The moderation effect of perceived intrusiveness on usage behavior is also examined. The proposed research model is empirically validated with data obtained from 466 VAPA users in India using a Structure Equation Modelling approach. We observe that perceived anthropomorphism does not affect emotional trust, whereas the effect of perceived intelligence on cognitive trust is significant. Social privacy concerns like VAPA and household privacy affect both forms of trust, whereas the effect of institutional privacy category is weak with only vendor & third-party privacy concern affecting emotional trust. Additionally, the findings establish the moderating role of perceived intrusiveness in dampening and negatively influencing the usage of VAPA's, with a stronger effect for large households.

INDEX TERMS Anthropomorphism, cognitive trust, emotional trust, perceived intrusiveness, voice activated personal assistant.

I. INTRODUCTION

In the recent years there has been a huge growth in the artificial intelligence (AI) based digital personal assistant market. Conversational interface that uses voice as the communication modality is the striking feature of these digital personal assistants, as advancements in natural language processing (NLP) and machine learning (ML) techniques have made it

The associate editor coordinating the review of this manuscript and approving it for publication was Akin Tascikaraoglu.

more intuitive and easier to use this form of communication mode over the more traditional text-based communication modality [1]. Since Apple's release of *Siri* back in 2011, the popularity of these voice-activated personal assistants (VAPA) has increased, as evident from various other commercially available products like Amazon *Alexa*, Google *Assistant*, Microsoft *Cortana*, and Samsung *Bixby* just to name a few. The presence of these VAPA's is now ubiquitous, as they are found both as software agents almost in all types of smart devices like smartphones, laptops, tablets, and smart-home

gadgets and even in devices having physical embodiment like smart speakers (e.g., Google Home, Apple HomePod, and Amazon Echo Dot). Due to their ubiquitous nature, these find application in a variety of scenarios ranging from smart-home solutions to weather forecast, playing music/videos, telling jokes, to even in voice-assisted smart vehicles for the purpose of navigation, or controlling on-board equipments. Using voice offers a lot of convenience to the users when interacting with the machines, as they do not need to physically interact with the machines apart from their voice [2].

Despite the advantages that VAPA's bring, current research suggests that many users are still reluctant towards adopting these type of voice-based systems [3], [4]. This reluctance can be due to the low perceived usefulness of such systems or lower levels of enjoyment while using such systems, both of which will lead to a lower system usage [5], [6]. Many times, the users also face with technical difficulties during interactions, due to pauses while speaking, repetition of words, accent of speaking, ungrammatical utterances, together with other inconsistencies that decrease the performance of VAPA's [7], [8]. Such scenarios alleviate user frustration, since when things go wrong during interaction with a VAPA the onus falls on the user to repair and start afresh such broken communications. The commercial VAPA's that are currently available in the market can be seen as "black boxes" that provide little information about such communication failures and rely on the users' experience and intuition for finding a solution to the problem [9]. Such an uncertainty and bad user experience is found to decrease the trust of humans on machines [10]. Privacy and security concerns are some of the other highly discussed factors by existing research that negatively affect the adoption of VAPA's. For example, researchers have demonstrated that voice-based systems can be easily manipulated [11], they can be controlled and operated remotely [12], and even most often users willingly disclose their information that they perceive to be non-personal [13].

From the above discussion the pros and cons of VAPA's are evident. In particular, through this work we would like to iterate the importance of the users' mental models and the need of trust in this voice-based paradigm. We make an attempt to directly respond to very recent works in [14] and [15] that call for further exploring the users' interactions with these systems, especially the trusting beliefs. Since trust is an implicit and fundamental tenet of human existence, it is imperative that emerging technological paradigm like voice-based systems will try to earn and build trust among its users for increasing their adoption and diffusion into the society. However, while other topics in Human Computer Interaction (HCI) have attempted to map the meaning and role of trust in different contexts like autonomous systems [16], e-commerce solutions [17], or even service robots [18], this has not yet been done in the VAPA context, and in general for any voice user interface. Users can have a range of issues while interacting with VAPA's that fall under the umbrella of trust, yet they might be fundamentally different. For instance,

a person may/may not trust a VAPA because they think that their personal information is not stored confidentially [19], [20], or they may not trust it because they think that it is malicious and trying to deceive them [20] and [21], or even because the user might not like the overall feel of the VAPA [22]. We argue that it is important to differentiate the different aspects of trust and what shapes them keeping in mind the specialties of the VAPA context: an aspect that has been ignored by current research.

One uniqueness of VAPA's is that these are "always on" as they continuously analyze every sound in their background to recognize the so-called "wake-up word" such as "Hey Siri", "Alexa", or "OK Google". Only after the wake-up word is detected, the VAPA's start interacting with the users, record the sound and upload it to a remote server (cloud based) where it is transcribed, and the detected word sequence is interpreted as a command. This "always on" listening mode makes these devices pervasive and intrusive. To make matters worse these wake-up words are not precise, and the devices may get triggered even when the words have not been uttered [23]. For example, Google's voice assistant misinterprets "cocaine noodles" as "OK Google" that can be exploited to execute unauthorized commands [23]. The problem is most of the time the users are aware of this "always-on" and intrusive nature of the VAPA's, yet it is unclear that whether such a perceived intrusiveness affects the usage of these devices. Quiet strangely HCI and information systems (IS) researchers have investigated various adoption related issues of voice-based systems [2], [24], [25]; however; very few of them have done so keeping in mind this inherent intrusive nature of voice technology, and whether the users get used to the presence of such devices or not. We strongly feel that for ensuring a wider diffusion of VAPA's in the society, the unique aspects that a voice-based interaction scenario presents must be considered, e.g., the perceived intrusiveness, anthropomorphism, intelligence, and various types of privacy concerns specific to this scenario. Since the VAPA's continuously sense the environment, we believe that the users would have a feeling of being continuously watched/spied upon that might in turn affect their usage of these devices. Therefore, it becomes imperative that trusting VAPA's is a central aspect, but as pointed out earlier what shapes trust in the VAPA context needs to be conceptualized and verified.

Based on the above discussion, the central theme of the current research is to conceptualize the idea of trust as applicable in the VAPA context together with the different types of privacy and human-like antecedents that might shape the different types of trust, keeping in mind the inherent intrusive nature of voice-based technology. Particularly, we propose four unique privacy concern modalities and two human-like traits (anthropomorphism and intelligence) possessed by the VAPA's that can affect trust. Following are the research questions of this study:

RQ₁: How do we conceptualize trust in the VAPA context and what are its antecedents?

RQ₂: What effect does perceived intrusiveness has on the usage of the VAPA's?

For answering the above questions, we have used a grounded theory approach for conceptualizing our proposed theoretical model. This is followed by a rigorous quantitative evaluation of the model based on data collected from an online survey. There are several contributions of this work. First, we provide a conceptual understanding of trust and what does it mean in the voice based HCI context. Second, we reason how privacy perceptions and anthropomorphism help in shaping trust. In doing so we include various privacy relational dynamics that current research has overlooked; yet are highly relevant for the present use case. For example, privacy concerns from family members or vendors add novelty in the context of emerging technologies like voice, and how they are related to trust formation. Third, VAPA's being a classical example of artificial intelligence (AI) based products, tend to have a certain degree of humanness. In a HCI interaction scenario such humanness may amplify (or diminish) a human's perception of goodness or badness of a technology, and consequently the extent to which it can be trusted. We have incorporated this anthropomorphic lens too as an antecedent of trust. Finally, we try to provide a theory-based reasoning as to how intrusive the users perceive the VAPA's to be that has an impact on their daily usage.

In the remainder of the article, first we provide a synthesis of the trust aspect and why it is needed to investigate this concept in the conversational HCI domain (Section II). This is followed by an analysis of the literature where we attempt to find out the various trust antecedents based upon the current gaps (Section II). Wherever applicable relevant hypotheses are proposed together with the theoretical model (Section III). The data collection and methodology is presented in Section IV followed by a detailed mathematical analysis in Section V. In Section VI the findings are contextualized highlighting the theoretical and practical contributions. Finally, Section VII provides the conclusion and drawbacks together with the scope of future work.

II. LITERATURE REVIEW

A. UNIQUENESS OF THE VAPA PARADIGM AND THE CURRENT GAPS

One unique capability of humans that separates us from other living beings is our ability to communicate via spoken languages. Therefore, it is quite natural for the research community to build computers that can understand human languages and communicate through voice. In the Industrial 4.0 era where each day more number of devices are getting connected to the Internet through the Internet of Things (IoT) technology, the use of voice to connect and control these multiple devices has become very important. Therefore, it becomes necessary to understand why people will adopt this new form of human to machine communication, along with their apprehensions in this regard.

Unlike other forms of human to machine communication, the VAPA paradigm has certain uniqueness as follows:

- These are hands-free, can be operated via voice
- Like human-to-human communication they use natural and conversational style of interface
- These are “always-on”, which makes them very intrusive
- These are often shared among multiple members of the same household
- The voice data is processed in the cloud
- During their interaction they try to opt for human personification
- These are a typical representation of anthropomorphic technology, wherein users try to build relationships
- These have typical personalities like human-like trait and behavior trait

These devices are activated by using some specific phrases, e.g., “Hey Siri”, or “OK Google”, due to which they are always-on and listen to their environment continuously. Likewise, for meaningful interactions these devices must always be connected to the internet, since all the processing happens in the cloud. However, there are several concerns related to whether these devices are secure, what happens to the voice data, who gets access to this voice data, and likewise [21], [26]. In many cases the voice data is stored by the vendors on the cloud outside a particular country where service is being provided [27]. Additionally, it is not known clearly as to how this voice data can be abused, e.g., for unwanted marketing purpose. All these suggest that voice-based human to machine communication is inherently very intrusive. On one hand the users know about the presence of a machine that is continuously listening to all the conversations going on, and at the same time they do not have any control over when, where, or how this personal voice data is getting stored and processed. Although there are several studies that have focused on various adoption aspects of the VAPA paradigm by considering dependent variables like behavioral intention [28], [29], [30], attitude [31], [32], [33], continued usage [34], [35], [36], user satisfaction [30], [36], or even perceived value [33], [37]; the central question of how trust is formed and what effect perceived intrusiveness has on the usage of the VAPA's has been unexplored.

Second, VAPA's are a typical example of anthropomorphic systems. Their conversation style and human personification makes users to perceive and interact with them in an intimate manner [38]. There are existing studies that focus on the effect of anthropomorphism on the adoption scenario [36], [39], [40]. Overall, the results suggest that people favor the personification, and it helps to improve the acceptance level. There is another view, however, which argues that the relationship between anthropomorphism and the use of such systems is non-linear [41], [42]. Beyond a certain level an improper calibration can create feelings of discomfort, unpleasantness, and eeriness for the users. This has a serious implication towards trust. For example, researchers have found out that if robots

TABLE 1. Current empirical studies on VAPA adoption.

#	Objective	Key Constructs	Anthropomorphism	Privacy	Trust
[2]	Examining factors motivating individuals to use smart speakers	Dependent: AU Independent: UB, HM, SB, SP, SA, PR	×	Privacy is treated as a moderator. Details of privacy dimensions not explored	×
[28]	Examining the perception of users towards privacy concerns that influence the adoption	Dependent: AD Independent: BI, EE, PE, HM, PV, FC, TR, PC, PR	×	Generalized. Not explored in detail	Trust as a single construct
[29]	Examining the attitude of users and how trust is developed	Dependent: INT Independent: PEOU, PU, HM, SP, SC, PC, ATT, TR	Focus on social closeness to technology	Generalized. Not explored in detail	Trust as a single construct
[30]	Examining user satisfaction and behavioral intention from system and information quality perspective	Dependent: INT Independent: ATT, PU, PEOU, IS, SS, IQ, SQ	×	×	×
[31]	Developing an acceptance model for investigating consumers' intention to use smart speakers	Dependent: INT Independent: PU, PEOU, HM, PR, TO, SQ, SD	×	The issue of surveillance is examined. However, privacy types are not explored	×
[33]	Examining the factors affecting consumer's attitude towards smart speaker through perceived values	Dependent: CI Independent: ATT, HM, SV, EV, FV, CO	×	×	×
[34]	Examining factors affecting the willingness to disclose personal information that affects continued usage	Dependent: CI Independent: PID, PR, PB, HM, TR, PS	×	The issue of information disclosure is examined. However, privacy types are not explored	Trust as a single construct
[35]	Exploring the utilitarian and hedonic attitudes of users towards continued usage of smart speakers	Dependent: CI Independent: UE, TR, PR, SS, HM, UB	×	Generalized. Not explored in detail	Trust as a single construct
[36]	How the smart speakers voice interaction creates a flow experience that affects user's attitude and behavior	Dependent: SS, CI Independent: FI, CR, SN, FE, VI	Dependent: SS, CI Independent: FI, CR, SN, FE, VI	×	×
[37]	Examining factors related to adoption of smart speakers from the platform perspective	Dependent: AD Independent: PV, PR, PB, PC, EV, FV	×	Generalized. Not explored in detail	×

Note: AD (adoption), ATT (attitude), AU (actual usage), BI (behavioral intention), CI (continuance usage intention), CO (Coolness), CR (creativity), EE (effort expectancy), EV (economic value), FC (facilitating condition), FE (flow experience), FI (functional intelligence), FV (functional value), HM (hedonic motivation), INT (usage intention), IQ (information quality), IS (information satisfaction), PB (perceived benefits), PC (privacy concern), PE (performance expectancy), PEOU (perceived ease of use), PID (personal information disclosure), PR (privacy risk), PS (personalized service), PU (perceived usefulness), PV (perceived value), SA (social attraction), SB (symbolic benefit), SC (social cognition), SD (system diversity), SN (sincerity), SP (social presence), SQ (system quality), SS (system satisfaction), SV (social value), TO (technology optimism), TR (trust), UB (utilitarian benefit), UE (user engagement), VI (voice interaction)

are too human-like, the users do not tend to trust them [43]. Keeping in mind the intrusive nature of the VAPA paradigm as discussed above, we argue that trust is a key factor that will determine user's behavior. If the trust is too high, it can lead to "overtrust" that might result in detrimental behaviors. Some of these behaviors can be fatal, for example when supervising an autonomous vehicle the failure to monitor such a system [44]. Likewise, if trust in the system is too low it can lead to "undertrust" that may in turn lead to lower adoption [45]. Therefore, in the presence of anthropomorphism proper trust calibration is important and it is an important aspect that shapes the adoption scenario.

In Table 1 we have summarized some of the recent studies that have focused on the VAPA adoption. As evident from the results, the scope of current adoption related research is confined to measuring the usage intention, satisfaction, value, or attitude towards these devices. These issues are discussed in detail in the next sections.

B. HUMAN COMPUTER TRUST IN THE VAPA CONTEXT

Human computer trust (HCT) is an important aspect in any type of interactive systems [46], [47]. It can be thought of as a combination of confidence in a system and the willingness to act as per the recommendations provided by the system. Based on the analysis of current VAPA literatures, we identified three distinct research themes related to the trust aspect of these voice-based systems: aesthetic driven trust (ADT), usage driven trust (UDT), and transparency driven trust (TDT) (Figure 1). ADT emerges from the design features of VAPA's, e.g. haptics, form factor, voice features, and gender of voice [46], [47], [48]. There are two broad sub-themes of this research area: visual, and auditory. Visual trust formation is related to embodiment, coolness of looks, and avatars [33], [46], [47]. Presence of these design cues has shown to improve the trustworthiness of the systems. The second aspect of auditory trust emerges from voice-specific properties of the VAPA, e.g., tone, pitch, accent or even

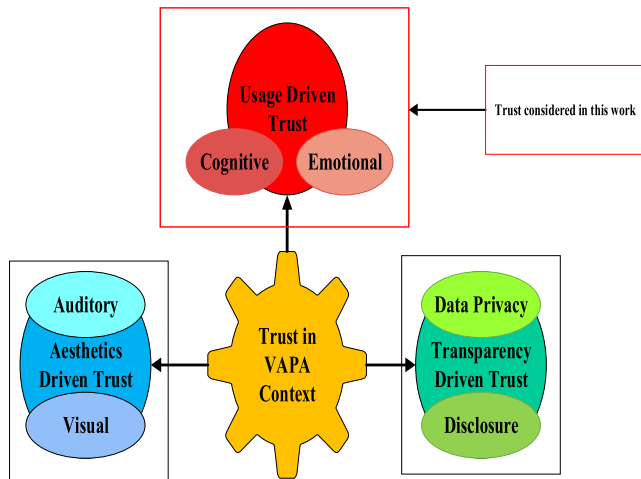


FIGURE 1. The three dimensions of trust in VAPA context.

gender [48], [49]. Generally, it has been observed that natural sounding voice (like humans) are capable of eliciting higher trust levels than synthetic voice (like text to speech) [50].

Usage driven trust (UDT) emerges out from the interactions that happen between human and VAPA's over a period of time. We identified two distinct sub-themes for this category: cognitive and emotional trust. Cognitive trust refers to the experience-based confidence that users develop by evaluating their overall experience and information pertaining to the competence of the VAPA's. The users apply their mental models and develop a perception based upon the knowledge and evidence they receive from these systems, which they expect to be reliable and deliver the intended promises [51]. Competency of the VAPA's is therefore one key aspect in this regard that makes the users believe that these systems have appropriate knowledge and skills [52].

On the other hand, emotional trust is developed when the users feel that they have established some relationship with the VAPA's, either because they are responsive, or they demonstrate care and concern [52], [53]. This leads to the development of an emotional bond. The VAPA's show varying degree of care, empathy and warmth during their interaction with the users [54], [55], which results in emotional exchanges that are critical for emotional trust to develop [38].

Transparency Driven Trust (TDT) is related to the degree of understandability and transparency provided by the VAPA's (normally their vendors) to the users in terms of their data collection and processing. For instance, self-disclosure has often been discussed in current literatures as an effective way to boost trust [56], [57]. The VAPA's should frequently communicate with the users regarding what data they are collecting in return for what value users get. Thus, there must be a transparency with regards to how user data is being dealt with. Greater the transparency, more will be the trusting belief.

As evident from the above discussion, the three dimensions of trust that we present are unique. Aesthetic driven trust is more relevant for the designers of voice-based systems,

as it enables to choose the most appropriate technical factors that must be kept in mind while building such systems to maximize trust. Usage driven trust on the other hand considers the interaction scenario between the users and VAPA's. Therefore, this dimension is most relevant for the present case since the objective is to see whether presence of these devices have any effect on the user adoption. Additionally, the third dimension of transparency driven trust is also extremely relevant. However, this dimension is more concerned with data privacy issues, and how these issues affect trust. Considering the importance of privacy, and the mention of this concern in almost all recent HCI and IS literatures related to technology adoption of VAPA's, we decided to treat this as a separate construct conceptually. Our analysis of the current literatures shows that although privacy concern has been a popular construct per se, however, its usage and conceptualization is oversimplified. This issue is discussed in the next section. Therefore, for this study we refer to trust as it is formed from the interaction between users and VAPA's in a cognitive or affective (emotional) format.

C. PRIVACY CONCERNS IN THE VAPA CONTEXT

Several studies have looked into the privacy aspects of the VAPA paradigm. These systems are being used in multiple locations and in diverse ways [58]. The sensitivity of an activity, the type of data collected, the data retention period, and even the physical location of the sensed data will affect how much comfortable people are sharing their information [59]. For example, authors in [59] found out that users do not want to share their data in scenarios which they perceive to be risky and feel that the collected data will be misused and be harmful for them. Likewise, using VAPA's in a public location can be uncomfortable [13]. Generally, people are cautious when sending private information that depends on factors such as their location (public vs. private place) or even on the communication modality (keyboard vs. voice) [13]. Overall, it has been revealed in the VAPA context that privacy risks are highly relevant, and they weaken the relationship between the users motivation and actually using these systems [2]. Table 1 also suggests that till date researchers have taken an undifferentiated view of privacy where the multiple stakeholders involved in the VAPA context have been ignored. The differentiation between the privacy risks presented by the devices themselves, the manufacturing vendors (e.g., Amazon, or Google), any third parties or additional stakeholders is not clear. Authors in [60] tried to differentiate this privacy aspect for Amazon Echo and Google Home users by analyzing online reviews and conducting a survey. They identified seven different type of privacy concerns: hacking the device, collection of personal information, recording private conversations, listening 24/7, respecting the user's privacy, data storage repository, and creepy nature. Although these findings are useful and enable conceptualizing different privacy dimensions, but the results are descriptive, and not motivated by any type of privacy theory. Similar exploratory studies have been conducted by authors in [61] and [62]

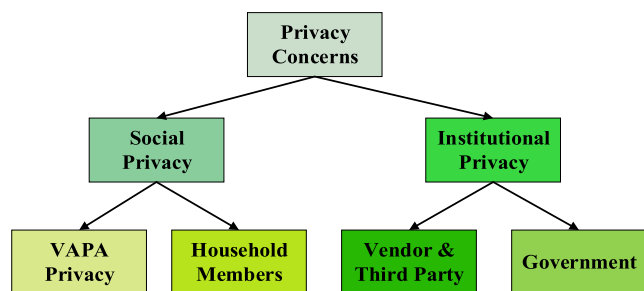


FIGURE 2. The four types of privacy in VAPA context.

seeking the perception of household users, visitors and other incidental users where a variety of concerns were identified ranging from data collection, monitoring, data usage, targeted advertisements, to selling data, however, these results too were not motivated by any privacy theories.

Based on the current works, we propose four distinct privacy concerns under social and institutional categories (Figure 2). We identify these categories based on the source of privacy concern origin. If the privacy concerns emerge due to the system itself (VAPA's in the present context) or due to the users themselves, we classify them into the social category. Likewise, if the privacy concerns originate from any other source except the system itself or the users, we classify them into the institutional category. This classification of privacy concerns under social and institutional heads has been well documented by existing privacy literatures also [63], [64], but has been overlooked in the VAPA context. Below we present a brief explanation of each of these privacy concerns:

(i) VAPA Privacy Concern (VPC): This type of concern arises from the system itself. These devices are used for a variety of purpose and are considered to be "social agents". Whenever, a device or system is perceived as a social agent, users tend to develop a relationship. As outlined previously also, VAPA's are different from other interactive technologies like video games, or web browsing, in that users communicate via their voice, similar to human-to-human communication. These devices have to be always on to serve the users, making the usage context highly intrusive. Therefore, being on and listening to background conversations 24/7 together with recording these conversations to be analyzed either in real-time or later can lead to privacy concerns due to the social nature of the VAPA's. As evident this type of privacy concern arises due to the inherent nature of the system itself.

(ii) Household Member Privacy Concern (HPC): Typically, VAPA's are shared among multiple family members and can be used for tracking and surveil purpose also. By default, all conversations of the VAPA's are logged, which can be accessed by the account holder of the device. Under certain scenarios, such surveillance may seem to be appropriate, for e.g., parental control of young children for ensuring that they are not accessing age-inappropriate contents. However, on a broader perspective research has shown that such surveillance may lead to a power imbalance among the family members in terms of technological intimate household member

violence [65]. For instance, it is possible to monitor every movement, search activity, and even the conversation of the victims through these VAPA's. Therefore, the presence of these devices can create conflicts and tensions in the user's mind. The users are not only concerned about their conversations getting recorded (VPC) but are also concerned about their privacy getting violated because somebody else might be able to listen in on them. Further, research has shown that the collected conversational data is used for the purpose of targeted advertising [62]. Such personalized ads might be too personal that the user feels uncomfortable sharing those with other family members. This unique aspect of VAPA's where they are used and shared as a common household device although has been known to researchers, but the corresponding privacy implications have sadly been ignored.

(iii) Vendor & Third Party Privacy Concern (VTPC): The voice data collected by the VAPA vendors like Amazon, Apple or Google are used for profiling purpose for provisioning targeted advertisements [62], [66]. The data is collected, and user profiles are generated that add value and monetize the VAPA vendors [66]. For e.g., profiling helps Amazon to motivate users with special offers for voice-based shopping that will ultimately help its e-commerce segment to grow. Likewise, these vendors listen to the recordings for improving their services. This has serious privacy implications as the personal conversations and sensitive information are being heard by the vendors. It has even been reported that sometimes these audio recordings have been subjected to mockery, raising concerns about the sensitivity and professionalism of these invisible stakeholders. Apart from the vendors there are third parties/app developers who develop so-called "skills" or "apps" that enhance the user experience with the VAPA's. These skills/apps may be developed for various purposes, like food delivery, checking account balance, or even reading stories. For developing these skills/apps the user data needs to be shared with these third-party developers. These external developers often act as the first entry point of selling the customer data to data brokers [67]. Therefore, this entire data eco-system may have leaks, and these third-party developers may not always have the correct intentions. Given the sensitive and personal data that VAPA's collect, privacy concerns arising from the vendors and third-party developers can be problematic.

(iv) Government Privacy Concern (GPC): The role of government and regulatory bodies in protecting the consumer's privacy cannot be overlooked. Recent global developments suggest that the responsibility of keeping user's data private is gradually shifting from the users to the government [68]. For example, the European Union (EU) formulated the General Data Protection Regulation (GDPR) act, which provides users with rights related to the collection and storage of their personal data. With respect to GDPR, while some vendors have added additional configuration options in terms of compliance modules, these are often perceived to be difficult to be navigated by the users [68]. Likewise, other vendors often block access to their services when accessed from within

the EU in order to avoid having to comply [69]. In the VAPA paradigm most of the processing happens in the cloud, making the data flow almost worldwide. Yet, individual data can be used in the local courts. For example, in USA for a specific case data from VAPA was subjected to subpoena, raising concerns about how government and other agencies could gain access to the private recordings [70]. Therefore, from an institutional view point the ability of government to access private information, the government spying through these devices, or even voice data being produced as evidence in court are all concern areas in the VAPA context that cannot be overlooked.

D. ANTHROPOMORPHISM IN THE VAPA CONTEXT

Anthropomorphism describes instilling non-human agents with real or imagined behavior, together with human-like characteristics, motivation, or emotions. Humans tend to anthropomorphize and generate social expectations from the VAPA's, although they know that these are non-humans [29], [50], [53]. In the broader AI applications scenario previous studies have explored various anthropomorphic system components like facial expressions [71], voice features [9], attractiveness [33], [71], personality [36], and playfulness [2], [8] among others. Although these are a part of the greater anthropomorphic notion, yet such a broad coverage is beyond the scope of the present work. Instead, we focus on the users' perception of the system to be human-like, i.e., perceived anthropomorphism, which is based on the characteristics the VAPA's possess. We have adopted anthropomorphism as described by authors in [72], who proposed that this can result from features and attributes that are either uniquely human (such as cognition, sociability, agreeableness and openness), or typically human (extraversion, warmth, emotions, and friendliness). We decided to use this flavor of anthropomorphism since there have been numerous studies that investigated both these scenarios in the VAPA context. For example, works in [36], [52], and [53] have taken the uniquely human approach, while those in [40], [47], [50], and [54] have taken the second typically human approach.

A second closely related aspect (but somewhat different) with anthropomorphism is that of intelligence. The VAPA's will be perceived to be intelligent if they understand the user's commands properly, and act according to what they have been instructed to do. Moreover, since these are devices having AI built into them, it is expected that over a period of time they will be able to learn from the newly acquired information and user's behaviors, and able to complete the tasks satisfactorily. Therefore, initially when the VAPA's are put into service it is expected that they will assist in whatever the users instruct them to do. Over time, they learn more from the user interactions, and try to make this interaction scenario more engaging. This change in perception of initially perceiving the VAPA's merely as a tool for task completion to a more engaging and collaborative means of decision making has been discussed in current literatures [73], [74]. Therefore, it becomes evident that competency of the VAPA's is the key if

these are to process information efficiently and communicate effectively with the users.

The perceptions of anthropomorphism and intelligence as discussed above might seem to be confusing because they have a high overlap as per current literatures [75]. Highly anthropomorphic systems might naturally be associated with higher intelligence. However, we argue that conceptually these are two separate ideas due to which it is best to treat them as separate theoretical constructs. For instance, whenever any search engine is used (e.g., Google search) it is not only able to predict the intended search terms and autofill them but is also able to learn and remember our prior search pattern and behavior. Therefore, such systems although can be perceived to be highly intelligent by the users, do not have any aspect of anthropomorphism. Likewise, children's toy (e.g., robotic elephant) can move or make elephant like noises (more animal like), but not able to interact or process any information that makes them score high on the anthropomorphic aspect, but not having any intelligence. In case of VAPA's they might possess both attributes, but to varying degrees. They are intelligent because they respond to the user's commands either for fulfilling tasks or supplying information that is useful and relevant. Simultaneously, since they communicate via voice they can display humor, disappointment, and emotions that typically lead to anthropomorphic perceptions.

From the above discussion the research gaps are clear. None of the studies have taken into consideration the intrusive nature of the VAPA context and how this can affect the user adoption. In fact, intrusiveness can lead to disturbance, irritation, and lesser trust. There is no conclusive answer as to whether the normal household conversations get affected when users are aware of the presence of these devices. Trust is therefore a central idea in such a scenario, together with the anthropomorphic lens and privacy concerns that users have. This anthropomorphism, privacy, trust chain shaping users' adoption in the intrusive VAPA context is underexplored. Additionally, although existing literatures have highlighted the importance of privacy concerns, yet they present an undifferentiated view of privacy that fails to justify the intrusive as well as the relational nature of this paradigm.

III. HYPOTHESES AND RESEARCH MODEL DEVELOPMENT

Based on the research gaps identified in the previous section we develop a model that measures the in-home usage scenario of the VAPA's. This model is based on the cognitive and emotional aspects of trust that are formed from different anthropomorphic and privacy perceptions of the users that in turn affects the usage scenario. Further, the proposed model also explains the role of perceived intrusiveness as a moderator between both types of trust and the usage scenario.

A. PERCEIVED ANTHROPOMORPHISM AND TRUST

We define perceived anthropomorphism as "*uniquely human or typically human like characteristics possessed by the VAPA's like sociability, openness, warmth or emotions that*

leads to the users perceiving these non-human agents to be possessing human-like traits". The VAPA's have a lot of social and emotional cues due to which the users might perceive the interactions to be like interpersonal. Such personalized interactions have been found to reduce uncertainty and make the users feel more comfortable about relying on these systems [40], [51]. This is similar to the parasocial relationship phenomenon in which television viewers form an emotional connection with their television characters [38]. Consequently, a person's development of a social and emotional bond with these VAPA's can motivate their ongoing trust with these devices. Moreover, research has shown that politeness, humor, or empathy exchanges that are seen with these VAPA's lead to a greater emotional bonding and trust [38]. Overall in the conversational AI context, although a significant relationship between anthropomorphic cues and trust perceptions seem to exist [39], whether such a trust is cognitive or affective by nature is not clear. However, since perceived anthropomorphism leads to development of social and emotional cues between man and machines, wherein an attachment and relationship is developed, we attribute this to the emotional trust. Thus, we hypothesize:

H_1 : Perceived anthropomorphism (PA) is positively related to emotional trust

B. PERCEIVED INTELLIGENCE AND TRUST

The users use the VAPA's for a variety of purpose ranging from utilitarian to hedonic activities. Whatever might be the usage purpose, if the VAPA's are able to respond back with the needed information or able to complete the assigned tasks successfully within a reasonable time period, users will tend to rely more on their services. We define perceived intelligence as "*the competency possessed by the VAPA's that enables them to understand the user's commands properly and provide satisfactory response with regards to what they have been instructed to do.*" From the definition itself it is evident that perceived intelligence is related to the user experience received in terms of the usability of such systems. If the VAPA's are competent then they will be capable of giving a consistent level of performance, making them not only useful for the users, but also develop reliance on them. Specifically, in the VAPA context to the best of our knowledge research on perceived intelligence has been very limited. Authors in [38] found that perceived intelligence is related to trust in AI applications, however, the research was purely qualitative in nature providing no empirical basis. Moreover, it considered AI applications in general, ignoring the specialties of the VAPA paradigm. In other marketing and business literatures, often the technical quality of the service output together with the functional service quality have been found to affect the seller's trust [39], [76]. We expect that this observation will also be true for the interaction between the user's and VAPA's, because ultimately the objective is to develop an effective and trusting relationship. If we compare VAPA's with other non-intelligent systems, they are capable of giving a far superior interaction quality due to their

efficiency, goal-oriented nature, and ability to understand and communicate in natural language. Therefore, experience with VAPA's will enable generating cues related to their competence that in turn would help in shaping mental models related to trusting these systems. Thus, we propose:

H_2 : Perceived intelligence (PI) is positively related to cognitive trust

C. VAPA PRIVACY CONCERN AND TRUST

As social agents the VAPA's pose certain privacy concerns. This type of concern arises due to the nature of the system itself, as we have outlined previously in the literature review section. We define this construct as "*the characteristics associated with VAPA systems that poses threat to an individual's privacy due to continuous gathering of information beyond the individual's knowledge, and sometimes control.*". Current research has shown that devices such as Amazon Echo have security vulnerabilities that lets hackers get full control over these devices and exploit them [11]. This makes the devices behave unexpectedly, for e.g., giving wrong information, triggering unwanted actions like switching on/off home lights, etc. Such unwanted and unexpected outcomes can lead to a loss of confidence in these systems and induce user frustrations that in turn will dampen both the cognitive and emotional trust aspects. Similarly, when talking on sensitive topics even with other household members like banking/financial transactions, individuals are reluctant to do so in the presence of VAPA systems [13]. Not only these systems continuously sense the background environment, but they also require an extended set of software permissions to perform their various tasks, which users overwhelmingly provide [2]. Often this alleviates the risks of stealing passwords, financial details, and seemingly unsecure private conversations that reduces user's trust on these systems. Thus, we propose:

H_3 : VAPA privacy concern (VPC) is negatively related to cognitive trust

H_4 : VAPA privacy concern (VPC) is negatively related to emotional trust

D. HOUSEHOLD MEMBER PRIVACY CONCERN AND TRUST

Currently, VAPA's are an integral part of any smart-home ecosystem, which makes these devices getting shared among different household members. We operationalize this construct as "*the conflicts and tensions arising in the users mind due to the power imbalance together with the uncomfortableness of disclosing personal information to other household members.*". Being shared devices, current research has shown that it creates tensions among the different stakeholders – parents, children, siblings, and roommates [65]. Often there is a concentration of expertise, access and control with the person who selects and install these systems [65]. Such an aspect leads to a variety of abuses, harassment or violence of the members [65], [77]. For example, domestic abusers can monitor the movements, activities, location and even

conversations of the victims through the VAPA devices [22]. Such conflicts and tensions among household members will be affecting their trusting attitudes towards the VAPA's. Likewise, due to the highly personalized nature of these devices they might announce promotional advertisements or content in the presence of all the family members that might be uncomfortable or uneasy for some of the family members. Such uncomfortableness and uneasiness can develop negative emotions towards the VAPA's leading to a loss of trust. Therefore, we propose:

H₅: Household member privacy concern (HPC) is negatively related to cognitive trust

H₆: Household member privacy concern (HPC) is negatively related to emotional trust

E. VENDOR & THIRD-PARTY PRIVACY CONCERN AND TRUST

Lack of data transparency and what the various VAPA stakeholders do with the collected data has been one of the major concern of the users [3], [62]. The VAPA's blend so well with the user's daily life that often there is a lack of control and accountability of their working that leads to various concerns, specifically reliance on vendors and third-party providers. In this work we define this concept as *"user concerns with respect to unconsented personal data collection and their subsequent misuse and mishandling by the device manufacturers or third-party developers that leads to personal data leakage and/or user harassment"*. Often the users are unaware or unsure about the vendors keeping their voice recordings for an indefinite time and for what purpose they are analyzed. This opaqueness creates misconceptions and raises concerns in the user's mind. Audio recording capability of the VAPA's create the potential to amass huge amount of data from individual users. The influx of this big data can fundamentally change the nature and strength of the predictive models that companies generate for their users. The problem is, although this data gets generated by the users, yet they do not have any rights to such individual profiling. Current research has termed this as opportunistic behavior by the vendors and third parties, which is detrimental to any forms of trust [28], [78]. Consequently, the users lose their confidence about the credibility of these stakeholders and feel that they will not be able to deliver their intended promises, which in turn decreases the cognitive trust. Likewise, the third-party developers often act as the entry point in the supply chain of selling user data to the data brokers [67]. This can result in several unwanted consequences like harassment due to tele-calling, spamming of e-mails or even abusing on various social media platforms. In terms of emotional security this will reduce the user's faith, and they will perceive the VAPA's to be uncaring and unemotional, thereby effecting the emotional trust. Thus, we hypothesize:

H₇: Vendor & third-party privacy concern (VTPC) is negatively related to cognitive trust

H₈: Vendor & third-party privacy concern (VTPC) is negatively related to emotional trust

F. GOVERNMENT PRIVACY CONCERN AND TRUST

For any country government forms the primary institutional pillar for maintaining and safeguarding privacy of the people. However, with the emergence of innovative forms of digital technology including the VAPA's the stance of the government is unclear. While on one hand, laws like GDPR in Europe or Personal Data Protection Act (PDPA) in multiple Asian countries aim for protecting the user's privacy, but at the same time there have been reports of continuous government surveillance and access to user's data in the name of national security. In fact, in Germany, which is typically viewed as a privacy-focused country the government has announced that for fighting crime effectively it is important for the federal and state agencies to have access to the data collected by voice assistants like Alexa or Siri. As users of VAPA's, therefore it becomes a concern that various institutional mechanisms might be continuously surveilling in the background. Such a privacy aspect is new, and we define this construct as *"the user concerns generating from continuous government surveillance and snooping of voice data that leads to a loss of confidence in such mechanisms"*. For example, in recent past Arkansas police (in USA) issued a warrant to Amazon to hand over audio recordings from an Echo device of a particular user as a part of a murder investigation process [79]. This case highlighted how unclear current legal mechanisms are, and how aggressive law enforcement and interest in data can undermine the physical sanctity of user's homes and lives.

We argue that such incidents not only reduce the competence and effectiveness of government as a privacy protecting mechanism for the people (cognitive trust), but also serves as a deterrent for the users to develop any form of relationships with the VAPA's (emotional trust). The notion of continuous surveillance will make the users uncomfortable and less secure to use the VAPA's. Therefore, we propose:

H₉: Government privacy concern (GPC) is negatively related to cognitive trust

H₁₀: Government privacy concern (GPC) is negatively related to emotional trust

G. TRUST AND USAGE OF VAPA'S

Current IS literatures support the role of trust in predicting usage of systems for various contexts ranging from m-commerce [80], blockchain technology [81], to the conversation AI scenario [28], [29]. However, as outlined previously for the VAPA context the role of trust in predicting the usage scenario has been oversimplified. IS literatures have repeatedly treated trust to be multi-dimensional in nature, although these dimensions may vary as per the usage context. In this work we consider two such relevant dimensions: cognitive and emotional trust. We define cognitive trust as *"experience-based confidence that users develop by evaluating their overall experience and information pertaining to the competence of the VAPA's that enables them to rely on these systems"*. Emotional trust is defined as *"the feelings*

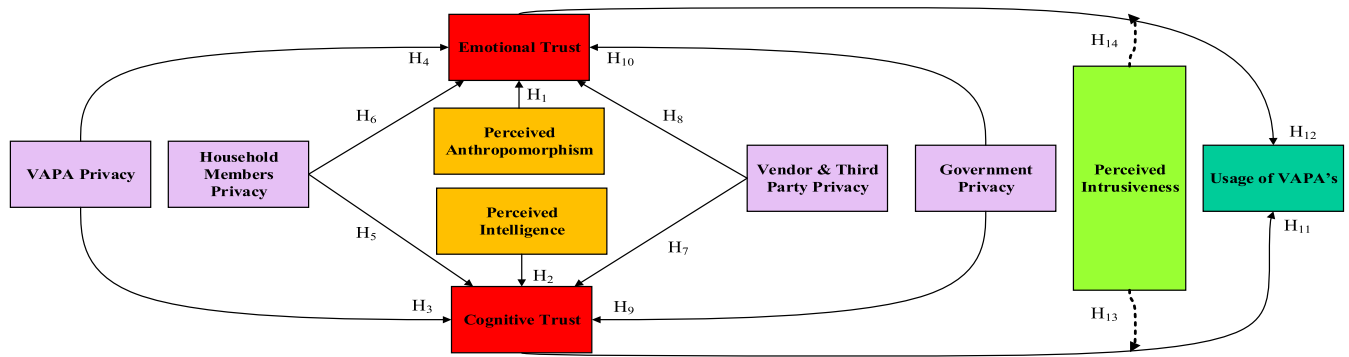


FIGURE 3. Research model.

of care and concern that users develop for the VAPA's after using them which helps creating an affective attachment and reliance". Both these types of trusts cannot be developed instantly if a user is using a technology or system for the first time [82]. These develop over a period of time as users keep on interacting with the systems [82]. Cognitive trust is more knowledge and competence driven that arises from the accumulated experience of the users after using the system that allows them to make predictions with certain level of confidence, regarding the likelihood that such systems will live up to the trusting perceptions. On the contrary emotional trust is the confidence that users place on the systems based on the generated feelings by the level of care and concern that the systems demonstrate. Such experience-based trust may affect the usage scenario, because if the trusting perceptions are not strong then the users will more likely not use the systems or may even switch to other alternatives [39], [82], [83]. Thus, we propose:

H_{11} : Cognitive trust (CT) is positively related to the usage of the VAPA's

H_{12} : Emotional trust (ET) is positively related to the usage of the VAPA's

H. MODERATING EFFECT OF PERCEIVED INTRUSIVENESS

Perceived intrusiveness is defined as "the perception of the users that the VAPA's abusively penetrate into their private lives". The notion of intrusiveness is highly relevant in the VAPA context. These devices have always-on microphones, cameras, and IR sensors that typically entail constant connectivity by continuously monitoring the background environment. Such 24/7 surveillance leads to the acquisition, storage and use of personal data for monitoring and controlling many things from screen-time and hygiene habits to meal and travel schedules and various other activities [84]. Such continuous surveillance has a negative connotation as the users feel that such intrusiveness is disturbing, irritating, and indiscreet [84], [85]. Another reason as to why the perceived intrusiveness of the VAPA's are high is because they are not only continuously listening for the magic "wake-up" word, but often times can make mistakes in the form of unintentional activations [23]. Such unintentional activations are likely to be at odds with

the user's usage scenario, creating a misfit between the two. When the users will perceive the VAPA's be intrusive, they will also feel a reduction in their trust levels [86]. Thus, it becomes evident that perceived intrusiveness will have a dampening effect between both forms of trust and the usage of the VAPA's. Accordingly, we hypothesize:

H_{13} : Perceived intrusiveness (PIN) will have a moderating negative effect on cognitive trust influencing individual's usage of the VAPA's

H_{14} : Perceived intrusiveness (PIN) will have a moderating negative effect on emotional trust influencing individual's usage of the VAPA's

Following the above conceptual discussion, Figure 3 provides the pictorial representation of the proposed hypotheses. The research model also accounts for four control variables, namely, age, gender, usage frequency, and household size on VAPA usage.

IV. RESEARCH METHODOLOGY

We conducted an online survey of VAPA users using the professional SurveyMonkey platform in India. This research has been approved by the human ethics board of the university, and also informed consent was obtained from all the participants. We used SurveyMonkey to recruit the respondents because it enables to reach the intended sampling frame based on the desired demographics in a convenient manner. This aspect is specifically important in a developing country like India where smart technologies are still evolving, which makes it difficult to find a trustworthy sampling frame [28]. Moreover, such professional data collection platforms ensure good data quality, and user friendliness. We did not limit our survey to any specific type of VAPA devices like Alexa or Siri, rather considered any type that the users were using to have a more realistic view of the current conversational AI scenario. The survey was administered for a period of three months starting from December 2021 to February 2022. We imposed only one strict screening requirement: respondents needed to have at least 6 months of usage experience with any VAPA. This was done because both cognitive and emotional trust cannot develop overnight as these are different from initial trust [82]. Hence, users need to interact with the systems

TABLE 2. Descriptive statistics of sample demographics (N = 466).

Characteristics	Indicators	Frequency	Percentage
Gender	Male	281	60.3
	Female	185	39.7
Age	Less than 25 years	49	10.5
	25 – 34 years	185	39.7
	35 – 44 years	151	32.4
	45 – 54 years	67	14.4
	55 years or more	14	3.0
Education Level	High school/diploma	92	19.7
	Undergraduate	218	46.8
	Graduate (Master's)	137	29.4
	Graduate (PhD)	19	4.1
Usage Experience with VAPA's	6 months – 1 year	229	49.1
	1 – 2 years	166	35.6
	2 years or more	71	15.2
Usage Frequency with VAPA's	Several times/ day	193	41.4
	Daily or almost daily	235	50.4
	At least weekly	38	8.2
Household Size	At most 2 persons	275	59.0
	At least 3 persons	191	41.0

and develop some experience for both these trust types to develop. Data were gathered from 541 respondents, of which 49 were unusable either due to missing values or respondents answering all the questions with the same value or following a pattern. Further, during analysis we found that the usage frequency of 26 respondents were seldom (at most once a month). We felt that such infrequent and intermittent users could bias the results because most probably although they have experience using VAPA's, yet they might have discontinued their usage. For both forms of trust to develop users not only need to have considerable experience but also be active users of these systems. Therefore, our final sample size was reduced to 466. Table 2 provides an overview of the sample demographics.

We adapted all the measures from existing literatures. Both cognitive and emotional trust were adapted from [51], perceived intelligence and anthropomorphism from [39], the different privacy types from [31], perceived intrusiveness from [85], and usage behavior from [2]. All the constructs were measured on a 5-point Likert scale and are outlined in Table 3. The internal consistency of all the constructs was checked by calculating the Cronbach's α values and found to be above the threshold limit of 0.50. Before finalizing each of the measures a pilot study was conducted. It involved six professors having expertise in information systems and human computer interaction. Based on the feedback received two items were dropped from perceived intelligence and VAPA privacy concern, while one item was dropped for each government privacy concern, emotional trust, and perceived intrusiveness. Overall, it was observed that the pilot study helped in improving the readability of the survey questionnaire.

Any type of data collection strategy that involves survey is associated with the problem of Common Method Variance (CMV). As a procedural remedy we followed a marker-variable approach, wherein within the survey itself we deliberately included two special marker variables [87].

The two marker variables used were: (i) I believe that the current COVID-19 pandemic will end in 2022, and (ii) This survey was of appropriate length. None of these marker variables had any significant association with the dependent variable (usage of VAPA) and had extremely low path coefficients. Additionally, a Harman's one factor test was carried out in SPSS and results showed that the highest variance contributed by the first single factor was 25.4% of the overall variance that is below the recommended level of 50% [87]. Moreover, when all the ten factors of the model are taken into account, the variance explained increased to 72.1%. Thus, there is no indication of any problem related to CMV.

V. DATA ANALYSIS AND RESULT

A. DATA NORMALITY AND STRUCTURAL EQUATION MODELLING (SEM) APPROACH

After data cleansing, we checked the assumptions for data normality. Each indicator was tested for normality (acceptable limits of skewness and kurtosis), as recommended by current literatures for ensuring the suitability of analyzing it with the SEM approach [88]. Results revealed that the skewness and kurtosis values for all the items fell within the acceptable range of ± 2 and ± 3 [88].

SEM is a prominent statistical modelling technique that is used for testing relationships between constructs in a complex research model. It is a second-generation analytical tool that combines factor analysis and multiple regressions. Therefore, recently this technique has gained in popularity by IS and HCI researchers. SEM has two varieties: variance-based Partial Least Squares approach: (PLS-SEM), and co-variance-based approach (CB-SEM). The variance-based approach is suitable when certain conditions are not met, for e.g., related to data normality, or when the focus is to improve the predictive capability of the model [89]. Co-variance-based method on the other hand provides a more robust approach when data normality conditions are met. Moreover, based

TABLE 3. Details of measurement items used in the survey.

Construct	Item	Item Description	Cronbach's α
Perceived Anthropomorphism (PA)	PA ₁	My VAPA is able to speak like a human	0.864
	PA ₂	My VAPA is friendly	
	PA ₃	My VAPA is caring	
	PA ₄	My VAPA is respectful	
	PA ₅	My VAPA is funny	
Perceived Intelligence (PI)	PI ₁	My VAPA can understand my commands	0.841
	PI ₂	My VAPA is able to provide me with useful answer	
	PI ₃	My VAPA can complete tasks quickly and correctly	
VAPA Privacy Concern (VPC)	VPC ₁	My VAPA is asking me personal questions	0.822
	VPC ₂	My VAPA is constantly listening	
	VPC ₃	My VAPA is operating in unexpected ways	
	VPC ₄	My VAPA turns itself on when it should not	
Household Member Privacy Concern (HPC)	HPC ₁	Other members can monitor my activity via my VAPA	0.892
	HPC ₂	Other members can listen to my VAPA recordings	
	HPC ₃	Ads announced by my VAPA in presence of other members makes me feel uncomfortable	
	HPC ₄	Having less access and control over my VAPA when compared to other members makes me feel irritated/tensed	
Vendor & Third-Party Privacy Concern (VTPC)	VTPC ₁	My VAPA vendor/third-party companies is selling my data without my consent	0.945
	VTPC ₂	My VAPA vendor/third-party companies use my personal data to generate targeted advertising	
	VTPC ₃	My VAPA vendor/third-party companies listen to my private conversations	
	VTPC ₄	My VAPA vendor/third-party companies are able to identify me from my personal data	
	VTPC ₅	My VAPA vendor/third-party companies indefinitely retain my personal data	
Government Privacy Concern (GPC)	GPC ₁	The government receives sensitive information about me through my VAPA	0.937
	GPC ₂	The government spy on me through my VAPA	
	GPC ₃	The police can access my personal voice data	
	GPC ₄	My personal voice data can be used as evidence in a court of law	
Perceived Intrusiveness (PIN)	PIN ₁	My VAPA is intrusive	0.835
	PIN ₂	My VAPA is indiscreet	
	PIN ₃	My VAPA is irritating	
	PIN ₄	My VAPA is disturbing	
Cognitive Trust (CT)	CT ₁	My VAPA has good knowledge	0.886
	CT ₂	My VAPA is a real expert	
	CT ₃	My VAPA is honest	
	CT ₄	I think my VAPA has got integrity	
Emotional Trust (ET)	ET ₁	I feel safe about relying on my VAPA	0.902
	ET ₂	I feel comfortable about relying on my VAPA	
	ET ₃	I feel content about relying on my VAPA	
Usage of VAPA (UV)	UV ₁	I plan to continue using my VAPA in the future	0.918
	UV ₂	I intend to continue using my VAPA in the future	
	UV ₃	I predict I would continue to use my VAPA in the future	

on large scale Monte-Carlo simulations current research has shown that CB-SEM outperforms PLS in terms of parameter consistency and is preferable in terms of parameter accuracy as long as the sample size exceeds a certain threshold (250 observations) [89]. Therefore, in this work we decided to adopt the CB-SEM technique as both the normality and sample size restrictions are satisfied. We follow the two-stage approach: examining the measurement model to assess the reliability and validity of constructs under consideration, followed by the structural model evaluation for testing the proposed hypotheses. AMOS software has been used for the purpose of this analysis.

B. ASSESSING THE MEASUREMENT MODEL

The purpose of the measurement model is to test the convergent and discriminant validity of all the constructs presented in the research model. We begin by assessing the goodness of fit (GoF) of the measurement model by considering the well-accepted indices: ($\lambda^2/df = 2.62,$

$RMSEA = 0.047, RMR = 0.018, SRMR = 0.044, CFI = 0.969, NFI = 0.961, GFI = 0.952$). All the values are within the recommended range that ensures a good model-fit indicating the appropriateness of the research model [88]. Moreover, we also check the reliability of the constructs by computing the composite reliability (CR) and average variance extracted (AVE) values. Both these values are presented in Table 4. The CR and AVE values are greater than 0.70 and 0.50 respectively (the lower cut-off limits) that guarantees the conformance of convergent validity for all the constructs [88]. Additionally, the AVE values for each of the constructs are greater than their corresponding maximum shared variance (MSV) values, together with the square-root of AVE for all the constructs being greater than their corresponding inter-construct correlation values, both giving evidence of adequate discriminant validity [90]. Since both the convergent and discriminant validities are satisfied, we conclude that the measurement model is satisfactory.

TABLE 4. Convergent validity, discriminant validity, and inter-construct correlation matrix.

	CR	AVE	MSV	PA	PI	VPC	HPC	VTPC	GPC	PIN	CT	ET	UV
PA	0.841	0.639	0.398	0.799									
PI	0.851	0.741	0.531	0.507	0.861								
VPC	0.865	0.762	0.558	0.312	0.357	0.873							
HPC	0.952	0.833	0.308	0.209	0.294	0.253	0.913						
VTPC	0.802	0.670	0.557	0.344	0.302	0.228	0.348	0.818					
GPC	0.879	0.648	0.326	0.396	0.315	0.301	0.312	0.323	0.805				
PIN	0.823	0.609	0.535	0.414	0.408	0.395	0.369	0.336	0.412	0.780			
CT	0.911	0.773	0.772	0.453	0.462	-0.388	-0.418	-0.396	-0.389	-0.387	0.879		
ET	0.874	0.722	0.524	0.467	0.411	-0.404	-0.422	-0.424	-0.357	-0.364	0.204	0.850	
UV	0.869	0.634	0.531	0.338	0.392	0.367	0.415	0.378	0.385	-0.411	0.515	0.520	0.796

Note: The numbers marked in bold represent the square-root of AVE

TABLE 5. Results of hypotheses testing.

#	Path	Path Coefficient (β)	p Value	Supported
H ₁	Perceived anthropomorphism -> emotional trust	0.135	0.084	×
H ₂	Perceived intelligence -> cognitive trust	0.482	< 0.001	✓
H ₃	VAPA privacy concern -> cognitive trust	0.401	0.010	✓
H ₄	VAPA privacy concern -> emotional trust	0.387	0.015	✓
H ₅	Household privacy concern -> cognitive trust	0.427	< 0.001	✓
H ₆	Household privacy concern -> emotional trust	0.505	< 0.001	✓
H ₇	Vendor & third-party concern -> cognitive trust	0.137	0.079	×
H ₈	Vendor & third-party concern -> emotional trust	0.322	< 0.001	✓
H ₉	Government privacy concern -> cognitive trust	0.118	0.225	×
H ₁₀	Government privacy concern -> emotional trust	0.142	0.249	×
H ₁₁	Cognitive trust -> usage of VAPA	0.428	< 0.001	✓
H ₁₂	Emotional trust -> usage of VAPA	0.359	< 0.001	✓
Control Variables	Age -> usage of VAPA	0.089	0.299	×
	Gender -> usage of VAPA	0.142	0.458	×
	Education level -> usage of VAPA	0.063	0.302	×
	Usage frequency -> usage of VAPA	0.095	0.316	×
	Household size -> usage of VAPA	0.316	< 0.001	✓

C. ASSESING THE STRUCTURAL MODEL

Next, the structural model is examined for assessing the proposed hypotheses. Overall, the structural model has got acceptable GoF measures: ($\lambda^2/df = 2.83, RMSEA = 0.051, RMR = 0.020, SRMR = 0.019, CFI = 0.967, NFI = 0.958, GFI = 0.960$) [88]. The results of hypotheses testing are presented in Table 5 (excluding the moderating relationships). Results indicate the importance of perceived intelligence towards developing cognitive trust ($\beta = 0.482, p < 0.001$), hence supporting H₂. However, perceived anthropomorphism does not have any significant effect on emotional trust ($\beta = 0.135, p = 0.084$), so rejecting H₁. Both the forms of social privacy, i.e., VAPA privacy concern and household privacy concern have significant negative effects on cognitive trust, thereby supporting H₃ ($\beta = 0.401, p = 0.010$) and H₅ ($\beta = 0.427, p < 0.001$) respectively; as well as emotional trust, thereby supporting H₄ ($\beta = 0.387, p = 0.015$) and H₆ ($\beta = 0.505, p < 0.001$) respectively. Among the institutional privacy category, the effect of government privacy concern on both cognitive and emotional trust is found to be non-significant, therefore rejecting H₉ ($\beta = 0.118, p = 0.225$) and H₁₀ ($\beta = 0.142, p = 0.249$). However, for vendor & third-party concern the relationship is supported only for emotional trust H₈ ($\beta = 0.322, p < 0.001$). The effect on cognitive trust is found to be non-significant, thereby

rejecting H₇ ($\beta = 0.137, p = 0.079$). Finally, both cognitive and emotional trust is found to significantly affect the usage of VAPA, supporting H₁₁ ($\beta = 0.428, p < 0.001$) and H₁₂ ($\beta = 0.359, p < 0.001$) respectively.

Our research model also controlled for four factors: age, gender, usage frequency, and household size. The results in Table 6 suggest the non-significant effect of all the control variables, except household size. For the household size we observe a significant positive association with the usage of VAPA's ($\beta = 0.316, p < 0.001$). The demographic details show two types of household size: those having at most 2 persons, and those having at least 3 persons. We categorize the former as small household and the later as large household size for the purpose of analysis.

D. MODERATION EFFECT OF PERCEIVED INTRUSIVENESS

We carried out a moderation analysis to test the moderating role of perceived intrusiveness, and hence to examine the remaining two hypotheses H₁₃ and H₁₄. In line with current research, for creating the moderation analysis, first we created new variables in SPSS to examine the effect of the moderating variables. First, we adapted the independent construct (e.g., cognitive trust) and the moderating construct (perceived intrusiveness) using the mean-centering approach, as both these are quantitative in nature. Moreover, the

TABLE 6. Results of moderation analysis.

#	Path	Path Coefficient (β)	T Statistics	p Value	Supported	Effect
H ₁₃	(Cognitive trust \times perceived intrusiveness) \rightarrow usage of VAPA	-0.114	-4.482	= 0.06	\times	Negative
H ₁₄	(Emotional trust \times perceived intrusiveness) \rightarrow usage of VAPA	0.193	4.497	< 0.05	\checkmark	Dampening

mean-centering approach reduces potential multicollinearity issues with the model when multiple constructs are present. Accordingly, a new interaction term was created by multiplying the independent construct with the moderating construct, i.e., (*cognitive trust \times perceived intrusiveness*). Therefore, for hypothesis H₁₃, the dependent construct (usage of VAPA) was regressed on the independent construct (cognitive trust), the moderator (perceived intrusiveness), and the newly created interaction term (*cognitive trust \times perceived intrusiveness*). The same process was repeated for the other hypothesis H₁₄. The result is shown in Table 6. We observe two types of effects: dampening and negative. When there is a reduction in the strength of the relationship between the original dependent and independent constructs in the presence of the moderator (but not changing the sign of the original relationship), it is called the dampening effect. However, when the relationship between the dependent and independent constructs become negative in the presence of the moderator; it is called the negative effect. Results show that although the effect of emotional trust to usage of VAPA remains positive with the introduction of perceived intrusiveness as the moderator, the effect is significantly reduced (when compared to Table 5). Therefore, perceived intrusiveness is a concern for individuals and a barrier for the development of emotional trust, which in turn will lead to a less system usage. Results are however totally different for the interaction between cognitive trust and perceived intrusiveness. In this case although a negative effect is obtained, yet the result is non-significant, which means that perceived intrusiveness does not have any effect in the relationship between cognitive trust and usage of the VAPA's.

E. POST HOC ANALYSIS

Although the above analysis is sufficient for answering the research questions, yet the findings triggered some interesting new research questions. Conducting a post-hoc analysis is appropriate in such scenarios, where certain additional analyses need to be done based on the context. For example, effect of household size was found to be significant on the usage of VAPA's. We wanted to further explore that how the results vary with different household sizes (small vs. large). To this effect we conducted a multi group analysis (MGA) by selecting the bootstrapping method, where the bootstrapping confidence output illustrated the confidence interval between each household size. A particular result is significant if either the p -value is less than 0.05 or greater than 0.95 (assuming 95% confidence interval) for a specific difference between the path coefficients for the respective samples. The results indicate a significant difference between perceived anthropomorphism and emotional trust with regard to the household size (Small household: $\beta = 0.408, p = 0.03$; Large household:

$\beta = 0.121, p = 0.092$; *MGA significance difference* = 0.033). Additionally, a significant difference is found between household privacy concern and emotional trust based on household size (Small household: $\beta = 0.266, p = 0.001$; Large household: $\beta = 0.595, p < 0.001$; *MGA significance difference* = 0.002). Lastly, depending on household size the results also significantly differ for the path between emotional trust and usage of VAPA (Small household: $\beta = 0.378, p < 0.001$; Large household: $\beta = 0.199, p = 0.121$; *MGA significance difference* = 0.024). The implications of these findings will be discussed in detail in the next section.

Further, we analyzed the effect of the moderator on the two different household sizes. Overall, the results indicate a stronger interaction effect for the large household size. No significant difference is found between the two samples in relation to the moderating effect between cognitive trust and usage of VAPA's. However, a significant difference is found in relation to emotional trust. The results indicate that perceived intrusiveness has less effect on small households when compared to large households (Small household: $\beta = 0.218, p = 0.22$; Large household: $\beta = -0.159, p = 0.31$, *MGA significance difference* = 0.02).

In this work while proposing the trust variables we had used a grounded theory approach for identifying the relevant types as mentioned before. Accordingly, we identified cognitive and emotional trust by conceptualizing and treating them as separate theoretical constructs in our proposed model. Although, we believe that in line with previous trust descriptions it is a multi-dimensional concept, yet we wanted to check that whether separating trust into cognitive and emotional types have any additional theoretical advantage over when we treat both of these as a single construct. For this, we created an alternative model 2 wherein we integrated both the trust types into one single construct and re-ran the same analysis. It was observed that all the model fit indices for our initial model were far superior to the alternative model 2. Further, a Chi-square difference test between the two models also gave statistically significant results (higher Chi-square for model 2), indicating that theoretically separating the two trust constructs give a better model fit.

VI. DISCUSSION

A. THEORETICAL CONTRIBUTIONS

First, in this work we have identified two unique trust types in the VAPA usage context: cognitive and emotional trust. Other trust aspects arising from product aesthetics and data transparency have also been discussed, however since the present work considers a real-life usage scenario of the VAPA's,

usage driven trust is considered to be the most relevant one. Theoretically, although trust has been used in existing technology adoption models pertaining to VAPA's, but very few of them consider the multi-dimensional nature of trust [21], [28], [29], [35], [91]. In fact, current IS literatures have repeatedly called for treating trust as multiple dimensions due to its complex nature, although these dimensions may vary from one usage context to another [44], [92], [93]. However, such a conceptualization is missing in the VAPA context that has been repeatedly pointed by recent literatures [14], [15]. Therefore, as an answer to our first research question (RQ₁) we have identified the cognitive and emotional dimensions of trust that take into account the specialties of the conversational AI scenario. To the best of our knowledge very few works pertaining to conversational AI domain has provided the current conceptualization of trust, along with its empirical validation. Additionally, for checking that by separating trust into two separate and distinct aspects of cognition and emotion makes sense theoretically, we propose and tested an alternative model that had both these aspects coupled together in one single entity. Results indicate that by decoupling cognition and emotion into separate entities, a better model fit is obtained when compared to the other scenario. Therefore, we believe that the current findings will not only advance trust-specific literatures in the conversational AI context, but for other anthropomorphic systems too in general.

Second, for answering the next part of RQ₁, i.e., what are the different trust antecedents, we take into account two unique aspects of the VAPA context: the perceived humanness of this technology together with the associated privacy concerns. Accordingly, we propose perceived anthropomorphism, intelligence, social privacy (VAPA privacy and household privacy) and institutional privacy (vendor & third-party privacy and government privacy) to be the different antecedents of the two trust dimensions. For the humanness aspect what was more interesting from our literature review was that most of the current works have treated perceived anthropomorphism and perceived intelligence similarly in an interchangeable fashion. Although the idea of anthropomorphic information systems is new, and such confusions are commonplace in the formative stage of any research segment, especially with highly correlated (yet fundamentally different) concepts, in this work we have attempted to clearly differentiate between these two aspects. We try to extend the interplay between trust, intelligence and anthropomorphism that had been proposed previously in [38], but had some theoretical limitations. The work in [38] had a qualitative approach, which is excellent for understanding exploratory relationships between different factors, but such exploratory findings must be validated by further follow-up studies. Moreover, the research in [38] treated trust as a single entity too. The results from this work advance our general understanding of anthropomorphic information systems by clearly differentiating between intelligence and anthropomorphism, together with their effect on the respective trust types. It is observed that perceived anthropomorphism does

not affect emotional trust, whereas cognitive trust is affected by perceived intelligence. The cues for emotion, sociability, warmth, or care as expressed by the VAPA's is only in terms of its voice. There is a lack of visual cues like facial expressions, or communicative gestures that influence people's perception of human-likeness and trust when compared to other forms of anthropomorphic systems like social robots [73], [82]. For the HCI research community this finding carries a significant implication, since it seems that the effect of voice-anthropomorphism is weaker compared to non-verbal anthropomorphism when trying to establish man-machine relationships. Moreover, it also explains as to why a non-significant result is obtained for anthropomorphism and emotional trust. On the contrary, since perceived intelligence is related to how well the VAPA's understand the users and how competent these are to perform the requested tasks, its effect on cognitive trust is significant. Therefore, by separating the humanness aspect of technology the current work is able to contribute to the broader literature of trust in anthropomorphic information systems.

Third, the findings contribute to the existing privacy theories as applicable in conversational AI scenarios. While the effect of privacy concern on trust and technology usage is not unknown and has been discussed widely among the research community, what was missing is the compartmentalization of the different privacy types. VAPA's provide an entire new ecosystem of communication to the users due to which the privacy researchers would be benefitted if the different privacy types that are relevant for the current scenario can be identified. Accordingly, in this work we identified two broad privacy categories (social and institutional) with two subtypes for each category. To the best of our knowledge such a differentiation has seldom been attempted in the conversational AI scenario and should help the research community not only to distinguish between the different forms, but also examine how they influence the overall adoption process of such systems. Out of eight privacy related hypotheses towards trust, all four from the social category are found to be true, while only one from the institutional category is true. The results clearly suggest that the users have a two-dimensional view of their privacy concerns. Depending on the source of the privacy, the results vary. If the concerns are generated due to the direct interaction between the VAPA's and the users, then these are significant, however, if the concerns originate from any other source (apart from the user or the system) then the results are mixed. This explains that why current literatures related to VAPA's have shown mixed effect of privacy on the usage scenario, with some reporting it to be relevant [2], [4] and others not relevant [28], [29]. The users distinguish the VAPA's (for e.g., Alexa) from their parent companies (for e.g., Amazon), where they see the later to be a mechanism for trust protection. The users know that their personal data needs to be collected for getting personalized services that VAPA's provide, and the value of these services seem to outweigh the privacy concerns. Due to this reason vendor & third-party privacy concern does not affect the cognitive

trust. However, the emotional aspect of trust is still relevant as users perceive the targeted advertisements, telemarketing, or spamming emails sent by these stakeholders to be frustrating and disappointing. Another result that we would like to highlight is the non-significant effect of government privacy concern on both the trust types. While concerns over government surveillance or even smart speaker data being subjected to subpoena may be valid in a Western context [79], its relevance is not important in the Indian scenario where the growth of conversation agents and other AI/IoT based technologies has not matured. Likewise, people expect that the current laws related to digital privacy or other efforts from the government will act as effective privacy protection tools, rather than the government or other state agencies using them for surveillance purpose on the citizens.

The fourth major contribution of this research is to address the moderating role of perceived intrusiveness by answering RQ₂. Although intrusiveness is a highly relevant aspect in the VAPA usage scenario, yet very few studies have investigated the effect of this construct. Our results show that perceived intrusiveness has a dampening effect on emotional trust and VAPA usage, whereas a statistically non-significant negative effect on cognitive trust and VAPA usage. This observation illustrates another uniqueness of voice-based anthropomorphic systems, i.e., their sharedness and interconnectedness. The users can start a search on their smartphone, and then carry over the remaining task on their smart speaker, making these systems highly interconnected. Moreover, such a high cohesion also increases the sharing aspect of these devices, at least in a home usage scenario. Users may feel uncomfortable using the VAPA's in the way they want, when they know that these devices are getting shared among other users too [62]. VAPA's being personalized devices will always provide recommendations based on the primary user's preferences, that he/she might not want to reveal to other family members. Although these aspects were discussed in current literatures, they were done so in an exploratory fashion, providing no empirical evidence of the same [61], [62]. However, the current results show how the feeling of intrusiveness can weaken the emotional trust aspect leading to a lesser system usage. In contrary, the cognitive trust aspect is not affected by the intrusiveness perception. In fact, although insignificant but the negative relationship shows that for users' presence of cognitive trust is more than the feeling of intrusiveness. Cognitive trust is developed when the users perceive the VAPA's to be competent and consistent in their performance, which does not have any relationship with the intrusiveness aspect.

Moreover, in this work we find that household size (small vs. big) has an effect on the different motivators and the usage of the VAPA's. Given the popularity of the smart speakers, we can easily attribute them to be household items that further extends the current knowledge about their household usage scenario. Smaller households share a stronger anthropomorphic bondages with the VAPA's leading to a greater emotional trust, when compared with large households. Current

literatures have shown that anthropomorphic bondages will be strong when there is a greater sense of emotion, care and attachment between man and machines [38], [50], [58]. Users tend to objectify these devices as their personal belonging, and consequently develop feelings [62]. However, for such feelings to develop the VAPA's need to learn a lot about its user and provide in turn with highly personalized services. In large households normally VAPA's are used as shared devices, which often act as a source of rift between household members [65]. As a consequence, for larger households the development of emotional trust due to anthropomorphism is weaker when compared to smaller households, where there is a greater scope for personification. Moreover, the negative effect of household privacy concern on emotional trust is also greater for large households. We attribute this to the sharedness and interconnectedness of the VAPA's that we had discussed earlier. There seems to be a personalization vs. sharing paradox in the mind of the users, where in one hand the users know the benefits of sharing more personal information, however, on the other hand they are uncomfortable in doing so in a shared environment. This is a new finding that we attribute to the specific features of voice anthropomorphic systems.

With respect to household size, in addition to the above findings we also observe that the effect of perceived intrusiveness is more prominent in larger households that affects the emotional trust and VAPA usage. This further strengthens our previous disposition about personalization vs. sharing paradox, where the intrusive nature of the VAPA's inherently restrict the users to develop a feeling of emotional trust. Theoretically, the existence of such a personalization vs sharing paradox seems to be a specialty of VAPA's, and future studies should explore this aspect in more details.

B. PRACTICAL IMPLICATIONS

From the discussion of the result, it becomes evident that out of the two trust types, emotional trust is more volatile by nature. In most cases the cognitive trust is not affected when compared to emotional trust. Since cognitive trust is formed due to the competency and reliability of the VAPA's, it indicates that advances in IoT technologies together with AI, NLP and machine learning techniques have come a long way to create devices that are not only usable, for provide a good user experience too. Despite this, the users are not able to form any emotional attachment (or a very less degree of attachment) with the VAPA's. Although this is an inherent limitation of voice-based communication in general, the manufacturers should look for alternative communications modalities too, for e.g., touch, gesture, gaze, etc. Multimodes of communication will make it easier for the users to interact with these systems and may invoke the perceptions of emotion too. Additionally, since different voice features like tone, pitch, language spoken, or even accent have been found to induce emotions among people, manufacturers should take this cue and provide multiple voice options in their VAPA's. Although, most of the commercially available

VAPA's already provide multiple voice options (both male and female), we recommend the manufacturers to go one step ahead based upon our current understanding of para-social relationship theories, which state that users can easily form a deep attachment with their favorite television or film characters (hero or heroines). The manufacturers can take this to their advantage and include voice of prominent personalities (depending upon different geographic locations) and incorporate them into these devices. Such an aspect might make the users more engaged and develop a strong bond with these devices. Additionally, from the robotic research community suggestions must be taken, especially related to the embodied aspect of anthropomorphism. Not only in robotics but is multiple scenarios research has shown that visual aesthetics play an important role in users developing relationships. Keeping this in mind, the manufacturers can come up with innovative design features, and even target multiple user groups. For e.g., in case of children smart speakers can be made to look like popular cartoon characters, or for the young generation the looks can be made cool and innovative with bold colors or multiple patterns or even using different textured materials that the users can choose from based on their preferences and likings. Although the inherent drawbacks of voice-only communication mode cannot be eliminated, however, emotional trust can be improved following the above suggestions.

The second concern area that arises from the current work is that of the personalization vs. sharing paradox. In this regard some steps have already been taken by the manufacturers, like introduction of voice profiles for authentication purpose. Current VAPA's like Alexa supports multiple voice profiles who can trigger/turn-on these devices. However, the problem is since every VAPA is associated with a unique user-id, although multiple persons can unlock these devices (provide they are authorized to do so), yet they land into one common user profile. Provision should be made to have separate user-profile for each user, so that on a dynamic basis depending on who unlocked the system, the VAPA will automatically select the most appropriate user profile. Moreover, in addition to giving physical mute button to turn-on/off the microphones, the manufacturers should give more control to the users in terms of how they want their notifications to be received. This will enable the users to have a fine gain control not only over their usage, but also in terms of the unexpected announcements the VAPA's often make based upon the personalized interactions, which will be helpful in respecting the privacy when these devices are shared among family members.

The final concern area we observed was related to the social privacy aspect that affected both cognitive as well as emotional trust. In this respect we recommend the manufacturers to adhere to strict security and privacy frameworks, for e.g., by using the Privacy-by-design (PbD) philosophy. PbD principles can provide practical guidelines to companies for incorporating privacy into every aspect of data collection during the user interactions and create a better rule towards data accountability. In addition to PbD other tools like the

NIST cybersecurity framework can also be used as the basis to identify, assess, and manage the privacy risks to promote greater user confidence and trust. Moreover, since privacy is translated to culture, and privacy protection can succeed only if it is culturally authentic, the realm of PbD must be broadened taking into consideration the cultural effects, giving rise to a new era of Privacy by Culture (PbC). Since the conversational AI segment is a data-centric business obtained from the users the responsibility lies on the manufacturers to get the privacy right that has cultural variations.

VII. CONCLUSION, LIMITATION, AND FUTURE WORK

In this work we have examined the usage scenario of the VAPA's from the dual perspectives of cognitive and emotional trust. Although existing literatures related to VAPA adoption have included the trust lens, however its treatment has been over-simplified that is in contrary to the complex nature of trust that current IS literatures have established. Therefore, in this work we proposed cognition and emotion to be the two relevant trust dimensions together with their antecedents. While selecting the trust antecedents we kept in mind the specialties of the conversational AI paradigm: the humanness and intrusiveness of this technology. Accordingly, we proposed anthropomorphism and intelligence to reflect the humanness aspect, together with two distinct privacy types: social, and institutional; all affecting the trust factors. Additionally, the moderating effect of perceived intrusiveness on the relationship between the different trust types and VAPA usage were also examined.

However, this work is not without limitations. First, data was collected from only one country (India). India is a typical representation of a collectivist society that is different from the Western individualistic society. Further, trust and privacy aspects vary with country and culture, due to which future studies must adopt a cross-cultural approach for generalizing the current findings.

Second, we collected cross-sectional data rather than longitudinal data. VAPA's are an emerging paradigm, wherein the perception and user behavior can change in a very short span of time. Therefore, we encourage future research to study the different trust, privacy, and usage aspects over a longer time duration.

Third, our findings with respect to household size is subjected to certain restrictions. We categorized small household as those which had at most 2 people, whereas large household as those which had at least 3 people. However, we did not consider any additional details like the composition dynamics of the households. For e.g., households containing adults only, or a mix of adults and children, or couples and roommates. Future research can focus on different household dynamics and what effect it has on the trust aspects and usage behavior.

Fourth, we did not find any significant effect of age, gender, or education level on VAPA usage. Future studies should further confirm this finding in a multi-cultural setting.

Lastly, future research must consider the role of perceived intrusiveness. We found a dampening moderating role of

perceived intrusiveness. Researchers should further examine this concern over intrusiveness during their interaction with the VAPA's. We recommend the use of qualitative techniques like interviews that might be able to bring out the key concerns as to how the perceived intrusiveness changes the user behavior with the VAPA's.

REFERENCES

- [1] M. Z. Iqbal and A. G. Campbell, "From luxury to necessity: Progress of touchless interaction technology," *Technol. Soc.*, vol. 67, Nov. 2021, Art. no. 101796, doi: [10.1016/j.techsoc.2021.101796](https://doi.org/10.1016/j.techsoc.2021.101796).
- [2] G. McLean and K. Osei-Frimpong, "Hey Alex? Examine the variables influencing the use of artificial intelligent in-home voice assistants," *Comput. Hum. Behav.*, vol. 99, pp. 28–37, Oct. 2019, doi: [10.1016/j.chb.2019.05.009](https://doi.org/10.1016/j.chb.2019.05.009).
- [3] N. L. Tenhundfeld, H. M. Barr, E. H. O'Hear, and K. Weger, "Is my siri the same as your siri? An exploration of users' mental model of virtual personal assistants, implications for trust," *IEEE Trans. Human-Machine Syst.*, vol. 52, no. 3, pp. 512–521, Jun. 2021, doi: [10.1109/THMS.2021.3107493](https://doi.org/10.1109/THMS.2021.3107493).
- [4] D. Pal, X. Zhang, and S. Siyal, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach," *Technol. Soc.*, vol. 66, Aug. 2021, Art. no. 101683, doi: [10.1016/j.techsoc.2021.101683](https://doi.org/10.1016/j.techsoc.2021.101683).
- [5] H. Yang and H. Lee, "Understanding user behavior of virtual personal assistant devices," *Inf. Syst. E-Business Manage.*, vol. 17, no. 1, pp. 65–87, Mar. 2019, doi: [10.1007/s10257-018-0375-1](https://doi.org/10.1007/s10257-018-0375-1).
- [6] D. Pal, C. Arpnikanondt, S. Funilkul, and W. Chutimaskul, "The adoption analysis of voice-based smart IoT products," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 10852–10867, Nov. 2020, doi: [10.1109/JIOT.2020.2991791](https://doi.org/10.1109/JIOT.2020.2991791).
- [7] D. S. Zwakman, D. Pal, and C. Arpnikanondt, "Usability evaluation of artificial intelligence-based voice assistants: The case of Amazon Alexa," *Social Netw. Comput. Sci.*, vol. 2, no. 1, p. 28, Feb. 2021, doi: [10.1007/s42979-020-00424-4](https://doi.org/10.1007/s42979-020-00424-4).
- [8] J. Kiseleva, K. Williams, J. Jiang, A. H. Awadallah, A. C. Crook, I. Zitouni, and T. Anastasakos, "Understanding user satisfaction with intelligent assistants," in *Proc. ACM Conf. Hum. Interact. Retrieval*, 2016, pp. 121–130, doi: [10.1145/2854946.2854961](https://doi.org/10.1145/2854946.2854961).
- [9] J. Cho and E. Rader, "The role of conversational grounding in supporting symbiosis between people and digital assistants," *Proc. ACM Hum.-Comput. Interact.*, vol. 4, no. CSCW1, pp. 1–28, May 2020, doi: [10.1145/3392838](https://doi.org/10.1145/3392838).
- [10] L. M. Hirshfield, S. H. Hirshfield, S. Hincks, M. Russell, R. Ward, and T. Williams, "Trust in human-computer interactions as measured by frustration, surprise, and workload," in *Foundations of Augmented Cognition. Directing the Future of Adaptive Systems*. OR, USA: Springer, 2011, pp. 507–516.
- [11] E. Alepis and C. Patsakis, "Monkey says, monkey does: Security and privacy on voice assistants," *IEEE Access*, vol. 5, pp. 17841–17851, 2017, doi: [10.1109/ACCESS.2017.2747626](https://doi.org/10.1109/ACCESS.2017.2747626).
- [12] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Trans. Microw. Theory Techn.*, vol. 69, no. 5, pp. 2642–2650, May 2021, doi: [10.1109/TMTT.2021.3058585](https://doi.org/10.1109/TMTT.2021.3058585).
- [13] A. Easwara Moorthy and K.-P.-L. Vu, "Privacy concerns for use of voice activated personal assistant in the public space," *Int. J. Hum. Comput. Interact.*, vol. 31, no. 4, pp. 307–335, Apr. 2015, doi: [10.1080/10447318.2014.986642](https://doi.org/10.1080/10447318.2014.986642).
- [14] V. N. Lu, J. Wirtz, W. H. Kunz, S. Paluch, T. Gruber, A. Martins, and P. G. Patterson, "Service robots, customers and service employees: What can we learn from the academic literature and where are the gaps?" *J. Service Theory Pract.*, vol. 30, no. 3, pp. 361–391, Apr. 2020, doi: [10.1108/JSTP-04-2019-0088](https://doi.org/10.1108/JSTP-04-2019-0088).
- [15] J. Wirtz, P. G. Patterson, W. H. Kunz, T. Gruber, V. N. Lu, S. Paluch, and A. Martins, "Brave new world: Service robots in the frontline," *J. Service Manage.*, vol. 29, no. 5, pp. 907–931, Nov. 2018, doi: [10.1108/JOSM-04-2018-0119](https://doi.org/10.1108/JOSM-04-2018-0119).
- [16] T. Dirsehan and C. Can, "Examination of trust and sustainability concerns in autonomous vehicle adoption," *Technol. Soc.*, vol. 63, Nov. 2020, Art. no. 101361, doi: [10.1016/j.techsoc.2020.101361](https://doi.org/10.1016/j.techsoc.2020.101361).
- [17] P. Beatty, I. Reay, S. Dick, and J. Miller, "Consumer trust in E-commerce web sites: A meta-study," *ACM Comput. Surveys*, vol. 43, no. 3, pp. 1–46, Apr. 2011, doi: [10.1145/1922649.1922651](https://doi.org/10.1145/1922649.1922651).
- [18] O. H. Chi, S. Jia, Y. Li, and D. Gursoy, "Developing a formative scale to measure consumers' trust toward interaction with artificially intelligent (AI) social robots in service delivery," *Comput. Hum. Behav.*, vol. 118, May 2021, Art. no. 106700, doi: [10.1016/j.chb.2021.106700](https://doi.org/10.1016/j.chb.2021.106700).
- [19] A. Ponticello, M. Fassel, and K. Krombholz, "Exploring authentication for security-sensitive tasks on smart home voice assistants," in *Proc. 17th Symp. Usable Privacy Secur. (SOUPS)*, Aug. 2021, pp. 475–492. [Online]. Available: <https://www.usenix.org/conference/soups2021/presentation/ponticello>
- [20] T. Bolton, T. Dargahi, S. Belguith, M. S. Al-Rakhami, and A. H. Sodhro, "On the security and privacy challenges of virtual assistants," *Sensors*, vol. 21, no. 7, p. 2312, Mar. 2021, doi: [10.3390/s21072312](https://doi.org/10.3390/s21072312).
- [21] D. Pal, C. Arpnikanondt, M. A. Razzaque, and S. Funilkul, "To trust or not-trust: Privacy issues with voice assistants," *IT Prof.*, vol. 22, no. 5, pp. 46–53, Sep. 2020, doi: [10.1109/MITP.2019.2958914](https://doi.org/10.1109/MITP.2019.2958914).
- [22] M. P. Garcia and S. S. Lopez, "Building trust between users and telecommunications data driven virtual assistants," in *Proc. IFIP Int. Conf. Artif. Intell. Appl. Innov.*, 2018, pp. 628–637.
- [23] L. Schönherr, M. Golla, T. Eisenhofer, J. Wiele, D. Kolossa, and T. Holz, "Exploring accidental triggers of smart speakers," *Comput. Speech Lang.*, vol. 73, May 2022, Art. no. 101328, doi: [10.1016/j.csl.2021.101328](https://doi.org/10.1016/j.csl.2021.101328).
- [24] D. Pal, C. Arpnikanondt, S. Funilkul, and M. A. Razzaque, "Analyzing the adoption and diffusion of voice-enabled smart-home systems: Empirical evidence from Thailand," *Universal Access Inf. Soc.*, vol. 20, pp. 797–815, Aug. 2020, doi: [10.1007/s10209-020-00754-3](https://doi.org/10.1007/s10209-020-00754-3).
- [25] A. Mishra, A. Shukla, and S. K. Sharma, "Psychological determinants of users' adoption and word-of-mouth recommendations of smart voice assistants," *Int. J. Inf. Manage.*, vol. 67, Dec. 2022, Art. no. 102413, doi: [10.1016/j.ijinfomgt.2021.102413](https://doi.org/10.1016/j.ijinfomgt.2021.102413).
- [26] H. Chung, M. Iorga, J. Voas, and S. Lee, "Alexa, can i trust you?" *Computer*, vol. 50, no. 9, pp. 100–104, 2017, doi: [10.1109/MC.2017.3571053](https://doi.org/10.1109/MC.2017.3571053).
- [27] D. A. Orr and L. Sanchez, "Alexa, did you get that? Determining the evidentiary value of data stored by the Amazon® echo," *Digit. Invest.*, vol. 24, pp. 72–78, Mar. 2018, doi: [10.1016/j.diin.2017.12.002](https://doi.org/10.1016/j.diin.2017.12.002).
- [28] M. Vimalkumar, S. K. Sharma, J. B. Singh, and Y. K. Dwivedi, "'Okay Google, what about my privacy'? User's privacy perceptions and acceptance of voice based digital assistants," *Comput. Hum. Behav.*, vol. 120, Jul. 2021, Art. no. 106763, doi: [10.1016/j.chb.2021.106763](https://doi.org/10.1016/j.chb.2021.106763).
- [29] V. Pitardi and H. R. Marriott, "Alexa, she's not human but? Unveiling the drivers of consumers' trust in voice-based artificial intelligence," *Psychol. Marketing*, vol. 38, no. 4, pp. 626–642, Apr. 2021, doi: [10.1002/mar.21457](https://doi.org/10.1002/mar.21457).
- [30] M. B. Yılmaz and K. Rızvanoğlu, "Understanding users' behavioral intention to use voice assistants on smartphones through the integrated model of user satisfaction and technology acceptance: A survey approach," *J. Eng., Design Technol.*, pp. 1–27, Jun. 2021, doi: [10.1108/JEDT-02-2021-0084](https://doi.org/10.1108/JEDT-02-2021-0084).
- [31] P. Kowalczyk, "Consumer acceptance of smart speakers: A mixed methods approach," *J. Res. Interact. Marketing*, vol. 12, no. 4, pp. 418–431, Oct. 2018, doi: [10.1108/JRIM-01-2018-0022](https://doi.org/10.1108/JRIM-01-2018-0022).
- [32] J. Chung, M. Bleich, D. C. Wheeler, J. M. Winship, B. McDowell, M. S. D. Baker, and P. Parsons, "Attitudes and perceptions toward voice-operated smart speakers among low-income senior housing residents: Comparison of pre- and post-installation surveys," *Gerontol. Geriatric Med.*, vol. 7, pp. 1–9, Mar. 2021, doi: [10.1177/23337214211005869](https://doi.org/10.1177/23337214211005869).
- [33] M. Ashfaq, J. Yun, and S. Yu, "My smart speaker is cool! Perceived coolness, perceived values, and users' attitude toward smart speakers," *Int. J. Hum. Comput. Interact.*, vol. 37, no. 6, pp. 560–573, Apr. 2021, doi: [10.1080/10447318.2020.1841404](https://doi.org/10.1080/10447318.2020.1841404).
- [34] D. Pal, C. Arpnikanondt, and M. A. Razzaque, "Personal information disclosure via voice assistants: The personalization–privacy paradox," *Social Netw. Comput. Sci.*, vol. 1, no. 5, pp. 1–17, Sep. 2020, doi: [10.1007/s42979-020-00287-9](https://doi.org/10.1007/s42979-020-00287-9).
- [35] D. Pal, M. D. Babakerkhell, and X. Zhang, "Exploring the determinants of users' continuance usage intention of smart voice assistants," *IEEE Access*, vol. 9, pp. 162259–162275, 2021, doi: [10.1109/ACCESS.2021.3132399](https://doi.org/10.1109/ACCESS.2021.3132399).
- [36] A. Poushneh, "Humanizing voice assistant: The impact of voice assistant personality on consumers' attitudes and behaviors," *J. Retailing Consum. Services*, vol. 58, Jan. 2021, Art. no. 102283, doi: [10.1016/j.jretconser.2020.102283](https://doi.org/10.1016/j.jretconser.2020.102283).

- [37] K. Park, C. Kwak, J. Lee, and J.-H. Ahn, "The effect of platform characteristics on the adoption of smart speakers: Empirical evidence in South Korea," *Telematics Informat.*, vol. 35, no. 8, pp. 2118–2132, Dec. 2018, doi: [10.1016/j.tele.2018.07.013](https://doi.org/10.1016/j.tele.2018.07.013).
- [38] I. Troshani, S. Rao Hill, C. Sherman, and D. Arthur, "Do we trust in AI? Role of anthropomorphism and intelligence," *J. Comput. Inf. Syst.*, vol. 61, no. 5, pp. 481–491, Sep. 2021, doi: [10.1080/08874417.2020.1788473](https://doi.org/10.1080/08874417.2020.1788473).
- [39] S. Moussawi, M. Koufaris, and R. Benbunan-Fich, "How perceptions of intelligence and anthropomorphism affect adoption of personal intelligent agents," *Electron. Markets*, pp. 343–364, Mar. 2020, doi: [10.1007/s12525-020-00411-w](https://doi.org/10.1007/s12525-020-00411-w).
- [40] E. Moriuchi, "An empirical study on anthropomorphism and engagement with disembodied AIs and consumers' re-use behavior," *Psychol. Marketing*, vol. 38, no. 1, pp. 21–42, Jan. 2021, doi: [10.1002/mar.21407](https://doi.org/10.1002/mar.21407).
- [41] C.-C. Ho and K. F. MacDorman, "Revisiting the uncanny valley theory: Developing and validating an alternative to the godspeed indices," *Comput. Hum. Behav.*, vol. 26, no. 6, pp. 1508–1518, Nov. 2010, doi: [10.1016/j.chb.2010.05.015](https://doi.org/10.1016/j.chb.2010.05.015).
- [42] C.-C. Ho and K. F. MacDorman, "Measuring the uncanny valley effect," *Int. J. Social Robot.*, vol. 9, no. 1, pp. 129–139, Jan. 2017, doi: [10.1007/s12369-016-0380-9](https://doi.org/10.1007/s12369-016-0380-9).
- [43] M. B. Mathur and D. B. Reichling, "Navigating a social world with robot partners: A quantitative cartography of the uncanny valley," *Cognition*, vol. 146, pp. 22–32, Jan. 2016, doi: [10.1016/j.cognition.2015.09.008](https://doi.org/10.1016/j.cognition.2015.09.008).
- [44] A. R. Wagner, J. Borenstein, and A. Howard, "Overtrust in the robotic age," *Commun. ACM*, vol. 61, no. 9, pp. 22–24, Aug. 2018, doi: [10.1145/3241365](https://doi.org/10.1145/3241365).
- [45] N. L. Tenhundfeld, E. J. de Visser, A. J. Ries, V. S. Finomore, and C. C. Tossell, "Trust and distrust of automated parking in a Tesla model X," *Hum. Factors, J. Hum. Factors Ergonom. Soc.*, vol. 62, no. 2, pp. 194–210, Aug. 2019, doi: [10.1177/0018720819865412](https://doi.org/10.1177/0018720819865412).
- [46] R. Riedl, P. N. C. Mohr, P. H. Kenning, F. D. Davis, and H. R. Heekeren, "Trusting humans and avatars: A brain imaging study based on evolution theory," *J. Manage. Inf. Syst.*, vol. 30, no. 4, pp. 83–114, Apr. 2014, doi: [10.2753/MIS0742-1222300404](https://doi.org/10.2753/MIS0742-1222300404).
- [47] E. J. de Visser, S. S. Monfort, R. McKendrick, M. A. B. Smith, P. E. McKnight, F. Krueger, and R. Parasuraman, "Almost human: Anthropomorphism increases trust resilience in cognitive agents," *J. Experim. Psychol., Appl.*, vol. 22, no. 3, pp. 331–349, Sep. 2016, doi: [10.1037/xap0000092](https://doi.org/10.1037/xap0000092).
- [48] J. Feine, U. Gnewuch, S. Morana, and A. Maedche, "A taxonomy of social cues for conversational agents," *Int. J. Hum.-Comput. Stud.*, vol. 132, pp. 138–161, Dec. 2019, doi: [10.1016/j.ijhcs.2019.07.009](https://doi.org/10.1016/j.ijhcs.2019.07.009).
- [49] D. Pal, C. Arpikanondt, S. Funilkul, and V. Varadarajan, "User experience with smart voice assistants: The accent perspective," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–6, doi: [10.1109/ICCCNT45670.2019.8944754](https://doi.org/10.1109/ICCCNT45670.2019.8944754).
- [50] L. Qiu and I. Benbasat, "Evaluating anthropomorphic product recommendation agents: A social relationship perspective to designing information systems," *J. Manage. Inf. Syst.*, vol. 25, no. 4, pp. 145–182, Apr. 2009, doi: [10.2753/MIS0742-1222250405](https://doi.org/10.2753/MIS0742-1222250405).
- [51] S. Y. X. Komiak and I. Benbasat, "The effects of personalization and familiarity on trust and adoption of recommendation agents," *MIS Quart.*, vol. 30, no. 4, pp. 941–960, Dec. 2006, doi: [10.2307/25148760](https://doi.org/10.2307/25148760).
- [52] V. Chattaraman, W.-S. Kwon, J. E. Gilbert, and K. Ross, "Should AI-based, conversational digital assistants employ social- or task-oriented interaction style? A task-competency and reciprocity perspective for older adults," *Comput. Hum. Behav.*, vol. 90, pp. 315–330, Jan. 2019, doi: [10.1016/j.chb.2018.08.048](https://doi.org/10.1016/j.chb.2018.08.048).
- [53] Q. Hu, Y. Lu, Z. Pan, Y. Gong, and Z. Yang, "Can AI artifacts influence human cognition? The effects of artificial autonomy in intelligent personal assistants," *Int. J. Inf. Manage.*, vol. 56, Feb. 2021, Art. no. 102250, doi: [10.1016/j.ijinfomgt.2020.102250](https://doi.org/10.1016/j.ijinfomgt.2020.102250).
- [54] H. Chin, L. W. Molefi, and M. Y. Yi, "Empathy is all you need: How a conversational agent should respond to verbal abuse," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2020, pp. 1–13, doi: [10.1145/3313831.3376461](https://doi.org/10.1145/3313831.3376461).
- [55] S. Aeschlimann, M. Bleiker, M. Wechner, and A. Gampe, "Communicative and social consequences of interactions with voice assistants," *Comput. Hum. Behav.*, vol. 112, Nov. 2020, Art. no. 106466, doi: [10.1016/j.chb.2020.106466](https://doi.org/10.1016/j.chb.2020.106466).
- [56] J.-G. Lee, K. J. Kim, S. Lee, and D.-H. Shin, "Can autonomous vehicles be safe and trustworthy? Effects of appearance and autonomy of unmanned driving systems," *Int. J. Hum. Comput. Interact.*, vol. 31, no. 10, pp. 682–691, Oct. 2015, doi: [10.1080/10447318.2015.1070547](https://doi.org/10.1080/10447318.2015.1070547).
- [57] M. L. Cummings, M. Buchin, G. Carrigan, and B. Donmez, "Supporting intelligent and trustworthy maritime path planning decisions," *Int. J. Hum. Comput. Stud.*, vol. 68, no. 10, pp. 616–626, Oct. 2010, doi: [10.1016/j.ijhcs.2010.05.002](https://doi.org/10.1016/j.ijhcs.2010.05.002).
- [58] A. Guzman, "Ontological boundaries between humans and computers and the implications for human-machine communication," *Hum. Mach. Commun.*, vol. 1, pp. 37–54, Feb. 2020, doi: [10.30658/hmc.1.3](https://doi.org/10.30658/hmc.1.3).
- [59] P. E. Nacini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh, "Privacy expectations and preferences in an IoT world," in *Proc. 13th Symp. Usable Privacy Secur. (SOUPS)*, Jul. 2017, pp. 399–412. [Online]. Available: <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/nacini>
- [60] L. Manikonda, A. Deotale, and S. Kambhampati, "What's up with privacy? User preferences and privacy concerns in intelligent personal assistants," in *Proc. AAAI/ACM Conf. AI, Ethics, Soc.*, Dec. 2018, pp. 229–235, doi: [10.1145/3278721.3278773](https://doi.org/10.1145/3278721.3278773).
- [61] N. Meng, D. Keküllüoğlu, and K. Vaniea, "Owning and sharing: Privacy perceptions of smart speaker users," in *Proc. ACM Hum. Comput. Interact.*, vol. 5, no. CSCW1, Apr. 2021, pp. 1–29, doi: [10.1145/3449119](https://doi.org/10.1145/3449119).
- [62] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers," *Proc. ACM Hum.-Comput. Interact.*, vol. 2, no. CSCW, pp. 1–31, Nov. 2018, doi: [10.1145/3274371](https://doi.org/10.1145/3274371).
- [63] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Rev.*, vol. 79, no. 1, pp. 119–157, 2004. [Online]. Available: <https://nyuscholars.nyu.edu/en/publications/privacy-as-contextual-integrity>
- [64] K. Raynes-Goldie, "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook," *1st Monday*, Jan. 2010, doi: [10.5210/fm.v15i1.2775](https://doi.org/10.5210/fm.v15i1.2775).
- [65] C. Geeng and F. Roesner, "Who's in control? Interactions in multi-user smart homes," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, May 2019, pp. 1–13, doi: [10.1145/3290605.3300498](https://doi.org/10.1145/3290605.3300498).
- [66] M. Büchi, E. Fosch-Villaronga, C. Lutz, A. Tamò-Larriex, S. Velidi, and S. Viljoen, "The chilling effects of algorithmic profiling: Mapping the issues," *Comput. Law Secur. Rev.*, vol. 36, Apr. 2020, Art. no. 105367, doi: [10.1016/j.clsr.2019.105367](https://doi.org/10.1016/j.clsr.2019.105367).
- [67] K. Martin, "Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop?" *Inf. Soc.*, vol. 32, no. 1, pp. 51–63, Jan. 2016, doi: [10.1080/01972243.2015.1107166](https://doi.org/10.1080/01972243.2015.1107166).
- [68] J. Haney, Y. Acar, and S. Furman, "It's the company, the government, you and I: User perceptions of responsibility for smart home privacy and security," in *Proc. 30th USENIX Secur. Symp. (USENIX Security)*, Aug. 2021, pp. 411–428. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity21/presentation/haney>
- [69] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy... Now take some cookies," *Informatik Spektrum*, vol. 42, no. 5, pp. 345–346, Oct. 2019, doi: [10.1007/s00287-019-01201-1](https://doi.org/10.1007/s00287-019-01201-1).
- [70] S. Buhr, "An Amazon echo may be the key to solving a murder case," *TechCrunch*, San Francisco, CA, USA, Tech. Rep., Dec. 2016.
- [71] B. R. Duffy, "Anthropomorphism and the social robot," *Robot. Auton. Syst.*, vol. 42, no. 3, pp. 177–190, 2003, doi: [https://doi.org/10.1016/S0921-8890\(02\)00374-3](https://doi.org/10.1016/S0921-8890(02)00374-3).
- [72] N. Haslam, S. Loughnan, Y. Kashima, and P. Bain, "Attributing and denying humanness to others," *Eur. Rev. Social Psychol.*, vol. 19, no. 1, pp. 55–85, Sep. 2008, doi: [10.1080/10463280801981645](https://doi.org/10.1080/10463280801981645).
- [73] I. Seeber, E. Bittner, R. O. Briggs, T. de Vreede, G.-J. de Vreede, A. Elkins, R. Maier, A. B. Merz, S. Oeste-Reiß, N. Randrup, G. Schwabe, and M. Söllner, "Machines as teammates: A research agenda on AI in team collaboration," *Inf. Manage.*, vol. 57, no. 2, Mar. 2020, Art. no. 103174, doi: [10.1016/j.im.2019.103174](https://doi.org/10.1016/j.im.2019.103174).
- [74] P. Ebel, M. Söllner, J. M. Leimeister, K. Crowston, and G.-J. de Vreede, "Hybrid intelligence in business networks," *Electron. Markets*, pp. 313–318, Jun. 2021, doi: [10.1007/s12525-021-00481-4](https://doi.org/10.1007/s12525-021-00481-4).
- [75] A. Waytz, J. Heafner, and N. Epley, "The mind in the machine: Anthropomorphism increases trust in an autonomous vehicle," *J. Experim. Social Psychol.*, vol. 52, pp. 113–117, May 2014, doi: [10.1016/j.jesp.2014.01.005](https://doi.org/10.1016/j.jesp.2014.01.005).

- [76] J.-S. Chiou, "Service quality, trust, specific asset investment, and expertise: Direct and indirect effects in a satisfaction-loyalty framework," *J. Acad. Marketing Sci.*, vol. 34, no. 4, pp. 613–627, Oct. 2006, doi: [10.1177/0092070306286934](https://doi.org/10.1177/0092070306286934).
- [77] K. Lebeck, K. Ruth, T. Kohno, and F. Roesner, "Towards security and privacy for multi-user augmented reality: Foundations with end users," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 392–408, doi: [10.1109/SP.2018.00051](https://doi.org/10.1109/SP.2018.00051).
- [78] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," *Social Netw. Appl. Sci.*, vol. 2, no. 2, pp. 1–12, Feb. 2020, doi: [10.1007/s42452-020-2025-8](https://doi.org/10.1007/s42452-020-2025-8).
- [79] J. Jerome, *Alexa, is Law Enforcement Listening?*. Accessed: Mar. 9, 2022. [Online]. Available: <https://cdt.org/insights/alexa-is-law-enforcement-listening/>
- [80] J. J. Sim, S. H. Loh, K. L. Wong, and C. K. Choong, "Do we need trust transfer mechanisms? An M-commerce adoption perspective," *J. Theor. Appl. Electron. Commerce Res.*, vol. 16, no. 6, pp. 2241–2262, Sep. 2021, doi: [10.3390/jtaer16060124](https://doi.org/10.3390/jtaer16060124).
- [81] C. Ferreira da Silva and S. Moro, "Blockchain technology as an enabler of consumer trust: A text mining literature analysis," *Telematics Informat.*, vol. 60, Jul. 2021, Art. no. 101593, doi: [10.1016/j.tele.2021.101593](https://doi.org/10.1016/j.tele.2021.101593).
- [82] T. Gompei and H. Umemuro, "Factors and development of cognitive and affective trust on social robots," in *Proc. Int. Conf. Social Robot.*, 2018, pp. 45–54.
- [83] D. Johnson and K. Grayson, "Cognitive and affective trust in service relationships," *J. Bus. Res.*, vol. 58, no. 4, pp. 500–507, 2005, doi: [https://doi.org/10.1016/S0148-2963\(03\)00140-1](https://doi.org/10.1016/S0148-2963(03)00140-1).
- [84] K. Plangger and M. Montecchi, "Thinking beyond privacy calculus: Investigating reactions to customer surveillance," *J. Interact. Marketing*, vol. 50, no. 1, pp. 32–44, May 2020, doi: [10.1016/j.intmar.2019.10.004](https://doi.org/10.1016/j.intmar.2019.10.004).
- [85] L. Lucia-Palacios and R. Pérez-López, "Effects of home voice Assistants' autonomy on intrusiveness and usefulness: Direct, indirect, and moderating effects of interactivity," *J. Interact. Marketing*, vol. 56, pp. 41–54, Nov. 2021, doi: [10.1016/j.intmar.2021.03.005](https://doi.org/10.1016/j.intmar.2021.03.005).
- [86] A. Benlian, J. Klumpe, and O. Hinz, "Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation," *Inf. Syst. J.*, vol. 30, no. 6, pp. 1010–1042, Nov. 2020, doi: [10.1111/isj.12243](https://doi.org/10.1111/isj.12243).
- [87] N. K. Malhotra, S. S. Kim, and A. Patil, "Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research," *Manage. Sci.*, vol. 52, no. 12, pp. 1865–1883, Dec. 2006. [Online]. Available: <http://www.jstor.org/stable/20110660>
- [88] B. M. Byrne, *Structural Equation Modeling With Mplus*. London, U.K.: Routledge, 2013, doi: [10.4324/9780203807644](https://doi.org/10.4324/9780203807644).
- [89] W. Reinartz, M. Haenlein, and J. Henseler, "An empirical comparison of the efficacy of covariance-based and variance-based SEM," *Int. J. Res. Marketing*, vol. 26, no. 4, pp. 332–344, 2009, doi: [10.1016/j.ijresmar.2009.08.001](https://doi.org/10.1016/j.ijresmar.2009.08.001)
- [90] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis: A Global Perspective*, 7th ed. Uppersaddle River, NJ, USA: Pearson Prentice-Hall, 2010.
- [91] D. Pal, P. Roy, C. Arpnikanondt, and H. Thapliyal, "The effect of trust and its antecedents towards determining users' behavioral intention with voice-based consumer electronic devices," *Heliyon*, vol. 8, no. 4, Apr. 2022, Art. no. e09271, doi: [10.1016/j.heliyon.2022.e09271](https://doi.org/10.1016/j.heliyon.2022.e09271).
- [92] W.-L. Hu, K. Akash, T. Reid, and N. Jain, "Computational modeling of the dynamics of human trust during human-machine interactions," *IEEE Trans. Human-Machine Syst.*, vol. 49, no. 6, pp. 485–497, Dec. 2019, doi: [10.1109/THMS.2018.2874188](https://doi.org/10.1109/THMS.2018.2874188).
- [93] F. Acikgoz and R. P. Vega, "The role of privacy cynicism in consumer habits with voice assistants: A technology acceptance model perspective," *Int. J. Hum. Comput. Interact.*, vol. 38, no. 12, pp. 1138–1152, Jul. 2022, doi: [10.1080/10447318.2021.1987677](https://doi.org/10.1080/10447318.2021.1987677).



DEBAJYOTI PAL received the B.E. degree in electrical engineering from Nagpur University, Maharashtra, India, in 2005, the M.Tech. degree in information technology from the Indian Institute of Engineering Science and Technology Shibpur, Shibpur, Kolkata, India, in 2007, and the Ph.D. degree in information technology from the School of IT, KMUTT, Bangkok, Thailand. He is currently working as a Lecturer with KMUTT. His research interests include multimedia systems, the IoT, and human-computer interaction.



MOHAMMAD DAWOOD BABAKERKHELL was born in Afghanistan. He received the B.C.S. degree in computer science from Shaikh Zayed University, Khost, Afghanistan, in 2009, and the M.Sc. degree in network technology and management from the Amity Institute of Information Technology, Amity University, Uttar Pradesh, India, in 2019. He has been working as a Lecturer at the Information Technology Department, Computer Science Faculty, Shaikh Zayed University, since 2011, where he is currently working as a Vice Chancellor of student's affairs. His research interests include information technology management, computer network and security, cloud computing, and the Internet of Things.



PRANAB ROY (Senior Member, IEEE) received the Graduate degree in marine engineering from MERI, Calcutta, the M.Tech. degree in information technology from Bengal Engineering and Science University, Shibpur, and the Ph.D. degree in engineering from IEST, Shibpur, India. He is currently an Associate Professor at J. K. Laxmipat University, Jaipur, India. He worked as a Senior Marine Engineer Officer on board ships. His research interests include digital microfluidics, VLSI design automation, embedded systems, cognitive computing, AI and machine learning, graph theory, and algorithms. He is a member of ACM and a Corporate Member of IEI and RINA, U.K.