International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Usability Challenges in Smart Home Devices

Akash Kumar, Dr. Vishal Shrivastava, Dr. Ashok Kumar Kajla

Akashkumarsoni6171@gmail.com, vishalshrivastava.cs@aryacollege.in, ashokkajla@aryacollege.in

"Department of Artificial Intelligence and Data Science, Student of Artificial Intelligence and Data Science, Arya College of Engineering and IT, Kukas, Jaipur"

KEYWORDS

Smart homes, Users, Technologies, Smart devices, Authenticati - on, Households, Ener -gy, Assisted living, Usability Challenges,
Future Research

ABSTRACT

In this work, we describe designs and possible attacks of current smart home environments for the purpose of designing novel authentication mechanisms. Our work is motivated by the ever-increasing number of smart devices in people's homes that are intended to improve users' daily life. Examples of such devices include, but are not limited to, smart TVs, cleaning robots, devices for health and well-being, as well as for cooking. Such Devices can thus collect sensitive information and there after Derive information such as if a user is home how often they cook or Watch TV, etc. Smart home devices aim at convenience, efficiency, and security but are still a challenge on the usability front, which really restricts their adoption. Difficulties include complicated setting processes, lack of interoperability, and unintuitive user interfaces, which often are sources of frustration for users. Problems with connectivity, varied performance, and overdependence on smartphone applications really don't help the issue with usability. Other limitations to adoption include privacy concerns, security fears, ease of access, and cost. These encompass the user-centric design standards with basis, security robustness as well as intuitive interfaces that may challenge an innovator. Developers ought to solve these areas so better adoption rates are driven and ensure this promise of smart homes happens. In order to understand potential threats that may be emanated by smart devices accessing sensitive data we begin by drawing out a design and problem space. The work is further enhanced with an in-depth discussion of future research directions and Challenges as well as how threats can be mitigated by visionary novel authentication approaches.

1. INTRODUCTION

Smart home devices are coming onto the market at a rapidly accelerating pace. These devices collect and allow access to sensitive data. Simultaneously, appropriate authentication mechanisms are still scarce. However, they will increasingly be important as more devices enter our homes. Existing designs of smart home devices either omit authentication, demand one-time authentication only (e.g., establishing the Netflix account for the smart TV), or provide workarounds as smartphone apps, which usually represent the only interface to a device(s) for smart devices with unusual form factors or user interfaces. But we hardly notice authentication devices with peculiar (unusual) form factors or user interfaces. There is tremendous potential: Smart devices introduce new means of input, including touch interfaces, speech, etc., come equipped with novel output devices like haptic feedback, audio, etc., and are networked. These properties can be used by designers of

smart home devices, to come up with new authentication concepts – specifically such that are compliant with Nielsen's postulate for security mechanisms of the way users behave. One of the solutions for smart home automation or controlling lighting, heating and cooling, entertainment, and security systems has become widespread in mass markets. The main constituents of smart home systems are the controllers, sensors, and smart devices. A smart home can be controlled in many ways, such as mobile applications. Web interfaces, voice assistants, chatbots, physical interfaces. The advantage of a smart home is that it could automatically control the house's physical systems (doors, heating system, video surveillance, etc.). A good example of this would be setting lights in a house to go off when no one is in the room or dim them for a movie night. It means smart thermostats would learn your preferences, hence be in control of heating and cooling while adjusting temperatures for the most comfortable and energy efficiency use.

Information and communication technologies are integrated into consumer appliances, such as phones and TVs, and infrastructures, such as cities. and grids promises additional functionality, connectivity and manageability. Major technology developers, service providers and energy utilities now line up to extend the smartness beyond specific devices to the home as a whole and link these smart homes to the meters, wires and pipes of the utility networks. The market for smart home appliances alone is expected to grow from $40 m in 2012 to $26bn in 2019.

A smaller, but growing, number of social science researchers ask: Who are the users of smart homes, and why do they want or need them? Will the technological promise of "customized, automated support that is so gracefully integrated with our lives that it 'disappears" be fulfilled? Might there be unlooked-for or perverse consequences? Are smart homes an inevitability or a choice?

The increasing pressure of survival in modern society, the increasing percentage of old people, and the slow increase in the age of childbirth have made the problem of aging increasingly serious. Everywhere in the world, the number of older adults is increasing rapidly, and by 2050, it is projected that the proportion of older adults over 60 will double from 12 to 22% of the population, with 80% of these old people wanted to stay in low- and middleincome countries. In such circumstances, the physical, emotional, behavioural such circumsta- nces will critically alter the cognition-related aspects of elderly people; hence, it is also pretty relevant to research practical necessity among the elderly

In this work we make several contributions toward realizing this vision. First we outline a design space for smart home devices. This design space is meant to capture aspects relevant in the context of authentication. Second, we introduce a problem space that briefly summarizes potential threats to smart home authentication mechanisms. We then propose an approach that enables designers to evaluate possible threats to which their devices are potentially exposed. Finally, we introduce two highlevel authentication concepts that we envision for smart homes: (a) device-centric authentication mechanisms, and (b) home-centric authentication. We end with a discussion of challenges associated with these two concepts. With our work, we hope to provoke a discussion regarding the design of smart home authentication mechanisms. We see large opportunity to design novel mechanisms that blend with the way in which users interact in smart homes, hence making them not only secure but highly usable.

2. BACKGROUND

To set the scene for our work, we will provide a brief introduction to smart environments, authentication and threats.

2.1 Smart Homes & Devices

We consider a smart home to be creating an "intelligent living environment for daily convenient life". In addition, a smart home refers to a home that combines several IoT devices and appliances which can be controlled and operated remotely and automatically. Such configuration usually involves a smart central controller, multiple switch modules allowing access to various devices such as lightings or to values such as temperature and so on connection to the internet for remote access and control. In particular, smart devices are capable of communicating and computation from simple sensor nodes to home appliances and high-tech smart phones. Homes furnished with IoT devices and systems that help in monitoring, managing, and automating functions like light, heat, security, and entertainment at a distance. Most of the technologies need the IoT for communication with other devices for a very smooth user experience.

The ability of smart appliances to work with or without a human's input by using scheduled presets or real-time sensor inputs such as automatically turning lights on and off as one arrives or leaves home. It is the capability to access and control appliances from anywhere in the world via applications, websites, or voice assistants such as viewing and adjusting home security cameras from an office. Smart homes automate the most repetitive works, thereby allowing more quality time on other priorities. Voice assistants such as Alexa or Google Assistant offer operation without touching. Central apps or hubs make it more manageable for a large set of devices. Smart houses reduce waste in energy and also employ smart thermostats and lighting systems by adjusting usage patterns. The smart washing machine and other appliances work at the most efficient times, minimizing energy cost. Energy reports from the devices give the user an idea of how to cut consumption.

2.2 Interaction in Smart Homes

Interaction with a smart home and its devices is complex due to a) an arbitrary number of devices to control and b) multiple users of various target groups. Interaction with several devices or by several users can take place concurrently. To overcome this, Beigl suggests an appliance to point out the device to be acted first and then control it thereafter. User specified gesture techniques have been exposed even further Research. Some of the new interaction modalities are: controlling smart home using trigger-action programming. In addition to these touch, voice or tangibles are also possible in this setup. Since many of the smart devices do not have UIs such as keyboard or display the whole smart home is controlled by a central unit usually from the smartphone. Despite the fact that a centralized control unit for the smart home has been set up useful in with all these factors and previous works, we envision that the direct interaction paradigm will occur with decentralised, therefore when the number of smart devices increases drastically in the future. Interaction in smart homes is concerned with how one interacts and controls smart devices and systems. Simple or complex, they could be by voice, other times by routine automated operations. Interactions ought to be smooth and intuitive with efficiency to the user of technology in his daily life.

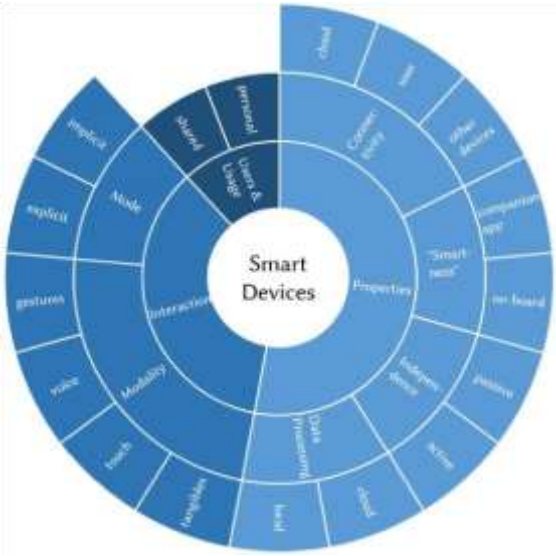


Fig. 1. Design Space: Dimensions of current smart devices that may a) possibly serve as vulnerable point for an attack and/or b) may be employed for existing as well as novel authentication mechanisms.

2.3 Authentication Mechanisms

Typically, we distinguish three classes of authentication mechanisms according to the authentication factor:

Knowledge based authentication mechanisms require users to remember a secret; token-based authentication mechanisms require the use of an object, such as keys or a smart card; and biometric approaches identify the user based on their physiology (e.g., fingerprints) or their behaviour (gait, typing). These authentication mechanisms are used in many areas (e.g., smartphones, websites). Of great interest in smart homes are online accounts, as they can be accessed through an increasing number of devices (e.g., smart TV) and make use of traditional knowledge-based factors (e.g., passwords). Other devices, such as smart speakers, may make use of alternative approaches like voice biometrics2. However, transferring these to the smart home is difficult. Such difficulties include entering secure (i.e. lengthy) passwords on remote controls (e.g., for logging into a SmartTV account), being tedious, time It becomes consuming, and frustrating to the users. Mostly it leads to a single login on setting up. Other problems arise from the fact that some different users might have differing access rights; however, this aspect might not be reflected by the authentication model.

Authentication mechanisms in smart home devices are important to guarantee secure access to systems and protect sensitive data. In addition, the interconnected nature of a smart home ecosystem means that solid authentication protects against unauthorized access and cyberattacks. Users log in to smart devices and applications using a username and password. Web or mobile apps controlling smart devices. Admin panels for routers and hubs. Identifying particular devices as trusted and allowing for seamless access. Smart locks automatically unlock when paired smartphones are detected in proximity. Devices can be paired using Bluetooth or NFC, such as wearable devices that authenticate users. Single signon systems which allow users to get into many smart devices and platforms with only one account (e.g. Google or Apple login), but it's an industry-wide standards that ensures safe and interoperable device communicate -on and robust authentication.

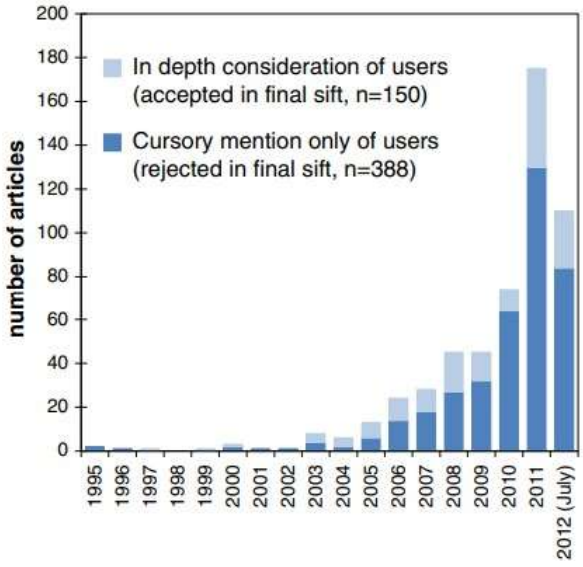
3. WHY THE SMART HOME?

Why is the smart home becoming a more and more significant field of research and development? Three general perspectives are to be seen in the literature: a functional perspective; an instrumental perspective; and a sociotechnical perspective. The functional perspective sees smart homes as technology for improved handling of the requirements of daily life. The instrumental perspective highlights the smart home's potential contribution to energy control and demand reduction in households within a broader transformation to a lowcarbon world. Socio-technical sees the smart home as the next stage of development in the ongoing electrification and digitalization of daily life.

3.1 Functional View

Advocates of the functional view contend that providing and integrating the functionality that is currently available in homes by a range of information and communication technologies (ICTs) will result in 'better living'. Much of the technologically centred literature on smart homes represents their benefits for end-users as both intuitive and comprehensive: comfort, security, scheduling tasks, convenience through automation, energy management and efficiency; and for some end-users, health and assisted living. Balta-Ozkan categorizes these benefits into three categories: lifestyle support, energy management and safety. Obviously, user-centered research focuses on the improvement of the current services rather than providing something new: "the point of technology is not to replace experiences that we already enjoy today with our families… [but to] support or enhance experiences you already enjoy… but in new ways ". Smart homes can provide for more intelligently connected workspaces, enhance any old televisions to provide interaction capability, and help bridge over digital divides by allowing elders and other previously excluded from information society households into being members.

The functional perspective does show an extremely broad range of tasks and functions that smart homes can be planned to assist individuals in performing: remote control over some home appliances, improving memory and recalling through automated reminder functions, improving security through simulated occupancy in homes that are vacant, etc. These all relate generally with users' perceived requirements for increased comfort, convenience, security, and entertainment. Improved in specific ways, security has a definite value for its users.



3.2 Instrumental View

A more clearly instrumental or goal-oriented view of smart homes emphasizes their potential to help achieve energy demand reduction goals, with attendant benefits to households, utilities, and

policymakers. The interests of households wishing to save money and energy align with the interests of utilities improving energy system management and the interests of policymakers in reducing greenhouse gas emissions and ensuring a secure and reliable energy supply. The instrumental approach thus sees the smart home as a central technological intervention to the supply of a low-carbon energy transition at affordable costs.

Building on current research in the commercial and institutional sectors on "intelligent" buildings with automated energy management systems. The instrumental view posits core parts of the smart home as: smart meters, smart energy-using appliances and energy management functionality to allow user-control and programmed optimization of appliance use and microgeneration. Thus, energy smart homes provoke a change from passive end users into 'micro-resource managers'.

Tailored, real-time and in-home information and feedback on energy use (and prices) via smart meters and in-home displays help to "make energy visible". Smart technologies also open up a variety of new possibilities for home energy management that were not accessible via older "dumb" systems of monthly feedback via energy bills. Smart homes, it is therefore claimed, will enable energy to be turned off, cut back, switched over, upgraded or relocated. But real proven energy saving accruing from the use of Smart home technologies is modest in experiments or field tests, although potential savings (or 'shaving') during peak times may be more substantial. Experiments on large scales of smart meters and in-home displays in the UK revealed average decreases of approximately 3 % of energy. Households' preference or tolerance for reducing energy consumption as a result of information feedback and price incentives would appear to be moderate, with information and price incentives exhausting quickly. The utilities that sell electricity are proponents of the instrumental position but don't care quite as much at the household level about savings so much as in using smart meters. These will provide utilities with near real-time data on demand and supply that are distributed through the millions of nodes of the distribution system [58]. Integrated in-home displays giving end-users information about usage and cost enable utilities to charge for electricity at its marginal cost, thereby sending a price signal to move or decrease demand when supply is expensive or limited. Households are therefore smoothly integrated into wider 'smart grids', where energy management capacity is considerably enhanced for utilities and also presents potential efficiency possibilities with allied This utility-focussed instrumental mindset is already very common in the USA and gaining ground in Europe as the rationale for smart meter rollouts and smart grid planning.

3.3 Socio-technical View

Instrumental and functional explanations dominate the reviewed literature, although a third "socio-technical" conceptualization of the smart home may also be discovered. This socio-technical approach is not interested in the concrete functionalities smart homes can deliver or in smart homes as utilitarian tools to realize other energy objectives but imagines smart homes as the latest (or perhaps next) installment in the coevolving record of technology and society. The socio-technical approach emphasizes how use and meaning of technologies will be socially constructed and iteratively negotiated, rather than being the inevitable outcome of assumed functional benefits. Røpke et al. place "the pervasive integration of ICT into everyday practices" within the context of what they refer to as the "third round of household electrification". Previous stages were lighting (early 1890s) and power and heating. The underlying technology of this generation is the micro-chip, which made creeping digitalisation of almost every aspect of daily life possible. Visionary ideas of technological innovators drive this sociotechnical vision. Park et al., for example, propose conceptual designs of smart pens, pillows, dressing tables, doormats, picture frames, sofas, walls, windows and so on with equally wide ranges of services, ranging from memorizing, reminding, scenteding, lighting, recognizing, resonating, connecting and rejuvenating. Taylor et al. draw attention to the potential of virtually any 'surfaces' (walls, doors, bowls) to be made 'smart' digital screens within an 'ecology of surfaces' with and through which people interact.

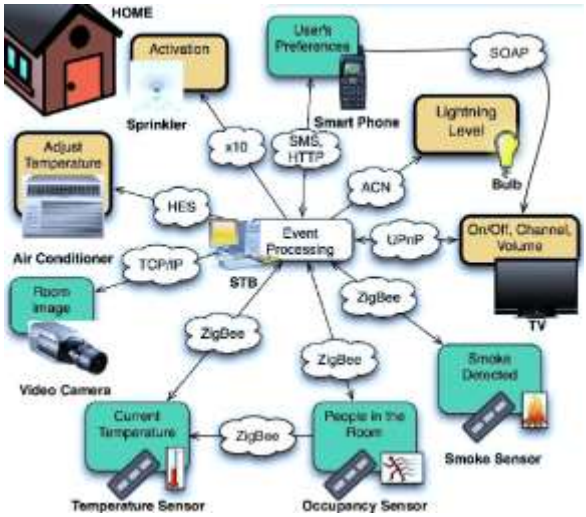
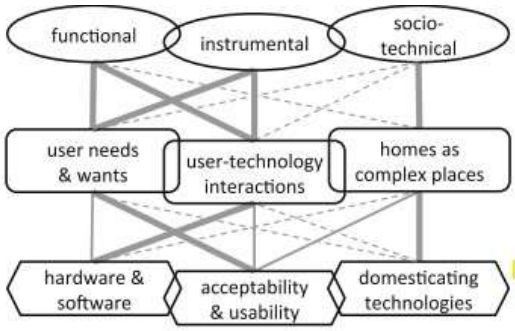


Fig. 3 This figure illustrates ***interactions between smart home devices*** *and a central* ***event processing system****.*



4. DESIGN SPACE: CURRENT SMART HOME DEVICES

To understand better the characteristics and properties of smart home devices and their implications on security, we chart a design space in the following (cf. Fig. 1). We are particularly He might find characteristics that would allow for an appropriate authentication and/or b) expose the device to possible attacks.

4.1 Users & Usage

Unlike many ubiquitous computing devices, smart home devices may not be used singly i.e., personal by an individual user, but shared naturally between small groups (e.g., families, flatmates, etc.). This poses additional challenges, such as account switching ability is required, increasing number of logins, etc. Smart home devices are utilized by a wide range of user groups to address different needs, improve quality of life, and enhance daily activities through automation, control, and convenience.

4.2 Interaction

1) *Mode*: The mode of interaction for the traditional home appliances has traditionally been explicit (for example, a person switching on the light when arriving home). With devices turning "smart", implicit interaction may increase more and more (e.g., the light comes on automatically as users enter a room).

2) *Modalities*: As described in section II-B, there are multiple interaction modalities in the smart home, such as gestures, voice, touch, and tangibles. This provides potential for input of knowledge-based authentication, but also (physiological as well as behavioural) biometrics.

4.3 "Smart" Properties

While an increasing number of consumer devices is called "smart", only few of them offer "intelligent" features. In the context of this work, we consider a home device to be smart if it has the following properties:

1) *Connectivity*: Many components of a smart home provide some form of connectivity. They may be connected with the cloud (i.e. the provider), the user (e.g., for remote control or other tools in the same space. It is so that, for example, it might send or receive data or commands

2) *Smartness*: The real "smartness" (that which distinguishes the "smart" appliance from its "dumb" peers) may lie in the device proper (in-board) or be supplied through an ancillary application, for example, on the cell phone.

3) *Autonomy*: Smart devices function on several levels of self-sufficiency: at one end, passive addons. (e.g. sensors gathering data on air quality), others active, so that the device can take in and manage (e.g. light controls), or even work alone (e.g. smart thermostat manages heating to save energy, yet keeps set temperature).

4) *Data Processing*: Smart devices can collect and/or process data. This may happen locally, to say for example to manage heating or could be done remotely in cloud to, for example, process voice input. To transmit or Receiving data can be done for a variety of reasons,

including but not limited to the automation of a home or analysis by a provider.

5. USABILITY CHALLENGES AND LIMITATIONS OF SMART HOME DEVICES

Smart home devices have changed modern living because they can automatically perform tasks, provide ease of use, and maximize efficiency. However, various usability challenges and limitations have limited the spread of such adoption. The causes are technical barriers, shortcomings in design, security risks, and user-centric concerns.

5.1 Complexity in Setup and Configuration

Most smart home devices require a series of steps to set up, such as connecting to Wi-Fi, pairing with apps, configuring automation rules, and integrating with other devices. This can be daunting for those with little technical knowledge. Smart thermostats require programming schedules, temperature settings, and user preferences in detail. With the requirement of integration of multiple devices and protocols with smart hubs, it becomes confusing. Thus, users stop using devices as they get frustrated with the setup process. Moreover, non-tech-savvy users require professional help that costs them money.

The communication protocol of the device can be one of these: Wi-Fi, Zigbee, Z-Wave, Thread, or Bluetooth. All may require other hubs or bridges to intercommunicate among your smart home devices. Only selected devices can be used on the ecosystem of Google Home, Amazon Alexa, or Apple HomeKit, which thus limits the seamless integration for cross-platforms. Lack of a universal standard also makes it difficult to integrate various devices from different manufacturers. Initiatives like Matter are in place to help address this, but the adoption is still evolving.

5.2 Interoperability Issues

Many smart home devices employ disparate communication protocols (ZigBee, Z-Wave, Wi-Fi, Bluetooth, and proprietary systems). Most of them are not interoperable, hence presenting problems in combining products of various manufacturers in one house. A ZigBee-based intelligent lighting system may not interoperate with another device, which uses Wi-Fi. Devices that are tied to specific ecosystems, such as Amazon Alexa, Google Home, or Apple HomeKit, may not integrate as smoothly. Users are locked into buying from the same vendor, thus incurring vendor lock-in. Complex Multiple apps and hubs.

These can easily become a major hurdle between seamless and cohesive smart homes: interoperability issues arising from fragmented ecosystems, assorted communication protocols, and of course, the lack of universal standards. Most home manufacturers design their devices specifically to work within their systems: Amazon Alexa, Google Home, Apple HomeKit for instance. A Nest thermostat cannot work directly with Apple's HomeKit without thirdparty workarounds. Where some ecosystems will allow for limited integration of third-party devices, native functionality is typically limited or cannot be matched.

5.3 Learning Curve and User Experience

Bad design and interfaces, confusing controls, as well as a high learning curve all usually lead to usability problems. Most devices require certain levels of technical knowledge, excluding both older generations and new users. With the Alexa or Google Home, commands need to be used for smart assistants, and this might get difficult at times to remember. Interfaces for highly complex apps with too many choices and menus are confusing. Reduces usability for older adults, children, and non-digital natives. Users fail to use advanced features, thereby limiting the value of smart devices.

5.4 Security and Privacy Concerns

Smart home appliances collect much personal and sensitive data from the user and therefore are susceptible to hackers. Most have poor methods of encryption as well as authentication. Smart cameras being hacked, with privacy breaches. Voice assistants, such as Alexa or Google Assistant, record the conversations by mistake. It reduces user trust in smart home technology. It raises ethical questions about data collection and sharing among manufacturers. The critical factors that are more likely to undermine the benefits and convenience drawn from devices in smart homes include insecurity and privacy issues surrounding those devices. As such, these

concerns are usually sourced from how devices collect, store, transmit, and utilise data; vulnerabilities that most likely expose a device to malicious access may also exist.

Manufacturers may use all the gathered data for purposes such as targeted advertising, to share with third parties without consent from the user. There are many devices that have a long, ambiguous privacy policy no one can understand what is done to their data. Most devices come preinstalled with weak or default passwords, which are an easy target. Some devices lack 2FA, making accounts easier to breach. Between a device and cloud servers, transmission data may not be encrypted suitably, thus exposing sensitive data to interception.

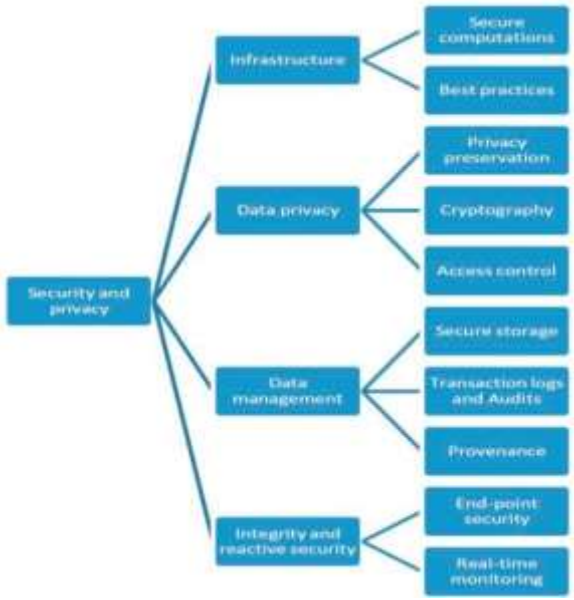


Fig. 5 Security and Privacy

5.5 High Costs and Affordability

Smart home technology is expensive, especially when using multiple devices. Costs are the purchase price, installation fees, and subscriptions for cloudbased services. High-end smart thermostats, such as the Nest, cost more money than a conventional thermostat. Some security systems require a subscription fee to store or even monitor video recordings. Limits adoption to high-income households. Cost becomes a barrier for the widespread implementation.

Basic smart plugs and bulbs are pretty inexpensive. Smart thermostats, cameras, and door locks can get pretty expensive, however. For example, a smart thermostat might cost around $150–$300, while a good security camera or system would be over $500. Some devices need more hubs or bridges to operate, which adds to the expense. Philips Hue lighting requires a separate bridge for full functionality.

5.6 Power and Battery Issues

Most smart devices consume power always: either by battery or while attached to the grid. The ones that consume the energy very fast or are energy-wasting have higher prices and more efforts on maintenance. Sensors and cameras requiring frequent battery replacement. Devices using standby power even after switching off. Decreases long-term costeffectiveness. Inconvenience to the users dealing with various battery-driven devices.

Devices such as smart speakers, hubs, cameras, and thermostats are on the internet 24/7, which means energy usage is constant. With a fully outfitted smart home, the combined power consumption of all devices can noticeably increase electricity bills. Many devices consume "vampire power" even when not in use. Battery-powered devices, such as smart locks, sensors, and cameras, often require frequent battery replacement or recharging. A smart doorbell camera will need its batteries replaced every 2–6 months, depending on usage.

5.7 Data Overload and Cognitive Fatigue

Smart home devices normally throw out too many notifications and data, flooding the user's inboxes with too much information. Security cameras that send alerts for minor movements like pets or leaves. Energy monitors that present complicated data that the user cannot make sense of. It causes cognitive fatigue and information overload. Users may turn off notifications or leave devices. Devices such as smart thermostats, energy monitors, and health trackers produce a continuous stream of data. Energy usage charts, temperature adjustments, and historical logs clutter the user interface. Users cannot distinguish between critical information (such as a fire alarm) and low-priority data (such as a temperature update). Smart home ecosystems often require users to learn new terminologies, device integrations, and troubleshooting methods, which adds to cognitive load.

5.8 Lack of Standardization

The absence of universal standards for device communication and integration creates a fragmented ecosystem. Users struggle with device compatibility across platforms. Smart lights that only work with specific hubs (e.g., Philips Hue with ZigBee). Devices incompatible with emerging protocols like Matter, an open-source standard. Forces users to stick to specific ecosystems, such as Apple, Google, or Amazon. Slows down market growth and adoption.

In other words, one of the significant bottlenecks that are coming against the very notion of smooth interoperability and convenience of the devices for users is a non-uniform approach toward creating standardization within smart home devices. With the non-standardized device approach in most cases, ecosystems cannot properly talk to one another and eventually break off; user frustrations arise due to various product lines unable to converse or work properly together due to some bypass or trick workarounds. The management of different applications for different devices increases complexity and reduces the benefit of a smart home.

5.9 Security Integration at (Smart) Home

In a smart home environment, interaction with devices often is only the secondary task: Hence there is the challenge how to integrate security (i.e. authentication mechanisms) so that they are manageable with little to no attention. Potential input required for authentication should not create any overhead at all. Novel authentication mechanisms, e.g., based on behavioural biometrics, offer great potential for unintrusive, easy, and effortless authentication integrated into the interaction itself. For example, the users could be determined by the type of interaction with one or several of their smart home devices. In the context of shared use of devices, it would be enough to begin with checking from time-to-time which user-coming from a relatively small user group like a family-is currently active to permit content or settings relevant to this user, like cafe latte.

Challenge	Key Issues	Impact
Complexity in Setup	Difficult installations, unclear manuals	Frustration, low adoption
Interoperability Issues	Incompatibility of protocols and devices	Fragmented user experience
Learning Curve and UX	Non-intuitive interfaces, steep learning	Limits access to tech-novice users
Internet Dependence	Device failure during connectivity issues	Reduced reliability
Security and Privacy Concerns	Data breaches, hacking risks	User distrust
High Costs	Expensive devices and maintenance	Limited adoption for low incomes
Accessibility Limitations	Inaccessible to disabled or elderly users	Excludes certain demographics
Power and Battery Issues	Short battery life and energy usage	Inconvenience, extra costs
Scalability Problems	Managing large numbers of devices	System inefficiency

Fig. 6 Summary table of usability challenges

6. User-related challenges for realising smart homes

While there are numerous opinions and proposals of the advantages that smart homes can bring to families, the vision is still not a reality at scale. The technical literature that prevails in smart home and user studies identifies the main technological and design challenges to be addressed. Specific problems in these two groups of challenges are consistent with the social impediments to the uptake of smart homes found in public deliberative workshops by Balta-Ozkan et al. Loss of control, reliability, privacy, trust, cost and Irrelevance. But there is a third group of concerns that more clearly places users in the home's adoption environment and looks at how and if smart home technologies can be effectively domesticated.

6.1 Latest technologies for smart home users

Various problems related to research, development, testing and trialling have to be solved prior to the wide-scale commercialization of smart homes. Technical issues of concern are: sensors and monitors that reliably detect and monitor what is happening in the home, and processing algorithms that sensibly deduce actions and trends from the resulting deluge of data; interoperability and backward compatibility of smart Home solutions, facilitated by well-thought-out and sound standards; and operational reliability and manageability. The priority of such technological challenges varies significantly in light of the underlying smart home vision among the technologists. Smart homes ought not to fail nor behave erratically. Edwards and Grinter highlight several of the different aspects of the problem of reliability, including: debugging smart homes constructed "unintentionally"

through piecemeal-adopted technologies; controlling and maintaining smart homes with self-healing systems that obviate the need for household or third party system managers; and making inferences regarding occupancy activity from potentially vague and untrustworthy sensor readings.

6.2 Designing technologies for smart home users

The usability of smart homes to consumers is connected closely with concerns of security, privacy, and trust and also with functional and ergonomic concerns with user-friendliness. These are viewed as being key design challenges because they concern user-smart home technology interactions. In security terms, for example, Cook observes that "many people are reluctant to bring sensor technologies into their home, not wanting to be leaving digital footprints" in order to gain control over such to break in when the house is unoccupied'. In smart homes with assisted living, Demiris et al. likewise quote users' concerns with privacy in contending that technologies that can detect and monitor activity within the home risk seeming intrusive incursions in the home space. For energy smart homes, both data security and the potential for utilities to be able to monitor inappropriately or even control household demand has resulted in consumer uprisings against smart metering. A recent UK survey of attitudes and values towards energy system change identified broad support for the development of smart homes.

The way homes are smart-designed will limit their acceptability to end-users in the future. Cook recommends firmly establishing and ensuring levels of privacy and safety and security of technologies. Paetz et al. suggest the necessity of much greater levels of transparency and accountability on the part of smart home developers—and particularly energy utilities—and an imperative to make it clear exactly how all interested parties could benefit from smart home development. Rohracher argues that all of these problems could be prevented through more participatory design practices. He proposes including a wide range of different stakeholders even in the visioning stage of smart home systems so that the maximum number of different interests and concerns are brought up and addressed. Several other studies indicate more specifically defined design challenges in terms of how accessible smart homes must be. Park et al., for example, outline the wide scope of potential smart applications but caution against "overpowering" users with "complex technologies". Different studies highlighted the difficulties of offering intelligent and simple user-interfaces with the level of complexity and number of options for user-control which might be available behind the interface. User-centred design has often been referred to as being a useful remedy to smart home design issues. Orpwood et al. identify a number of straightforward design solutions that are able to ease specific issues faced by dementia patients, such as fear of novel equipment and forgetting. By consulting carers, researchers could come up with relatively straightforward and occasionally low-tech solutions like making equipment seem normal, hiding it from view so the patient will not be alarmed and using cues and prompts rather than stripping the user of control. Different groups of users will require different solutions, not merely simply across houses but across cultures. Jeong et al., for example, reveal dramatic differences in the need for and awareness of control between USA and Korean smart home users.

6.3 Situating smart home technologies amid everyday life at home

This gives rise to new kinds of design rules for producing technologies that are conducive to and aligned with users' work of administering daily life. Technologies can be made 'for ambiguity, instability, concealment, and disinterest, and to be treated casually'. Davidoff et al. have provided a set of seven principles which indicate that the new technologies must be attuned to 'the organic evolution of routines and plans', 'periodic changes, exceptions and improvisation', 'breakdowns', 'multiple, overlapping and sometimes conflicting objectives' ' and must "engage with the building of family identity ". If the smart home idea is not re-designed in these ways, it will not work. But as Howard and co-authors warn, values of this sort would be "dreadfully hard to operationalize in technology research". The greatest user-centered challenge for successful smart home design is therefore not to functionalize or make technologies more reliable, or eliminate worries regarding trust, privacy or usability, but rather to redefine the concept of 'smart' itself, as a way of understanding how it is made up in users' everyday lives and how technologies are utilized within the home. To quote Taylor and authors: 'it is people who put intelligence into places by constantly connecting

things in the physical world and in their own routine and singular social arrangements.'.

7. APPROACHES AND FUTURE RESEARCH DIRECTIONS

For new smart devices in the smart home, usable security should be integrated by design, i.e., smart devices of the future should provide feasible, builtin authentication mechanisms, seamless and intuitive. Such methods shall include conventional ones like PINs and passwords but maybe also introduce new, novel, device- or even home-centric mechanisms based upon interaction behaviour, behavioural patterns and routines or chains of device usage.

7.1 Device-Centric Authentication

Traditional authentication is typically conducted on one device (e.g., log into a laptop) or service (e.g., log in to use Netflix). We view this as an asset to move onto arbitrary (smart) devices because it aligns with the users' mental model of "unlocking" a device before using it. To further enhance security, other mechanisms could also be moved onto smart devices. For example, a smart speaker could ask dynamic security questions before accessing personal content.

However, using legacy mechanisms mitigates some of the risks, such as listening for voice input or, in fact, introduces new ones, such as waiting for input at the smart door, which may enable burglary. Additionally, input modalities in smart environments vary and may limit possible authentication factors, such as not all devices allowing entry by a PIN via a numpad. In addition, the pain of remembering lots of passwords for various online accounts, remembering different Input modalities may impose additional loads on users. This can be alleviated by a) the same mechanism for a group of devices (which naturally, once again blurs security by introducing another "single point of failure") or b) other devices in the smart environment switch to. For example, the smartphone often acts as a hub and workaround to protect the smart appliance. Other devices may offer opportunities for token-based (e.g., token rings) or biometric (e.g., fingerprint sensors) authentication. Many smart appliances already provide secondary input devices (e.g., remote controls for smart TVs), where input authentication could be included.

7.2 Home-Centric Authentication

A smart home typically has many "smart" components that are connected. This makes it vulnerable on one side, but on the other side, it opens the possibility for future, scalable authentication in the smart home through a combination of these to authenticate, without losing usability as well as security. The smart home and its devices can be used for authentication in several ways. The (explicit) input for authentication can be performed on several instead of on a single device. For example, secret input can take into account the smart TV's remote control, light switch, and smartphone. Also, we can imagine implicit authentication in the smart home. Such an authentication mechanism would, for example, consider "natural" interaction with several devices in a certain context (i.e., switching on a certain light and TV channel when user comes home from work). It has several advantages. First, it is scalable and easy to expand; it is not limited to the devices currently present in the smart home. It is very usable and seamless because it avoids any additional burden, but instead uses the "normal" user interaction for authentication. In addition, it uses functionality a smart device provides by design; that is, being connected with other components in the smart home same smart home and is therefore easy to deploy. It can also improve security using multifactor authentication. For example, an authentication method can be chains of interaction with other devices or transfer the current level of security from one device to another.

8. CONCLUSION

We provided a design space for smart home devices, yet simultaneously talked about possible threats and challenges along with the opportunities for new and applicable authentication mechanisms in the smart Home. We describe how it can be applied to the design process and provide alternative security views for smart homes.

The smart home devices have revolutionized modern living by making it more comfortable, convenient, and efficient. However, usability challenges are one of the major barriers to the wide adoption and proper use of smart home devices. Key challenges include complex setup processes, interoperability issues, poor user experience (UX), security and privacy concerns, limited accessibility, and high costs. These problems do not only

limit the user experience but also prevent smart home from being inclusive and scalable at the same time. So, all of these shall be addressed in a broad approach. So, the agendas should be first on manufacturing usercentric designs. That includes making it simpler to operate these smart devices, enabling interoperability among various other devices without complication or interference, and making more aggressive security mechanisms for all possible user data. Then there is cost and elderly/physically challenged user considerations-making it possible for even wider audiences to utilize such devices. Collaborative efforts between technology developers, policymakers, and end-users are needed to create smarter, more reliable, and inclusive systems.

Smart homes are a developing wave of technological innovation whose realization depends on convergence between visions of technology designers for functionality and energy use and needs and demands from households in the complex place that is home. The user-centric research on smart homes is expanding, dominated by engineering, technical sciences and design but with a meaningful niche in health care research and with growing attention of social scientists ranging from ethnographers and domestication theorists to economists and applied energy researchers. However, there is an extensive and expanding recognition of the need to develop a better picture of who users are and how they might use smart homes.

Conclusion Despite the enormous potential of smart home devices, overcoming these usability challenges is crucial to achieving broad acceptance and long-term success. Future research should focus on the refinement of human-device interaction, enhancement of energy efficiency, and innovative solutions for emerging challenges. In this way, smart homes will become truly user-friendly environments, meeting the needs of all users and spurring sustainable growth in the IoT ecosystem.

REFERENCES

[1] *S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," 2016 3rd MEC International Conference on Big Data and Smart City, ICBDSC 2016, 2016.*

[2] K. Bing, L. Fu, Y. Zhuo, and L. Yanlei, "Design of an Internet of thingsbased smart home system," Proc. ICICIP 2011, no. PART 2, 2011.

[3] *P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," 4th IEEE Sponsored International Conference on Computation of Power, Energy, Information and Communication, ICCPEIC 2015, 2015.*

[4] *M. Wang, G. Zhang, C. Zhang, J. Zhang, and C. Li, "An IoT-based appliance control system for smart homes," Proc. ICICIP 2013, 2013.*

[5] *B. L. R. Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," Journal of Cleaner Production, vol. 140, pp. 1454–1464, 2017.* [6] *M. Beigl, "Point & click-interaction in smart environments," in Symposium on handheld and ubiquitous computing. Springer, 1999.*

[7] *C. Kuhnel, T. Westermann, F. Hemmert, S. Kratz, A. M ¨ uller, and ¨ S. Moller, "I'm home: Defining and evaluating a gesture set for smart- ¨home control," Int. Jour. of Hum.-Comp. Studies, vol. 69, no. 11, 2011.*

[8] *B. Ur, E. McManus, M. Pak Yong Ho, and M. L. Littman, "Practical trigger-action programming in the smart home," in Proc. CHI '14. ACM, 2014.*

[9] *T. Koskela and K. Va¨an¨anen-Vainio-Mattila, "Evolution towards smart ¨ home environments: empirical evaluation of three user interfaces," Personal and Ubiquitous Computing, vol. 8, no. 34, 2004.*

[10] *L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, Dec 2003.*