THEME ARTICLE: LIFE AND WORK AT HOME

A Framework for Evaluating the Security and Privacy of Smart-Home Devices, and its Application to Common Platforms

Ravindra Mangar, Timothy J. Pierson, and David Kotz, *Dartmouth College, Hanover, NH, 03755, USA*

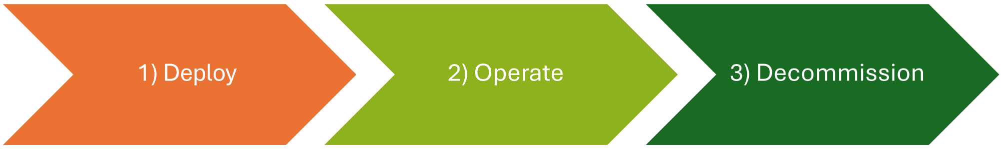
In this article, we outline the challenges associated with the widespread adoption of smart devices in homes. These challenges are primarily driven by scale and device heterogeneity: a home may soon include dozens or hundreds of devices, across many device types, and may include multiple residents and other stakeholders. We develop a framework for reasoning about these challenges based on the deployment, operation, and decommissioning life cycle stages of smart devices within a smart home. We evaluate the challenges in each stage using the well-known CIA triad—Confidentiality, Integrity, and Availability. In addition, we highlight open research questions at each stage. Further, we evaluate solutions from Apple and Google using our framework and find notable shortcomings in these products. Finally, we sketch some preliminary thoughts on a solution for the smart home of the near future.

As smart devices become increasingly present in our lives, the need for addressing issues of scale and complexity become ever more pertinent. Consider a family of four living together in a single-family home today. Each person in the family may have a laptop, a tablet, a smart phone, and a smart watch or fitness tracker. That family already has 16 smart devices. Add in other smart-home technology like televisions, gaming devices, door locks, lightbulbs, thermostats, and appliances, and the number of devices in the home grows rapidly. Analysts expect that many “dumb” things will soon become “smart” things by adding capabilities for sensing, computation, and communication. Smart clothing, for example, may become common, enabling the wearer to monitor pulse and respiration. Others envision smart forks that record what each resident eats. If each article of clothing owned by each resident becomes smart, and if each piece of cutlery similarly becomes smart, the number of devices present in the home will explode. It is fair to estimate that today’s homes contain dozens of smart devices, and tomorrow’s homes may contain hundreds of smart devices of varying types.

The purpose of this article is not to report on specific scientific discoveries, but rather to discuss the challenges involved with managing a home with dozens or hundreds of smart devices, to highlight open research questions, and to evaluate prominent vendor solutions. We also sketch a preliminary vision of a solution for the smart home of the near future.

Building on the definitions provided in previous studies,[1] we characterize a *smart device* as an object embedded with digital electronics and a network interface, facilitating communication with other devices and remote services within the framework of the Internet of Things (IoT). These devices are outfitted with sensors and sometimes actuators, enabling them to interact with their surroundings. These devices may be capable of exchanging data and coordinating activities using several different communication protocols and exhibit a wide range of characteristics including mobility, size, and power sources, all tailored to perform distinct functions. We define a *smart home* as a residence equipped with a collection of smart devices that can communicate and interact with one another, with or without a single common network. We refer to *management* as the comprehensive process of

Digital Object Identifier 10.1109/MPRV.2024.3421668



	1) Deploy	2) Operate	3) Decommission
Task	Initially configure devices	Use devices	Remove from service
Confidentiality	• Discover new devices • Make secure introductions • Manage different protocols & communication links	• Prevent privacy inferences	• Remove all sensitive information • Transfer ownership
Integrity	• Establish access control • Update and patch • Ensure safety	• Update access control • Update and patch	• N/A no longer part of the home environment
Availability	• Manage Scale • Accommodate device heterogeneity	• Repair • Handle mobile devices	• N/A no longer part of the home environment

FIGURE 1. Framework overview for evaluating the challenges involved with managing smart home devices during each stage of the life cycle.

configuring, controlling, and maintaining various interconnected smart devices to ensure they function efficiently and securely. Management of the smart home becomes more difficult as the number and type of devices increases.

We have never before faced the problem of configuring and managing so many home-computing devices. Starting in the 1980s, home computers became popular. Back then, a home might have a single computer operated by a technology enthusiast. In the 1990s, laptops became commonplace and homes frequently had multiple computing devices. By the 2010s, there was a computer in every pocket. In the 2020s, everyday items have become computers. If this trend continues, it will no longer be feasible for consumers (other than the most dedicated home enthusiast) to manage hundreds of devices. For example, it is impractical to expect consumers to install a separate management app for each brand of "smart shirt" they own.

Even if a person does not want smart devices in their home, they may soon become difficult to avoid. A recent trip to a local electronics store revealed that finding a nonsmart television is difficult, if not impossible.

The home has traditionally been a refuge from outside observers and constant vendor monitoring. Inviting these vendors into the home, especially if a single vendor controls all devices in the home, opens the door to privacy invasions to a degree never previously possible. *We need a scalable device management solution that promotes flexibility and privacy*.

EVALUATIVE FRAMEWORK

To comprehensively evaluate the challenges involved with device management in a smart home containing a large number of heterogeneous devices, we consider each stage of the device's life cycle. In particular, we examine the challenges when 1) the device is *deployed*—introduced to the home and configured to communicate with other devices, 2) the device is *operated*—used in daily life, and 3) the device is *decommissioned*—removed from the home environment.

We evaluate the challenges involved with each life cycle stage with the well-known CIA triad—Confidentiality, Integrity, and Availability. We chose this framework because it has been widely used to evaluate privacy and security threats.[2,3] *Confidentiality* means that data are only available to intended parties and is not available to others. *Integrity* means that data cannot be inappropriately injected, altered, or deleted (at least without detection). *Availability* means data and services are accessible for use when needed.

Figure 1 provides an overview of our evaluation framework. We first discuss the framework, highlighting open research questions, then use the framework to evaluate popular device management solutions from Apple and Google. We find those solutions have notable shortcomings.

Deploy Phase

The deployment of smart devices in a smart home entails the initial setup and integration of these technologies into a residential environment. This phase lays the groundwork for how effectively and securely the devices will function and interact with each other. Here we discuss the CIA triad in the Deploy phase.

Confidentiality

In the Deploy phase, confidentiality refers to establishing secure communications for a new device being introduced to the home environment. This includes connections between the new device and other devices already deployed in the home, as well as connections to the cloud and a cloud account. Some devices may only communicate with the cloud, while others may not communicate externally at all. The purpose of these secure connections, of course, is to ensure data are available to intended devices, but not others. We leave physically tampering with devices out of scope for this article.

Key confidentiality steps at the Deploy stage include discovering new devices, making secure introductions with other home devices, managing credentials, and handling multiple communication protocols and links.

Discover New Devices

The arrival of new devices must be quickly detected—and distinguished from new devices that may be nearby but outside the home, such as in a neighboring apartment. Khanafer et al. define four functions of device discovery: 1) learning of a device's presence in an area, 2) determining the device's identity, 3) determining whether the device belongs to the home, and 4) localizing the device in three dimensions.[4] Each of these steps can enhance the process when a new device enters a home, although localizing the device in three dimensions may not always be critical.

Open research questions:

- How can new devices be detected without human assistance, especially if the devices do not transmit signals without a trigger event?
- Sniffing network traffic is a popular choice to discover devices, but devices may operate using many different communication protocols (e.g., Wi-Fi, Bluetooth, Zigbee, Thread, and others). How can all devices be detected, regardless of their protocol?
- How can devices be specifically identified (i.e., what kind of device has arrived) while protecting against those that might spoof their identity? What about legacy devices that may not conform to any standard discovery protocols?
- How can a new device be identified as one the resident intends to include in the home network, as distinct from other devices that may enter the home but the resident does not intend to add to the home's infrastructure? (For example, a friend brings their smart phone into the home during a short visit; it should not necessarily be added to the smart-home infrastructure.)

Make Secure Introductions

Once a device has been discovered and identified as a candidate to join the home's network, it should be securely introduced to other devices in the home. A significant challenge is to determine *which* existing devices should communicate with the new device and to facilitate secure introductions with those devices. Further, an ideal management system would also impart configurations and policies on the new device that are consistent with user intent. For example, a new door lock should ultimately communicate with the hub over a secure connection. The door lock should first be introduced to the home's Wi-Fi router for confidential wireless communications and then should be provided the IP address of the hub. The resident may want the system to raise an alarm if the door is unlocked while the resident is not physically at the door. Making such a series of secure connections and inferring user intent becomes increasingly difficult as the number and type of devices in the home increases. Without help from a management system, the resident must take all of these actions themselves, an increasingly error-prone proposition!

Open research questions:

- How to determine which home devices should communicate with a newly discovered device?
- Once that set of devices is identified, how can secure communications connections between devices be accomplished with minimal (or no) human intervention?
- How can a system infer user intent for a new device? Should it operate like similar devices already in the home? If not, how can this new device's unique role be identified?
- What if the system makes an incorrect inference?

- What if there are policies that are inconsistent or impossible (e.g., open the windows if it is hot outside for comfort, but keep windows closed to keep out burglars for security)[5]?
- Should visitors and their devices be handled differently, and if so, how?

Manage Different Protocols and Communication Links

A home with a large number of smart devices of a variety of types may operate over many different protocols. Some devices may operate on Wi-Fi, while others use Bluetooth, or Zigbee, or Thread. Each of these protocols has its own methods to ensure data confidentiality. A management challenge is to ensure confidentiality on all communication links, over all protocols. This task is increasingly daunting as scale grows.

Open research questions:

- How can communication links between devices be established over multiple protocols?
- What happens as new protocols become popular? Matter, for example, is a new protocol seeing increasing adoption.[6] How could Matter be incorporated in a home with non-Matter compliant devices?
- How can nonexperts configure devices, even if devices use different protocols?

Integrity

In the Deploy phase of the smart home device life cycle, ensuring integrity involves establishing robust measures to prevent unauthorized data modifications and guarantee that the devices function as intended right from installation. Here we discuss some of the challenges associated with maintaining integrity during the Deploy phase.

Establish Access Control

In the Deploy phase, data integrity is influenced heavily by access control mechanisms. This step involves defining roles clearly, specifying which subjects can access which objects with which rights and which subjects can alter these permissions.[7] For instance, in a smart home, it is prudent that a toddler cannot activate the stove, a young child is barred from accessing a woodshop, a young teen is restricted from R-rated content, and a teenager cannot alter the security camera logs. The toddler should not be able to unlock the pet door—but the pet should—highlighting the complexity of access control. Moreover, landlords need certain oversight capabilities for safety reasons but should not have a full view into the home's devices, lest they infringe on the residents' privacy. Research indicates that decision-making within the household often falls to those with greater technical proficiency.[8]

As the complexity of the smart home ecosystem grows, so does the challenge of creating these permissions efficiently and securely (we discuss the challenges of maintaining appropriate access control in the Operate phase).

Open research questions:

- How can appropriate access control be implemented with limited (or no) human interaction?
- How should access control policies be implemented if smart devices do not include multiple levels of permissions (e.g., the device only allows or denies access, but does not grant varying levels of rights)?
- How to cater for cases where a user sometimes needs elevated rights, but not other times?
- What if the person who controls the permissions for existing devices refuses or is unable to cooperate with resident's intentions for the new device?

Update and Patch

When a smart device is integrated into a smart home, it may require an immediate update or patch to operate securely, especially if it has been sitting on a store shelf or in a warehouse for an extended period.

Open research questions:

- How can new devices be automatically brought up to current update or patch levels?
- What if an update breaks functionality with another device that expects the new device to run a lower software version? Is there a path to restoring operation?
- What if a vendor goes out of business between when a device is manufactured and when it is installed?

Ensure Safety

Smart-home devices may impact resident safety; we consider safety concerns to be an integrity issue. During deployment, safety concerns require the proper configuration of safety-sensitive components such as actuators that control physical aspects of the home like door locks, fire alarms, or window blinds. The initial installation must ensure that these devices are not only physically secure but also hardened against digital vulnerabilities that could allow unauthorized access. A compromise of these systems could potentially lead to physical harm (e.g., if a door is unlocked by a person with ill intent) or reputational harm (e.g., a window blind exposes a resident while they are undressing).

Open research questions:

- How can safety-sensitive deployments be recognized?
- How to prevent untrained residents from making mistakes deploying safety-sensitive devices?
- How can safety-sensitive deployments avoid conflicting or improper configurations or policies?

Availability

In the Deploy phase of smart home devices, focusing on availability is crucial to ensure that all devices are correctly configured and ready to function reliably from the outset, providing consistent access for residents.

Manage Scale

As the number of devices in a smart home increases, the complexity of deploying these devices also escalates. Creating these connections is not trivial, particularly in situations where a device may need to communicate with many other devices. This complexity arises from the need to ensure compatibility, manage network traffic, and maintain security across all connections. If these connections are not made at the deploy stage, the device may not be available, or may be available with decreased utility.

Another challenge with scale is that residents may not be familiar with the wide variety of devices from multiple vendors potentially present and may not be able to ensure secure setup is completed. For example, even for a single type of device—such as a light bulb—a single home may have bulbs from different vendors and tied to different lighting platforms. Despite their common functionality (lighting), they may need distinct companion apps or web interfaces—each with its own look and feel, as shown in Figure 2.

Open research questions:

- How can an unskilled resident make a new device available?
- How to deploy a new smart device that is required to communicate with another device, but that other device is unavailable at the time of deployment?
- With a large number of devices in a home, how does the resident know which device(s) to which the new device should connect?

Accommodate Device Heterogeneity

During deployment, device availability can be limited by lack of compatibility between devices from different manufacturers. Consumers frequently find that no single vendor offers a complete solution that meets all their needs. Consequently, homeowners may need to combine solutions from different vendors, creating a subsystem within their broader smart-home system. This approach requires navigating and integrating multiple communication standards and protocols, making the system both complex and potentially less reliable. For example, an Amazon motion detector might not connect with a smart bulb from a lesser known brand if they do not use compatible communication protocols.

This situation restricts consumer choice and can lead to increased costs and limited functionality, as users may have to forego features available in other devices because they are not compatible with their existing system, or purchase a more expensive device that is compatible. In short, this lack of interoperability reduces the overall availability of smart-home functions.

Open research questions:

- How can devices from multiple vendors be integrated?
- How to cater for legacy devices while considering security and privacy?

Operate Phase

The operation of a smart home involves the day-to-day use of installed smart devices. The goal of the Operate phase is to keep all devices executing as intended while dealing with changes from the deployment of new devices or decommissioning of existing devices. As in the deployment phase, we align the challenges with the CIA triad.

Confidentiality

In the Operate phase of smart home systems, we focus on maintaining confidentiality over time. We assume confidentiality was established during the Deploy phase when the device became part of the home's infrastructure.

Prevent Privacy Inferences

As the number of devices in a home grows, it raises the possibility of inferring increasingly fine-grained details about the home's residents. Some devices collect, log, analyze, and share sensitive data, including environmental sensor data like temperature, motion,

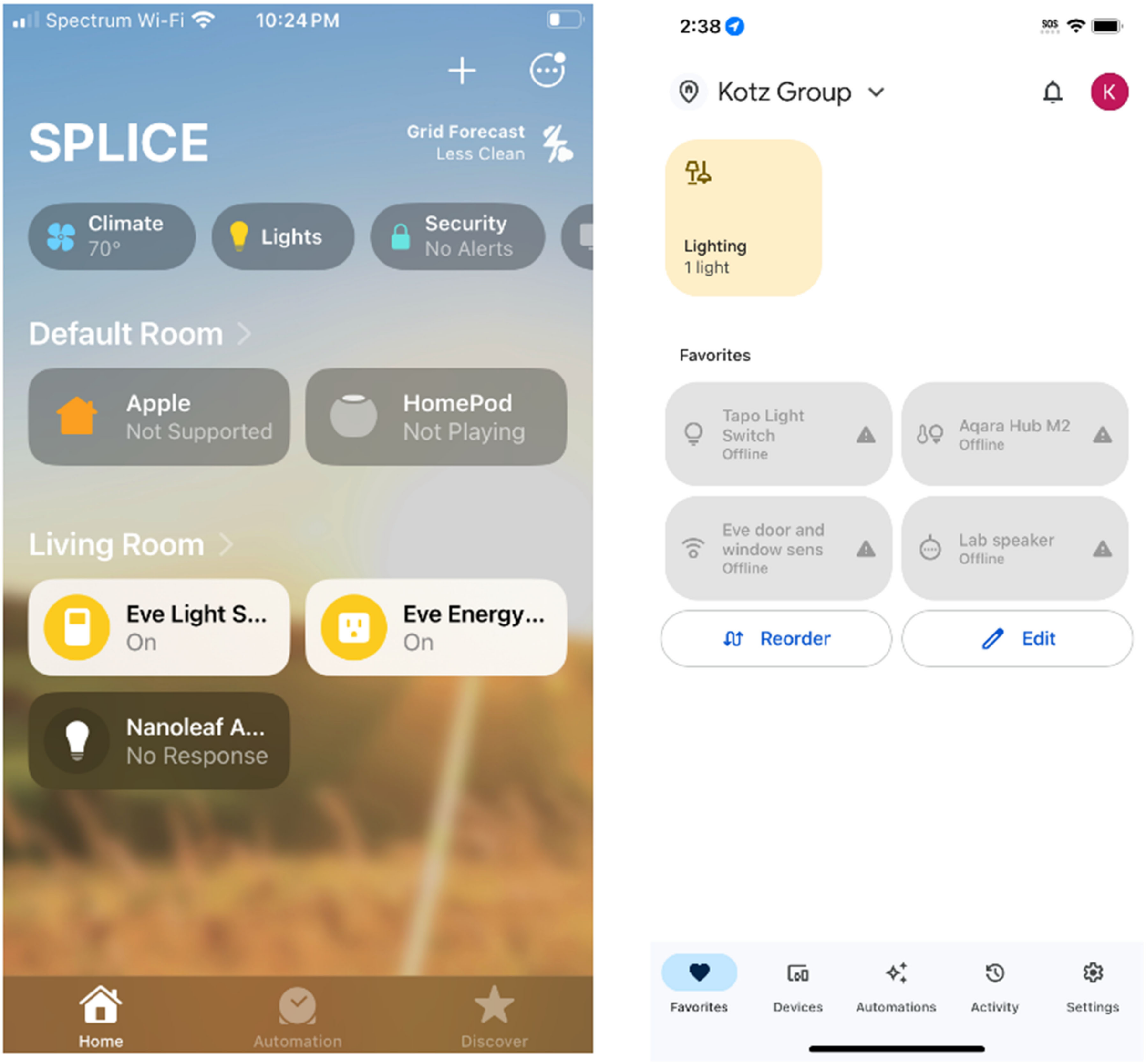


FIGURE 2. Home screen of popular ecosystems—Apple (L), Google(R). Note there are differences such as Apple allowing the addition of new devices from the home screen whereas users must go to a different screen in the Google Home app to add a new device.

and voice recordings, or device-usage patterns such as washing machine cycles, furnace operation, and water consumption. Each device in a smart home may collect a small amount of data about a resident, but in aggregate, that information can reveal a great deal about the resident's habits and preferences.

The data collected by smart devices also raises concerns about what happens to the data; is it stored locally or in the cloud? Who has access to the data and for how long? Not only is stored data a cause for concern, but data in transit can also pose security and privacy risks. Recent work has shown that many smart devices transmit data using plain-text HTTP,[9] which is an issue that should be addressed during device development but which may impose risks during device operation. Moreover, even if the data are encrypted, adversaries can sometimes deduce sensitive information. Liu et al. demonstrated that an eavesdropper can determine when residents are watching TV or getting dressed—despite the video traffic being encrypted.[10] While there has been some research[11] that attempts to solve privacy violations, less-complex methods are needed for nontechnical users.

Open research questions:

- How can the system monitor device communications for unencrypted communications?
- How can confidentiality be maintained as devices are updated?
- How can inference attacks be mitigated?
- How can data be protected after it leaves the home? How do we know a vendor's cloud service can be trusted with confidential data?
- How can residents navigate privacy concerns in an effective manner, even for data stored and processed in the cloud?

Integrity

In the Operate phase of smart-home systems, upholding integrity is critical to ensure that all system settings and device functionalities are correctly maintained and unaltered by unauthorized changes, preserving the system's reliability and trustworthiness.

Update Access Control

As devices are deployed into the home, are updated, or are decommissioned, home devices (and the network) may need access-control updates. In a home with many devices, removing one device may cause unexpected consequences as failures caused by the device removal cascade around the home. For example, if a hub is replaced, all connected devices that rely on this hub for communication and automation will need to be reconfigured to integrate with the new hub.

Separately, when parents allow their children access to streaming services but restrict access to thermostat settings, managing these permissions is straightforward. However, these settings must dynamically adapt over time, reflecting changes in residents' status or needs. For example, consider a scenario where a family member is granted temporary access to control smart locks while house-sitting. If their access is not properly revoked afterward, it could unintentionally leave the home vulnerable. Maintaining these changes without disrupting the system's integrity or introducing vulnerabilities is a complex task, particularly at scale, where small errors in configuration could propagate widely, affecting the system's functionality and security.

Open research questions:

- When a new device is deployed, how can relevant existing home devices be identified and updated for the new device?
- When a device is decommissioned, how can other devices update their access control? How can problems caused by the decommissioning be identified and rectified?
- How can access-control policies adapt to changing resident needs, such as a child becoming a trusted adult or a former spouse becoming untrusted?

Availability

In the Operate phase of smart home systems, availability is about ensuring all devices and their functionalities remain accessible and operational when needed.

Repair

Devices sometimes simply stop functioning. At times a simple reboot brings the device back online in a fully operational state. Other times more drastic action is required to restore availability.

Keeping all devices operational at all times is a difficult task. Suppose a home has 100 smart devices and each device fails once per year on average. In this scenario, a device must be repaired roughly every 3.6 days. Some devices are likely to fail more frequently, requiring more attention.

In environments where consumers may possess hundreds of smart devices, a key question arises: is continuous awareness of each device's status necessary, and if so, how can this be achieved without overwhelming the user? Attention management is critical to any effective solution. This leads to the necessity of developing attention management strategies to avoid cognitive overload caused by excessive alerts. Simplified monitoring solutions are needed to allow users to comprehend the overall state of their home environment at a glance. Furthermore, determining which residents should receive notifications about changes or issues presents an additional layer of complexity, particularly as the scale and diversity of smart devices increase. These aspects underline the importance of designing scalable, user-centric systems that can adapt to the expanding landscape of smart home technology.

In addition, given that the majority of smart devices are network-connected, they inherently consume bandwidth on the home network. This consumption can degrade the overall network experience for residents, particularly as the number of devices grows. Since many IoT devices rely on Wi-Fi and often operate on the same frequency band, they can interfere with each other, leading to diminished performance.

Furthermore, misconfigured devices may use excessive network resources. It is crucial for future home network infrastructures to include mechanisms that ensure high Quality of Service (QoS) for residents, or at least assist in diagnosing the cause of poor performance.

Open research questions:

- How can device failures across heterogeneous systems be detected?
- How can failures be addressed with minimal (or no) human interaction?
- How much do humans need to be aware about every failure? Does every resident need to know about every failure? What about the failure of a roommate's device?
- How can humans understand the status of their network without being overwhelmed?
- How can QoS be achieved as smart devices are deployed and decommissioned?

Handle Mobile Devices

Mobile smart home devices may leave the home. The absence of those devices from the home may create availability problems for other devices and residents.

Furthermore, changes to the home's infrastructure may arise while a mobile device is away. Ideally the device would "catch up" to the home status and configuration when it returns.

Open research questions:

- How can a mobile device catch up to the home's current status if the home's configuration changes while it is away? or, if new devices are deployed, and others decommissioned, when it is away?
- How can a mobile device determine if it should establish a connection with a device that was installed while the mobile device was away? What process would it use to establish a secure connection with the new device?
- What if a mobile depends on another home device, but the home device is decommissioned while the mobile device is away?

3) Decommission Phase

Decommissioning represents the final phase in our proposed framework for the life cycle of smart devices within a smart home. This phase marks the end of a device's active use within that environment. This stage involves the responsible disposal or transfer of ownership of the smart devices, ensuring that all sensitive data stored on the devices is securely deleted to prevent potential data breaches. While decommissioning is linked to security and privacy, ensuring data integrity and preventing unauthorized access, we treat it as a distinct phase to emphasize its importance. This separation also helps to clarify the chronological progression of a device's life cycle within our framework.

Once a device has been decommissioned and it is no longer part of the home's infrastructure, integrity, and availability are no longer considerations. Confidentiality, however, is still an issue that must be handled carefully.

Confidentiality

Removing sensitive data (such as personal preferences, sensor data, cloud credentials, or cryptographic keys) from the device before ownership transfer or disposal is important to prevent exposure of personal information.

Remove all Sensitive Information

Previous studies have demonstrated the potential for extracting sensitive information left on pre-owned smart devices when they are sold or discarded.[12] Similarly, a discarded device may remain connected to its owner's home network or cloud accounts. Consequently, residents of smart homes require a reliable method to guarantee that devices no longer in use do not become a security or privacy risk.

Open research questions:

- How can "sensitive information" be defined and identified?
- How can a resident trust the sensitive data were deleted (and not just claimed to be deleted?)
- What if a resident forgets to remove data? Can a device determine when to erase itself?

Transfer Ownership

For some devices, the final stage of that device's association with a home occurs when that device is transferred (sold or gifted) to a new owner. There may be situations where the primary owner of the device leaves the home but wishes to leave the device for use by remaining residents, or sells the device to a new owner who then removes the device to their own home. The challenge then becomes how to effectively erase sensitive data from the device while ensuring its continued operation for new users. Sometimes, the configuration and accumulated experiences of the device can significantly enhance its value and may even be the primary reason for acquisition by the new owner. For example, consider a environmental-control system that learns over time about the way the home responds to seasonal weather patterns, optimizing energy use... but also learns over time about the residents' behaviors, optimizing the internal environment to their needs and preferences. Models of the home's reaction to weather and seasonal patterns is worth retaining, while models of resident behavior may be considered sensitive personal information. In such cases, the challenge is to retain useful information for use by the new owner while effectively erasing any sensitive data.

Open research questions:

- How can "sensitive" information be defined and identified?
- In a situation where one resident leaves the home, but the device continues in service to remaining residents, how can sensitive data from one resident be removed while data from other residents is retained?
- How can we assure residents that sensitive data have been deleted?

EVALUATING COMMON PLATFORMS

Major manufacturers such as Amazon, Apple, Google, and Samsung have created platforms for managing home devices. In this article, we focus on the two largest market leaders, Apple and Google.[14] We discuss each of these platforms and evaluate them using our framework. While these platforms continue to evolve,[a] we found notable shortcomings at nearly every stage of the smart device life cycle. Neither platform provides a comprehensive management solution, but Apple HomeKit has more desirable features and fewer concerns than Google Home.

Apple HomeKit: Limited Variety of Devices

Apple's HomeKit is designed to be a platform for managing multiple types of devices throughout the smart-device life cycle. HomeKit attempts to provide a unified interface for all types of devices. Rather relying on separate setup applications for each type of device, a smart-home resident can use the same HomeKit interface (the "Home" app on iOS) for each of their varied smart devices.

Apple employs a stringent certification protocol known as the made for iPhone/iPad (MFi) certification. This program ensures that all devices integrated into the HomeKit ecosystem meet Apple's standards for security and functionality. The MFi certification is helpful for system integrity and security, but it limits the variety of devices that can be included in the HomeKit environment. This limited variety of devices is a significant drawback, because Apple and its approved partners do not sell every type of device a resident may want to deploy in their smart home.

Google Home: Less Consistent Management

Like Apple's HomeKit, Google Home is also meant to be a platform for managing many devices. In contrast, however, Google Home offers a more flexible integration approach, supporting a broader range of devices. This openness promotes user choice and system versatility. The significant downside to this approach is that it introduces variability in the reliability and security of the user experience.

Additional Issues

Both platforms struggle with the scalability of managing a large number of smart devices, especially given that most user interfaces are designed for management via smartphones with relatively small screens. Figure 3 shows how identifying devices might be challenging on a small screen. We see many devices listed, but it is unclear which icon refers to which device. This issue will become increasingly problematic as the number of smart devices in a home increases.

In addition, protocol updates by vendors can necessitate new hardware or software configurations, complicating the integration of older devices within the new framework. For instance, as shown in Figure 4, some devices that previously did not require a hub now require one after Apple upgraded its platform to conform with the Matter protocol. Although a helpful step in expanding future interoperability, this update broke functionality with every previously deployed device in our test bed.

Although basic functionality can be controlled through Google Home or Apple HomeKit, the concept of a central interface breaks down when device-specific actions are required. For example, maintenance tasks such as administering updates often require navigation through dedicated companion apps, which can vary in usability and may not always provide a seamless experience. These functions are not available via either platform's unified interface.

In Table 1, we review both Apple HomeKit and Google Home using our framework. In addition to the

[a] We tested with Apple iOS 17.3.1 and Google Home 3.10.103 in March 2024

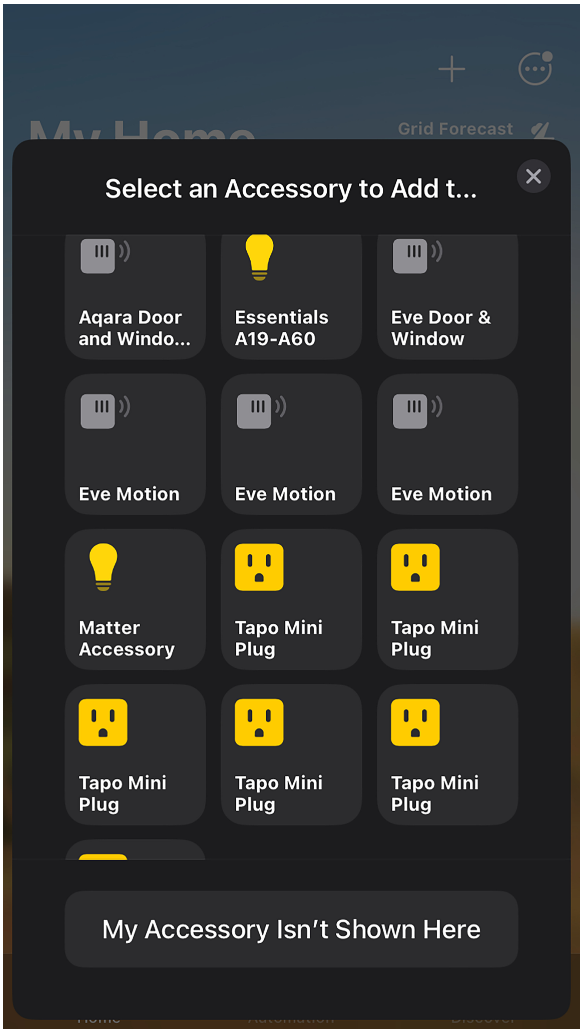
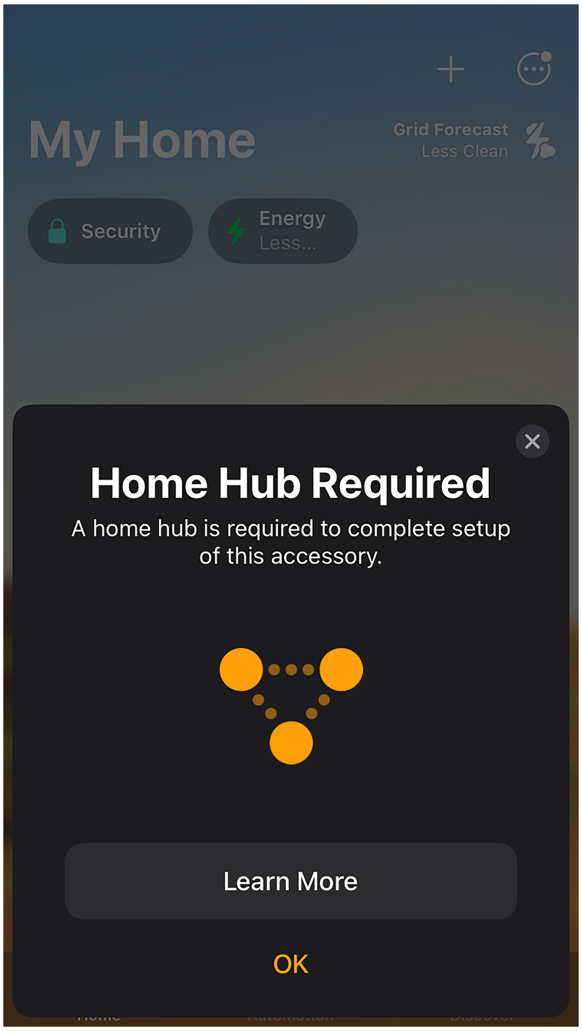


FIGURE 3. A challenge is to identify devices, especially from devices of the same kind.



Home Hub Required

A home hub is required to complete setup of this accessory.

FIGURE 4. Devices which previously did not need a hub now require one to work within the ecosystem.

comments above, we see these platforms have several issues. Among other concerns, they promote vendor lock-in[15] (limiting consumer choice) and collect usage statistics[16] (impinging on consumer privacy). Additional shortcomings also include complexity with the user interface. While Apple HomeKit and Google Home can be easy to use, that simplicity comes at a cost of accessing advanced features and thus there lies a challenge in creating a user-friendly interface that does not compromise on offering advanced features.

HOMECUBE SOLUTION

We propose a solution that extends the router's functionality through a conceptual device we dub the *HomeCube*. We envision the HomeCube as a small device that supplants the Wi-Fi router—performing the router's duty as an access point and Internet gateway—but also serves as a central hub for smart-home networks. We envision it being extensible, to accommodate additional hardware and software components. While other researchers[17] have recognized the need for a comprehensive smart-home management solution, their efforts often do not sufficiently address the needs of nontechnical users nor effectively manage devices at scale. The HomeCube would be different from other smart-home systems such as Home Assistant,[18] because it is meant to be a single system that is integrated into the router, a device that already exists in most home networks. As such, the footprint of our proposed solution is relatively small. The router is a logical location: as the Wi-Fi access point, the

TABLE 1. Comparisons of how apple homekit and google home handle different tasks using our framework. We find issues at nearly every life cycle stage for both platforms, but apple has more desirable features.

	CIA Triad	Task	Google Home	Apple HomeKit
Deploy	Confidentiality	Discover new devices	**Difficult since devices may use different commissioning mechanisms**	Apple MFi certification simplifies discovering and commissioning new devices
		Manage credentials	**Users need to manage their own credentials**	Simplified with Apple Keychain
		Manage different protocols	**Difficult to manage due to varied ecosystem**	MFi certification makes interoperability easier
	Integrity	Establish access control	Some controls are in place	Highly controlled via HomeKit framework
	Availability	Manage scale	**Difficult as number of devices increases**	**Difficult as number of devices increases**
		Accommodate device heterogeneity	**Difficult to manage due to diverse ecosystem**	**Only certified devices permitted**
Operate	Confidentiality	Prevent privacy interference	**Some integrations may not encrypt data[9]; collects usage statistics[13]**	Data might be encrypted but still susceptible to inference attacks
	Integrity	Update access control	**Controlled through app updates**	Managed via system updates
		Patch/upgrade	**Not supported, might have to use companion application to administer updates**	**Not supported, might have to use companion application to administer updates**
	Availability	Repair	**Support varies by device**	Standardized support through AppleCare
Decommission	Confidentiality	Remove sensitive information	**Manual process required**	Automated removal through settings

router is ideally suited to monitor communications within the home. As the gateway to the Internet, the router is able to monitor communications with the broader Internet. It thus provides a practical location to incorporate new security and privacy mechanisms. As a result, the smart home (and its smart things) do not need to rely on other computing devices—such as mobile phones that may not be present in the home when needed. Instead of creating a new account and downloading a new app for every new smart device, the HomeCube can use a single-sign-on approach and streamline the integration of smart devices into the smart home. The HomeCube can manage the necessary device-specific protocols behind the scenes. In addition, by emulating native apps but presenting a single interface to the user, HomeCube could manage device-specific protocols behind the scenes, such as those needed for TP-Link or Philips Hue devices, allowing users to enjoy a seamless experience without directly engaging with each device's native application.

The HomeCube can assist home residents to remain aware of the status of hundreds of smart devices in the home, without overwhelming them with alerts, by supporting an intelligent notification system that factors in urgency and relevance.

Visiting devices and visitors present an additional layer of complexity and potential vulnerability. We suggest the use of VLANs or firewall-like filters specifically tailored for guest devices. This sandboxing of visiting devices would allow them to connect to the Internet and to limited home functions without compromising the core network's integrity or accessing the primary residents' personal data and devices. By employing such measures, the HomeCube could offer dynamic, function-based, and ownership-aware network segmentation, significantly enhancing the smart home's resilience against privacy breaches and security threats. This tailored approach ensures that both resident and guest devices operate within a secure and controlled smart-home.

The HomeCube enables devices to discover and communicate with each other. It maintains an inventory of devices, and can detect the arrival (or disappearance) of devices in the home and distinguish them from unrelated devices in neighboring homes. It is designed to act as a bridge between different protocols, enforcing an open protocol throughout the home. This means if one product communicates using a proprietary protocol, and needs to interact with another product, which operates using a second protocol, the HomeCube can bridge the gap between the two. In some cases the HomeCube may need multiple network interfaces to facilitate this interoperability, such as Zigbee, Ethernet, and Wi-Fi. The HomeCube is designed to integrate higher layer protocols, facilitating communication across different application-layer protocols. Beyond simply bridging connectivity standards such as Zigbee, Bluetooth, and Wi-Fi, the HomeCube delves into the more complex task of translating between different application-layer protocols. This type of bridge includes converting messages and commands across platforms like MQTT for IoT messaging, and proprietary protocols used by various smart devices. By doing so, the HomeCube ensures interoperability and efficient communication within the smart-home ecosystem, enabling devices with differing native protocols to understand and interact with each other effectively, similar to the bridging capabilities of the Matter protocol.[6] This capability would also assist in ensuring legacy devices remain operational.

We foresee Artificial Intelligence (AI) playing a pivotal role in smart-home management. In response, we propose the HomeCube as a platform to facilitate AI applications, including resource provisioning and responding to configuration changes. For instance, when guests arrive, homeowners may face challenges such as configuring firewall rules or troubleshooting connectivity issues. An intelligent agent within the HomeCube could assist by learning users preferences so that minimal user intervention is needed when managing devices at scale.

SUMMARY

In this article, we examine the challenges associated with smart devices as they are used within a smart home, structured around three main device life-cycle phases: deploy, operate, and decommission. At each stage, we discuss the CIA triad and its specific implications for smart-home devices. We also highlight research challenges for each stage. Next we evaluate the smart-home management solutions from Apple and Google. Although their platforms continue to evolve, we saw distinct shortcomings in their offerings at the time of our review. Finally, we sketch a solution we call the “HomeCube” that may be able to help.

ACKNOWLEDGMENTS

This research results from the SPLICE research program, supported in part by the collaborative award from the SaTC Frontiers Program at the National Science Foundation under Grant CNS-1955805, Grant CNS-1955172, Grant CNS-1955228, Grant CNS-1955231, and in part by the VeChain Foundation.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors. Any mention of specific companies or products does not imply any endorsement by the authors, by their employers, or by the sponsors.

REFERENCES

1. D. Kotz and T. Peters, “Challenges to ensuring human safety throughout the life-cycle of smart environments,” in *Proc. Workshop Internet Safe Things*, 2017, pp. 1–7.
2. Q. Covert, D. Steinhagen, M. Francis, and K. Streff, “Towards a triad for data privacy,” in *Proc. Hawaii Int. Conf. Syst. Sci.*, pp. 4379–4387, 2020.
3. S. Mohanty, M. Ganguly, and P. K. Pattnaik, “CIA triad for achieving accountability in cloud computing environment,” *Int. J. Comput. Sci. Mobile Appl.*, vol. 6, no. 3, pp. 38–43, 2018.
4. M. Khanafer et al., “Device discovery in the smart home environment,” in *Proc. IEEE/ACM Workshop Internet Safe Things*, 2024.
5. Q. Wang, P. Datta, W. Yang, S. Liu, A. Bates, and C. A. Gunter, “Charting the attack surface of trigger-action IoT platforms,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, 2019, pp. 1439–1453, doi: 10.1145/3319535.3345662.
6. Connectivity Standards Alliance, “Matter specifications,” Accessed: Jun. 13, 2024. [Online]. Available: https://csa-iot.org/developer-resource/specifications-download-request/
7. IBM, “Subjects and objects,” Accessed: Feb. 9, 2024. [Online]. Available: https://www.ibm.com/docs/en/zos/2.4.0?topic=controls-subjects-objects

8. A. S. Schulz, "User interactions with Internet of Things (IoT) devices in shared domestic spaces," in *Proc. Int. Conf. Mobile Ubiquitous Multimedia*, 2023, pp. 583–585.
9. A. Girish et al., "In the room where it happens: Characterizing local communication and threats in smart homes," in *Proc. Internet Meas. Conf.*, 2023, pp. 437–456.
10. X. Liu, J. Wang, Y. Yang, Z. Cao, G. Xiong, and W. Xia, "Inferring behaviors via encrypted video surveillance traffic by machine learning," in *Proc. Int. Conf. High Perform. Comput. Commun./ Int. Conf. Smart City/ Int. Conf. Data Sci. Syst.*, 2019, pp. 273–280.
11. C. Stach, C. Gritti, and B. Mitschang, "Bringing privacy control back to citizens: DISPEL–A distributed privacy management platform for the Internet of Things," in *Proc. Symp. Appl. Comput.*, 2020, pp. 1272–1279.
12. R. Roberts, J. Poveda, R. Roberts, and D. Levin, "Blue is the new black (market): Privacy leaks and re-victimization from police-auctioned cellphones," in *Proc. Symp. Secur. Privacy*, 2023, pp. 3332–3346.
13. S. Youn, "Google workers can listen to your Google assistant recordings, company acknowledges," Accessed: Jun. 13, 2024. [Online]. Available: https://abcnews.go.com/Business/google-workers-listen-google-assistant-recordings-company-acknowledges/story?id=64291108
14. KBV Research, "Global smart home platforms market size, share & industry trends analysis report by deployment type (on-premise and cloud), by product, by type, by regional outlook and forecast, 2022–2028," Accessed: Jun. 13, 2020. [Online]. Available: https://www.kbvresearch.com/smart-home-platforms-market/
15. A. van der Zeeuw, A. J. van Deursen, and G. Jansen, "The orchestrated digital inequalities of the IoT: How vendor lock-in hinders and playfulness creates IoT benefits in every life," *New Media Soc.*, vol. 1, Nov. 2022, Art. no. 146144482211380.
16. S. Kim, M. Park, S. Lee, and J. Kim, "Smart home forensics–data analysis of IoT devices," *Electronics*, vol. 9, no. 8, 2020, Art. no. 1215.
17. A. C. F. da Silva, P. Hirmer, J. Schneider, S. Ulusal, and M. T. Frigo, "MBP: Not just an IoT platform," in *Proc. Int. Conf. Pervasive Comput. Commun. Workshops*, 2020, pp. 1–3.
18. Home Assistant, "Home assistant." Accessed on: Feb. 09, 2024. [Online]. Available: https://www.home-assistant.io

RAVINDRA MANGAR is currently working toward the Ph.D. degree in computer science at Dartmouth College, Hanover, NH, 03755, USA. His research interests include computer networks and wireless network security. He is the corresponding author of this article. Contact him at ravindra.r.mangar.gr@dartmouth.edu.

TIMOTHY J. PIERSON is a research assistant professor at Dartmouth College, Hanover, NH, 03755, USA. His research interests include privacy and security, the Internet of Things, and applied machine learning. Pierson received his Ph.D. degree from Dartmouth College. He is a member of IEEE. Contact him at timothy.j.pierson@dartmouth.edu.

DAVID KOTZ is the provost and the Pat and John Rosenwald Professor at Dartmouth College, Hanover, NH, 03755, USA. His current research involves security and privacy in smart homes and wireless networks. Kotz received his Ph.D. degree in computer science from Duke University. He is a fellow of the Association for Computing Machinery, a fellow of IEEE, and a 2008 Fulbright fellow to India. Contact him at David.F.Kotz@dartmouth.edu.