UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Aleksandra Sergeeva

Comprehensive survey of smart home technologies

Bachelor's Thesis (9 ECTS)

Supervisor: Chinmaya Kumar Dehury, PhD

Tartu 2024

Comprehensive survey of smart home technologies

Abstract: Smart home technologies integrate advanced computational and networking capabilities into everyday household environments, enhancing convenience, security, and energy management. These systems utilize a variety of communication protocols and platforms, ranging from proprietary systems developed by major tech companies to open-source solutions created by global communities. This study addresses the need for a thorough understanding of the current landscape and capabilities of various smart home platforms, which are critical in the transition towards more intelligent living environments. A detailed comparative analysis of twelve major smart home platforms is shown in this thesis. While many systems offer robust solutions, there is considerable variation in their adaptability, security features, and ease of use, which were previously underappreciated in the literature. This thesis enhances our understanding of how different platforms can cater to diverse user needs and technical requirements, challenging the one-size-fits-all approach often assumed in smart home technology. By mapping out the strengths and limitations of each system, this research contributes to a more nuanced view of smart home technology as a complex yet promising field. The insights gained here provide a foundation for consumers, developers, and researchers to make informed decisions about smart home technologies, fostering smarter, more efficient home environments. This broader perspective highlights the significance of customized technological solutions in striking a balance between user-focused design and technological evolution, which will be useful for developing other groundbreaking concepts in the smart home industry.

Keywords:
Smart home, Internet of Things, Zigbee, Wi-Fi, Bluetooth, Z-wave

CERCS: P170 Computer science, numerical analysis, systems, control

Nutika kodu tehnoloogiate põhjalik uuring

Lühikokkuvõte:

Nutikate kodutehnoloogiate integreerimine võimaldab lisada igapäevasesse kodukeskkonda edasijõudnud arvutus- ja võrguvõimalused, suurendades mugavust, turvalisust ja energiahaldust. Need süsteemid kasutavad mitmesuguseid suhtlusprotokolle ja platvorme, ulatudes suurte tehnoloogiaettevõtete poolt välja töötatud omandilistest süsteemidest kuni globaalsete kogukondade poolt loodud avatud lähtekoodiga lahendusteni. Käesolev uurimus käsitleb vajadust põhjaliku arusaama järele praegusest maastikust ja erinevate nutikodu platvormide võimalustest, mis on kriitilised üleminekul intelligentsematele elukeskkondadele. Käesolevas doktoritöös on näidatud kaksteist peamist nutikodu platvormi põhjalikku võrdlevat analüüsi. Kuigi paljud süsteemid pakuvad tugevaid lahendusi, on nende kohandatavuses, turvaelementides ja kasutusmugavuses märkimisväärseid erinevusi, mida varem kirjanduses ei hinnatud piisavalt. See doktoritöö parandab meie mõistmist sellest, kuidas erinevad platvormid suudavad rahuldada erinevate kasutajate vajadusi ja tehnilisi nõudeid, seades kahtluse alla üks-suurus-sobib-kõigile lähenemise, mida nutikodu tehnoloogias tihti eeldatakse. Iga süsteemi tugevuste ja piirangute kaardistamisega aitab see uurimus kaasa nutikodu tehnoloogia keerukama ja paljulubava valdkonna peenemalt nüansseeritud vaatele. Siit saadud teadmised loovad tarbijatele, arendajatele ja uurijatele aluse informeeritud otsuste tegemiseks nutikodu tehnoloogiate osas, soodustades nutikamaid ja efektiivsemaid kodukeskkondi. See laiem vaatenurk rõhutab kohandatud tehnoloogiliste lahenduste tähtsust tasakaalu saavutamisel kasutajakeskse disaini ja tehnoloogilise arengu vahel, mis on kasulik ka teiste murranguliste kontseptsioonide arendamisel nutikodu tööstuses.

Võtmesõnad:
Nutikas kodu, Internet of Things (IoT), Zigbee, Wi-Fi, Bluetooth, Z-wave

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

Contents

1 Introduction

Living in a fast-paced era of technology, smart homes present a lifestyle where technology is effortlessly incorporated, increasing levels of comfort, convenience, safety, and energy efficiency. This thesis explores 12 smart home platforms, including both open-source (openHAB, Domoticz, Calaos, OpenMotics(Renson), HomeGenie, and Home Assistant) and proprietary systems (Amazon Alexa, Google Nest, Apple HomeKit, Samsung SmartThings, Control4, and Wink), to provide an in-depth look at their current state and potential. These platforms transform households into interconnected, intelligent environments by automating functions like lighting, heating, and security optimized for user comfort and efficiency. The analysis in this thesis aims to unravel the complex ecosystem of these platforms, investigating their architectures, functionalities, user interfaces, and integration capabilities with other smart devices. The thesis is driven by the need to provide a nuanced view of how these platforms can be optimized to meet users' varying needs, focusing on their adaptability, security features, and ease of use. The smart home market is the fastest-growing global market, with significant potential for growth; its forecasted revenue is going to be $154.4 billion by 2024, although the penetration rate will be only 18.9%, and the annual growth rate will still be 10.67%, leading to a market volume of $231.6 billion by 2028. [1]. By providing an in-depth comparison and evaluation of these diverse systems, the research seeks to guide potential users and developers in making informed decisions that could shape the future landscape of smart home technologies. When writing the thesis, chatGPT's text robot assistance was used to receive feedback on the content of the work, the structuring of chapter outlines, and the correctness of language usage in the main text of the chapters. Based on the received feedback, the text of the work has been refined, and language errors have been corrected [2].

1.1 Motivation

The scholarly impetus of this thesis lies in the recognition of smart homes as the pivotal frontier of the integration of technologies where a diversity of devices and platforms converge to model modern living experiences. As the smart home solutions market grows, consumers are facing many options, which therefore require that one has a general understanding of the available technologies in the evaluation that is likely to aid the consumer in making informed decisions.

1.2 Goal

The main goal of the thesis is a complex analysis of the multi-element system, which forms the foundation of smart homes. This involves a systematic investigation of communication networks and platforms to elucidate the complexities inherent in this dynamic landscape. By elucidating the complexities of smart home technologies, the aim is to equip readers with the knowledge and tools necessary to navigate the diverse array of solutions and create personalized smart home ecosystems that align with their individual preferences and requirements.

1.3 Contributions

This thesis makes several critical contributions to the understanding and development of smart home technologies:

- Comprehensive Analysis of Leading Platforms: It evaluates 12 major platforms, including Apple HomeKit and Samsung SmartThings, through practical engagement. This analysis assesses their integration capabilities, user interface, automation features, and, importantly, their security and privacy measures. This holistic approach provides a deeper understanding of each platform's strengths and potential vulnerabilities.
- Documentation Review: An extensive review of official documentation and existing research provides a solid foundation for understanding the current functionalities and limitations of the platforms studied. This aspect ensures that the analysis is based on verified and up-to-date information, allowing for a reliable comparison across different systems.
- Evaluation Framework: A structured framework is introduced for assessing smart home technologies across various metrics, including ease of use, interoperability, and security. This framework enhances the ability to systematically compare and contrast different systems, highlighting critical differences and identifying leading solutions in the smart home market.

The thesis contributes to both the academic and practical discourses on the topic of smart home systems. The exposition on the existing state of research enlightened the reader on the up-to-date developments and stimulated further efforts in the field.

1.4 Thesis outline

The thesis opens with the Introduction section 1, which explains the importance of smart home technologies for residential life and their future potential for further development. The Background section 2 provides a comprehensive foundation for the exploration of smart home technologies. The subsequent Smart Home Platforms section 3 provides a critical examination of existing platforms, comparing their traits and benefits in practical utilization. The tangents include architectural structure, user-friendliness, and the possibility of integration with other systems. The Privacy and Security section 4 focuses on data protection and system resilience to ensure user safety. The Communication Protocols section 5 examines the interoperability potential of smart house smart devices by examining the nature of protocols. The Extensibility section 6 discusses the potential of integration and scalability of future systems. Last but not least, the above mentioned sections are rounded up with a conclusion in the Conclusion section 7.

2 Background

The foundation of any exploration into smart home technologies necessitates a comprehensive understanding of its constituent elements, including definitions, devices, platforms, and avenues for comparison. This section delves into the fundamental concepts underlying smart homes and provides a succinct overview of pertinent literature.

2.1 Smart home definition

Various definitions of Smart Homes exist, exhibiting both significant overlap and instances where common ground is lacking. Moreover, related terms with partially converging or analogous meanings to Smart Homes add complexity to the conceptual landscape. To facilitate our subsequent analyses, it becomes imperative to formulate a distinct and tailored definition. In the article "Smart Home Definition and Security Threats" [3] Michael Schiefer compares definitions from several resources and concludes: *"A Smart Home device is a thing, whose main functionality is extended with networking abilities to create a new one. The additional infrastructure for those devices, like a base or control station, falls also in Smart Home."* Babakura, A., Sulaiman, M.N., Mustapha, N., and Perumal, T. define Smart Home as p*lace with heterogeneous systems to many front devices with the support of embedded information and communication architectures* [4]. Gram-Hanssen, K. and Darby, S.J. describe the Smart Home as *a home with an integration of digital sensing and communication devices to produce services through seamless communications* [5]. Analyzing all the above-mentioned definitions, a comprehensive understanding of the term "Smart Home" emerges.

In essence, a Smart Home is a dynamic and interconnected residential environment where everyday devices are imbued with networking capabilities, fostering an intelligent and automated ecosystem. The synthesis of various perspectives in these definitions enriches our understanding of the multifaceted nature of Smart Homes, paving the way for ongoing advancements and discussions in the realm of connected living spaces.

2.2 Smart home devices

The proliferation of smart home devices has transformed contemporary living spaces, introducing a diverse array of technologies designed to enhance security, entertainment, comfort, and efficiency. In this comprehensive analysis categorization of these devices based on their primary functions, elucidating their roles within the broader spectrum of connected home environments. From security-oriented systems encompassing smart lights, cameras, and video doorbells, to entertainment-centric technologies like smart speakers and home theater systems, the ensuing exploration seeks to provide an academic examination of the multifaceted landscape of smart home devices. The Table 1 provides a concise overview of various smart home solutions, categorizing them based on their primary functions. Each category is listed in a row, with the devices or solutions within that category detailed in the corresponding columns.

Table 1. Functional Categorization of Smart Home Devices

Category	**Devices**
Security devices	Smart camera (incl. baby monitors) [6], Smart lights (incl. Smart bulbs) [7], Smart doorbells [8], Smart locks [9], Smart home security systems [10], Remote controller [11], Smart home hub [12], Smart energy hub [13]
Entertainment devices	Smart lights (incl. Smart bulbs) [7], Smart speakers (incl. Voice assistant) [14], Smart TV [15], Smart soundbars [16], Remote controller [11], Video game controllers [17], Projectors [18]
Kitchen Appliances	Smart Blender [19], Smart Steamer [19], Smart Cooker [20]
Cleaning devices	Smart robot vacuum [21], Smart trash can [22]
Sport devices	Smart sport equipment [23], Training display(Tempo Studio) [24]
Devices for outdoors	Smart camera (incl. baby monitors) [6], Smart lights (incl. Smart bulbs) [7], Smart doorbells [8], Smart sprinkler [25], Smart lawn mower [26]
Other smart home devices for comfort	Smart curtains [27], Smart toilet [28], Smart water purifier [29], Smart shower [30], Smart scale [31], Smart toothbrush [32], Smart air conditioner [33], Smart air purifier [34], Smart plug [35], Smart thermostat [36], Smart bed [37], Smart mirror [38]

2.3 Smart home platforms

In the evolving landscape of smart home technologies, the choosing a suitable platform plays a pivotal role in shaping the seamless integration and functionality of connected devices. This section explores a diverse array of smart home platforms, ranging from commercial giants such as Amazon Alexa, Apple HomeKit, and Google Nest, to open-source alternatives like Home Assistant and openHAB. The platforms are categorized into commercial and open source, providing a structured overview of the options available for users seeking to build and customize their smart home ecosystems.

Table 2. List of smart home platforms

Platform	Description
openHAB	open-source platform, well-regarded among home automation enthusiasts. Its development is community-driven, with a publicly available GitHub repository [1]
Amazon Alexa	Proprietary system by Amazon, extremely popular for its voice-activated control in various smart home devices [39].
Google Nest	Proprietar platform, which is highly favored for its seamless integration with Google's ecosystem of services and devices [40].
Apple HomeKit	Apple's proprietary solution, enjoying popularity particularly among users of Apple products [41].
Domoticz	Open-source platform that attracts do-it-yourself smart home enthusiasts with its versatile capabilities and with a publicly available GitHub repository[2] [42].
Calaos	Open-source and known in niche circles for offering a comprehensive home automation suite with a publicly available GitHub repository[3] [43].
OpenMotics (Renson)	Open-source solution for both hardware and software automation, primarily targeting the European market with a publicly available GitHub repository[4] [44].
HomeGenie	Open-source platform, is noted for its customizable options in smart home automation, with its codebase available on GitHub[5] [45].
Samsung SmartThings	Proprietary system by Samsung, is renowned for its compatibility with a broad range of devices and its extensive third-party integrations [46].
Control4	Proprietary high-end custom smart home systems and is popular among those looking for sophisticated home automation solutions [47].
Wink	Proprietary platform known for its user-friendly interface and broad compatibility with smart home devices [48].
Home Assistant	Highly flexible, open-source platform popular among do-it-yourself enthusiasts for its extensive integration capabilities with its codebase available on GitHub [6] [49].

[1] https://github.com/openhab
[2] https://github.com/domoticz/domoticz
[3] https://github.com/calaos
[4] https://github.com/openmotics
[5] https://github.com/genielabs/HomeGenie
[6] https://github.com/home-assistant

2.4 Points of comparison

In this segment, we delve into essential parameters for comparing smart home devices, addressing crucial aspects such as price, technical capabilities, security features, reliability, ease of use, and compatibility. These key points of comparison aim to offer a comprehensive understanding of the economic, technical, and user-oriented considerations associated with adopting various technologies in the realm of smart homes. The Table 3 provides a comprehensive overview of key parameters for comparing smart home platforms. Each parameter is meticulously defined to facilitate informed decision-making in the selection of smart home technologies. The parameters and their descriptions are as follows:

Table 3. Evaluation Criteria for Comparative Analysis of Smart Home Platforms

Parameters	**Description**
Affordability	This parameter assesses the cost considerations associated with each smart home platform, providing insights into the economic feasibility of adopting specific technologies.
Technical advantages and disadvantages	An analysis of the technical capabilities of each device, including supported devices, communication protocols employed, and any notable advantages or disadvantages in terms of technology.
Security	This parameter evaluates the security features implemented by each smart home platform, considering factors such as data encryption, and authentication protocols.
Privacy	An examination of the privacy measures integrated into each platform, with a focus on adherence to the General Data Protection Regulation (GDPR) standards, ensuring user data is handled responsibly and transparently.
Reliability	Examination of the reliability of each device, taking into account factors such as connectivity stability, device lifespan, and performance consistency.
Ease of use/intuitive	An exploration of the user interface and overall user experience, considering the simplicity or complexity of device setup, operation, and customization.
Compatibility and Support	Investigation into the compatibility of each platform with different networks and devices, with a special emphasis on the presence of vendor lock-in, which can restrict users to specific products or services and limit interoperability within the smart home ecosystem

3 Smart Home Platforms

As we step into the era of smart homes, we look towards the diversity of smart home platforms that are going to pave the way for this digital backbone of a connected space. According to a 2023 market analysis report by MarketsandMarkets [50], Amazon, Google, and Apple hold significant shares in the global smart home market, with Amazon leading due to its extensive range of compatible devices and robust Alexa ecosystem. This section provides a comparative exploration of these leading platforms alongside others, examining their development histories, technological capabilities, and ease of use. By delving into their origins, assessing their functionalities, and evaluating their user interfaces, we aim to offer a comprehensive guide for navigating the choices in the rapidly evolving landscape of smart home technologies. This approach not only highlights the market leaders but also uncovers the roles of emerging and niche platforms in shaping the future of home automation.

3.1 openHAB

OpenHAB[1], standing for Open Home Automation Bus, has been a beacon in the open-source smart home platform domain. Its journey began in 2010 when it was conceived as a project to create a universal integration platform for various home automation technologies. Over the years, it has evolved into a robust platform with a passionate community, continuously contributing to its growth and refinement.

The Figure 1 illustrates the openHAB system architecture facilitates seamless interaction and control of smart home devices. Users interact via the openHAB App or through voice commands, with the app providing audible and visual feedback. Commands are sent to the openHAB Device, which transmits data to the openHAB Cloud for processing. The cloud syncs settings and data, and processes commands, sending actionable responses back to the device. openHAB Services handle API calls and data responses, interfacing with external APIs to extend functionality. This integrated architecture ensures real-time feedback and robust control, enhancing the user experience in managing their smart home environment.

3.1.1 Affordability

OpenHAB is an affordable, open-source smart home solution that avoids licensing fees. It supports low-cost hardware such as the Raspberry Pi and is compatible with economical smart devices like Philips Hue and TP-Link, facilitating the creation of a cost-effective smart home.

[1] `https://www.openhab.org/`

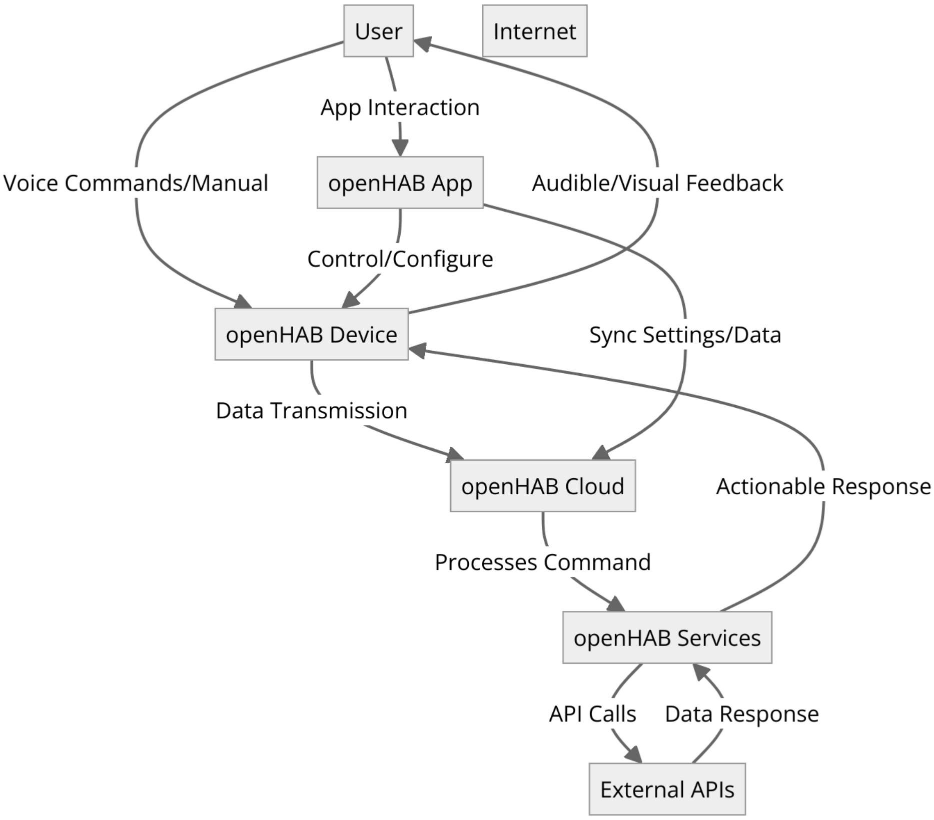

Figure 1. openHAB system architecture

3.1.2 Technical advantages and disadvantages

Advantages: OpenHAB's technical strengths stem from its open-source nature, affordability through compatibility with cost-effective hardware like Raspberry Pi, and support for a wide array of devices and protocols such as Zigbee, Z-Wave, and MQTT. This setup not only allows for significant customization but also enhances interoperability, which helps prevent vendor lock-in and promotes a diverse device ecosystem. The platform's community-driven approach offers strong support and collaborative opportunities for enhancements.

Disadvantages: The configuration of OpenHAB demands a high level of technical skill, which might discourage beginners. Security updates rely heavily on the user community, introducing risks if not regularly updated. Additionally, the system's reliability may vary with user configuration and hardware choices, sometimes leading to inconsistent performance. These issues highlight the need for careful setup and technical acumen for optimal operation.

3.1.3 Security

OpenHAB allows significant user control over security settings due to its self-hosted, open-source nature. It supports robust encryption and authentication protocols, safeguarding device communication and enhancing system integrity against unauthorized access.

3.1.4 Privacy

OpenHAB's platform enables users to extensively customize privacy settings, providing enhanced control over personal data management within a secure environment.

3.1.5 Reliability

System stability and device longevity depend on user-configured setups and hardware quality, supported by a proactive community for troubleshooting.

3.1.6 Ease of use/intuitive

Despite its steep learning curve due to high configurability, OpenHAB offers excellent device discoverability and integrates seamlessly with various smart home technologies like Z-Wave, Zigbee, and MQTT. Adding new devices can sometimes require manual configuration, especially for devices that are not natively supported. However, there are often community-contributed plugins and guides available to assist with integration. Removing devices typically involves removing them from the configuration files or interface, which can be straightforward once you're familiar with the system.

3.1.7 Compatibility and Support

Supports an expansive range of devices and protocols which aids in maintaining interoperability and vendor independence, with community forums available for additional user support.

3.2 Amazon Alexa

Amazon Alexa[2] is a proprietary system by Amazon, extremely popular for its voice-activated control in various smart home devices. It boasts extensive compatibility with a wide range of devices, making it a central hub for many users seeking hands-free control and automation in their smart homes.

The Figure 2 showcases the architecture of the Amazon Alexa ecosystem, emphasizing how user interactions are managed and processed. Users interact with the system via

[2] developer.amazon.com/alexa

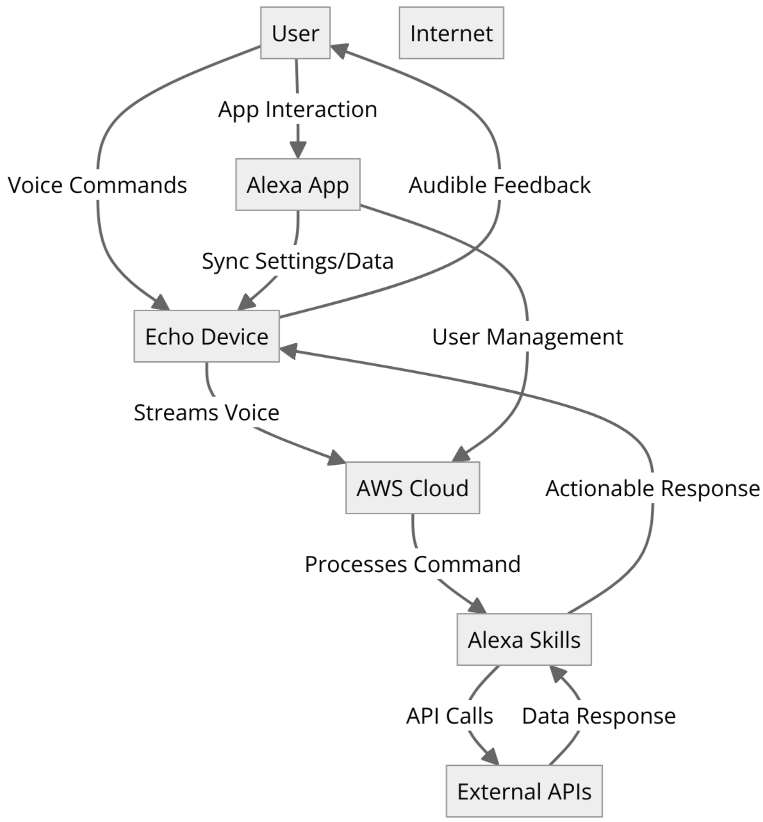

Figure 2. Amazon Alexa system architecture

the Alexa App or voice commands, with the Echo device streaming this data to the AWS Cloud. In the cloud, commands are processed, and user settings are managed, ensuring synchronization across devices. The system utilizes Alexa Skills and external APIs to enhance functionality and deliver actionable responses back to the user through the Echo device. This setup provides a seamless and efficient user experience, highlighting the integration and responsiveness of the Amazon Alexa ecosystem.

3.2.1 Affordability

Amazon Alexa devices themselves, like Echo speakers, vary in price 30$ - 300$ depending on the model and features. Basic functionality, such as controlling smart devices and using Alexa skills, is typically free. However, advanced features or services may require additional fees. Overall, Amazon Alexa devices are generally competitively priced compared to other smart home ecosystems.

3.2.2 Technical advantages and disadvantages

Advantages: Alexa's wide device compatibility and user-friendly interface simplify smart home integration, supported by Amazon's robust infrastructure and regular updates that improve functionality and security.

Disadvantages: Alexa's customization is limited compared to open-source platforms, potentially leading to vendor lock-in. Privacy issues have also been a concern despite GDPR compliance, requiring careful management of privacy settings.

3.2.3 Security

Alexa features strong security with regular updates and centralized support, though it allows limited user control over these settings. Security strengths are occasionally offset by privacy concerns, highlighting the need for careful privacy-security balance and the risk of vendor lock-in.

3.2.4 Privacy

Alexa complies with GDPR, offering tools for easy privacy management. However, Amazon's control over data and limited privacy settings require users to consider potential compromises between convenience and data control.

3.2.5 Reliability

Known for its reliability and strong connectivity, Alexa's performance is bolstered by durable Echo devices and comprehensive Amazon support.

3.2.6 Ease of use/intuitive

Alexa's intuitive interface and straightforward setup process make it highly accessible and easy to integrate into smart homes. Adding a new device to Amazon Alexa is simple through the Alexa app: just tap "Devices", then "Add Device" follow the prompts, and your device is ready. Removing a device is equally straightforward: select the device, tap "Forget" or "Remove," and confirm your choice. Alexa makes managing devices easy with its intuitive app interface.

3.2.7 Compatibility and Support

Extensive device compatibility promotes easy integration, though staying within Amazon's ecosystem might limit options. Centralized support ensures prompt issue resolution.

3.3 Google Nest

Google Nest[3] is another proprietary platform, highly favored for its seamless integration with Google's ecosystem of services and devices. Known for its user-friendly interface and robust capabilities, it provides a comprehensive solution for home automation, security, and energy management.

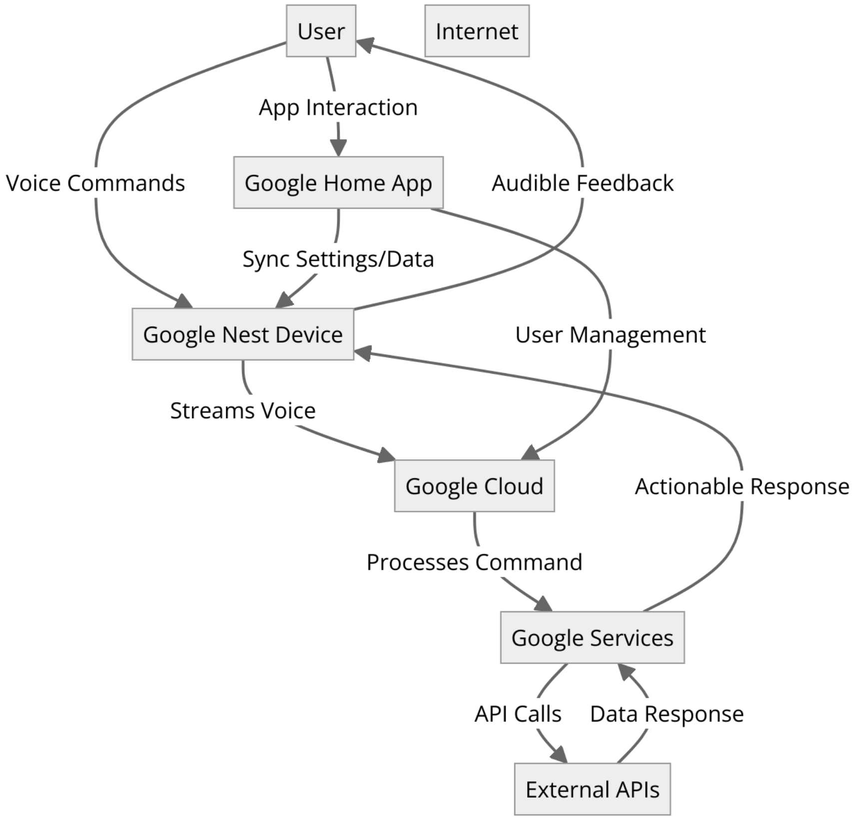

Figure 3. Google Nest system architecture

The Figure 3 offers an overview of the Google Nest architecture, clearly illustrating how the system is organized to enhance user interaction and automation within a smart home. In this setup, the user primarily interacts with the Google Home app, accessible via internet-connected devices, which allows for both app interaction and voice command inputs. These commands are directed to a Google Nest device, which is responsible for streaming voice data to the Google Cloud. The cloud processes these inputs, handles user management, and ensures security and personalization of actions across the user's devices. The system supports audible feedback, providing real-time auditory responses

[3] https://store.google.com/gb/category/connected_home?hl=en-GB

to user queries or commands, enhancing the interactivity of the Google Home ecosystem. Additionally, the architecture is integrated with Google Services and External APIs, which allow the Nest system to leverage a broader range of functionalities and connect with various smart home devices. These integrations enable the system to execute actionable responses efficiently, based on the data processed in the Google Cloud. This setup showcases the seamless integration of Google's services, providing a comprehensive and user-friendly approach to home automation.

3.3.1 Affordability

Google Nest offers various products, including thermostats, cameras, and smart speakers, each with its own price range. Additionally, Google offers subscription services like Nest Aware for video storage and advanced features, which can range from $6 to $12 per month per camera. Google Nest products tend to be on par with competitors in terms of pricing.

3.3.2 Technical advantages and disadvantages

Advantages: Nest devices are known for their seamless integration through the Google Home app, using Wi-Fi, and in some cases, Thread and Zigbee for robust local communication. This connectivity allows for a stable and reliable smart home experience, enhanced by regular updates and the robust security infrastructure of Google.

Disadvantages: Customization and device compatibility are somewhat limited as Nest promotes the use of its own ecosystem, potentially restricting interoperability with third-party devices. Privacy concerns are notable, given the extensive data integration with Google's services, which may deter users sensitive about personal data usage.

3.3.3 Security

Nest devices utilize strong security protocols backed by Google's comprehensive cyber infrastructure. Regular security updates help protect against vulnerabilities, providing users with peace of mind. However, the closed nature of the ecosystem means users have limited control over these security settings, similar to Amazon's approach with Alexa.

3.3.4 Privacy

While Nest devices comply with necessary legal standards, including GDPR, the deep integration with Google's services raises potential privacy concerns. Users have access to various tools to manage their privacy settings, but the extent of data collected by Google might be a consideration for those cautious about personal information.

3.3.5 Reliability

Google Nest products are generally reliable with strong connectivity features supported by continuous software updates and the use of advanced communication protocols like Wi-Fi, Thread, and Zigbee, ensuring minimal downtime and consistent performance.

3.3.6 Ease of use/intuitive

The Google Home app provides a user-friendly interface for all Nest devices, making setup and daily use straightforward. The integration of voice controls through Google Assistant enhances this ease, making it accessible even for those who are not tech-savvy. Adding devices to the Google Home app, which controls Google Nest devices, is generally easy, especially if the devices are compatible with Google's ecosystem. Removing devices can also be done through the app with a few simple steps.

3.3.7 Compatibility and Support

Nest's device compatibility is extensive within its own ecosystem, and while it supports some third-party integrations, it is optimized for use with other Google services. Support is centralized and generally responsive, benefiting from Google's extensive customer service resources.

3.4 Apple HomeKit

Apple HomeKit[4] is Apple's proprietary solution, enjoying popularity particularly among users of Apple products. It offers a high level of integration with other Apple devices, providing a cohesive and secure smart home experience. HomeKit emphasizes privacy and security, aligning with Apple's broader ecosystem policies .

The Figure 4 provides a clear representation of the architecture of Apple HomeKit, illustrating how it integrates various components to enhance user interaction and device management within a smart home system. In this setup, users interact with the HomeKit environment primarily through the HomeKit app, accessed via the internet on their devices. The app allows for both direct control and voice command inputs, which are processed by the HomeKit device. This device then streams voice data to the Apple Cloud, where commands are processed and user management is handled, ensuring that actions are personalized and secure. The system also supports audible feedback, providing users with immediate responses to their commands. This interaction cycle is supported by Apple's robust ecosystem, which includes Apple Services and External APIs. These components allow HomeKit to perform a wide range of functions, from simple device control to complex automations. Apple Services process the API calls

[4] https://www.developer.apple.com/homekit

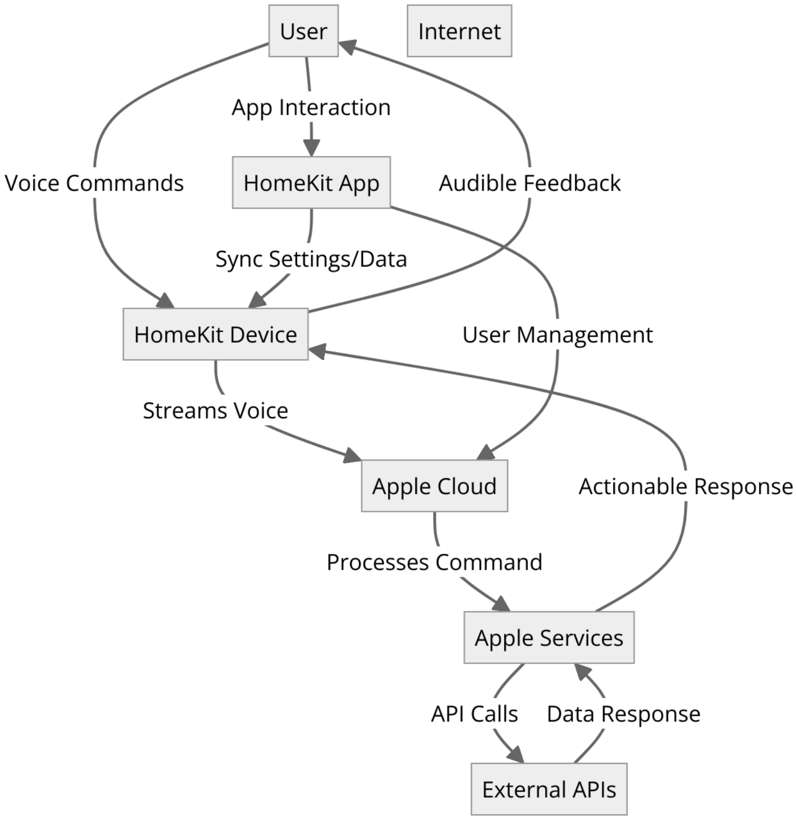

Figure 4. Apple HomeKit system architecture

and provide data responses, ensuring that every user command results in actionable and precise outcomes. This architecture not only demonstrates the interconnectedness of Apple's services but also highlights the seamless and intuitive user experience HomeKit aims to offer.

3.4.1 Affordability

Apple HomeKit itself does not have any subscription fees. However, to use HomeKit, you need compatible Apple devices like iPhones, iPads, or HomePods, which are typically more expensive compared to non-Apple alternatives. HomeKit-compatible smart home devices can also be slightly more expensive due to Apple's certification requirements.

3.4.2 Technical advantages and disadvantages

Advantages: HomeKit is renowned for its strong integration with Apple devices, ensuring a seamless user experience. It uses Wi-Fi and Bluetooth to communicate with devices, making connections stable and reliable. HomeKit's emphasis on security and privacy is a significant advantage, as it uses end-to-end encryption and all data is processed locally on the device, not in the cloud.

Disadvantages: The major drawback is the limited compatibility with non-Apple products, which can be a significant limitation for users looking for a more universal solution. The platform also tends to be more expensive due to the premium associated with Apple products and services.

3.4.3 Security

HomeKit prioritizes security with end-to-end encryption and strict data privacy measures, making it one of the most secure smart home options available. Regular updates from Apple keep devices secure without compromising privacy, adhering to Apple's high standards for data protection.

3.4.4 Privacy

Privacy is a cornerstone of HomeKit's design; all data is localized, processed on-device, and encrypted. Apple's proactive privacy measures ensure that user data is not only secure but also kept private from any third parties, including Apple, aligning with GDPR and other privacy regulations.

3.4.5 Reliability

HomeKit devices are generally highly reliable and integrate seamlessly with iOS, providing a consistent and dependable user experience. The use of Wi-Fi and Bluetooth supports robust and stable connections to various devices throughout the home.

3.4.6 Ease of use/intuitive

HomeKit is designed with a focus on simplicity and ease of use. Setting up and controlling devices through the Home app or Siri is straightforward, making it accessible even to those who are not particularly tech-savvy. Adding devices to HomeKit usually involves scanning a QR code or entering a setup code provided by the device manufacturer, which can make the process quite seamless. Removing devices is also straightforward through the Home app on iOS devices.

3.4.7 Compatibility and Support

While HomeKit's compatibility is extensive within Apple's ecosystem, it may not work as well with non-Apple products. This can be a limiting factor for users seeking flexibility in their smart home setups. However, for users of Apple products, the ecosystem is well-supported with responsive customer service.

3.5 Domoticz

Domoticz[5] is an open-source platform that attracts do-it-yourself smart home enthusiasts with its versatile capabilities. It supports a wide range of devices and offers extensive customization options, making it a flexible choice for those looking to tailor their smart home setup to specific needs.

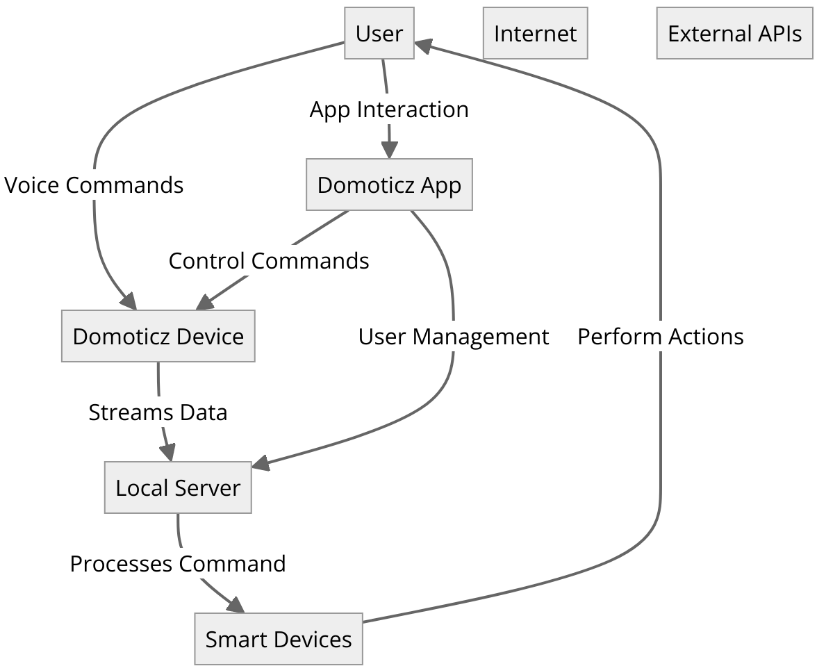

Figure 5. Domoticz system architecture

The Figure 5 illustrates the architecture of the Domoticz smart home system. It outlines the interaction between the user, the Domoticz application, and the connected devices within the smart home environment. Users interact with the system primarily through the Domoticz App, which can be accessed via internet-connected devices. This app sends control commands to the Domoticz Device, which serves as the central communication hub in the system. The Domoticz Device streams data to a local server, which processes the commands and manages the interactions with smart devices in the home, such as executing automation tasks and managing device statuses. Additionally,

[5] `https://www.domoticz.com`

the system supports voice commands, enhancing user interaction through more intuitive control options. The architecture also integrates with external APIs, allowing Domoticz to extend its functionality and interact with a broader range of devices and services outside its immediate ecosystem. This setup ensures a flexible and comprehensive control environment for the user, effectively managing the smart home through both local and web-based interfaces.

3.5.1 Affordability

Domoticz is a free and open-source home automation system that runs on various inexpensive and accessible hardware platforms like Raspberry Pi, Windows, macOS, and Linux servers. This makes it highly affordable and attractive for do-it-yourself enthusiasts and those who prefer to utilize existing hardware.

3.5.2 Technical advantages and disadvantages

Advantages: Domoticz supports a vast range of devices and protocols, including Z-Wave, Zigbee, MQTT, 1-Wire, and many others, making it incredibly versatile for integrating various smart devices. Its open-source nature allows for extensive customization and community-driven enhancements. The user interface is practical and can be accessed via any web browser, simplifying remote management and monitoring.

Disadvantages: The setup and configuration of Domoticz can be complex, especially for users without technical background. Its interface, while functional, is not as polished as commercial platforms like Google Nest or Apple HomeKit. The reliance on community support rather than dedicated customer service can be a drawback for users expecting immediate and professional support.

3.5.3 Security

Domoticz provides reasonable security options, such as encrypted connections for remote access. However, being an open-source platform, it depends heavily on the community and the user's ability to implement and maintain security measures, which can vary in robustness.

3.5.4 Privacy

With Domoticz, all data is stored locally, providing significant privacy benefits. Users have complete control over their data, and since it does not rely on cloud services, it is less susceptible to hacking and external surveillance compared to systems that store information in the cloud.

3.5.5 Reliability

Domoticz's performance and reliability heavily depend on the user's setup and the hardware used. On stable and compatible hardware with proper setup, it offers strong reliability, though users may experience variability based on their configuration and updates from the community.

3.5.6 Ease of use/intuitive

Domoticz might present a steeper learning curve due to its technical complexity and do-it-yourself nature. The platform requires manual setup and configuration, which can be challenging for non-technical users. Adding devices to Domoticz may require some manual configuration, depending on the device type and brand. However, there is usually good documentation and community support available. Removing devices typically involves accessing the Domoticz interface and deleting them from the device list.

3.5.7 Compatibility and Support

Domoticz is compatible with a wide array of devices and technologies due to its open-source protocol support. The community forums provide a wealth of knowledge and support from other users and developers, which can help mitigate issues and extend functionality through custom scripts and solutions.

3.6 Calaos

Calaos[6] is known in niche circles for offering a comprehensive home automation suite. As an open-source platform, it provides a full-featured solution for managing and automating various smart home devices, with a focus on flexibility and user control.

The Figure 6 outlines the architecture of the Calaos smart home system. Users interact with the system via the Calaos Web UI and the Mobile App, which both connect to the Calaos Server. This server acts as the central hub, processing commands and controlling various devices within the smart home setup. It manages a Wago PLC for automation tasks, various IP devices like cameras and sensors, and a Raspberry Pi for additional functionalities. This setup ensures that user commands are efficiently translated into actions, allowing seamless control of the smart home environment from multiple interfaces. The diagram effectively captures the flow of communication and control within the Calaos system, illustrating its comprehensive and integrated approach to home automation.

[6] `https://www.calaos.fr`

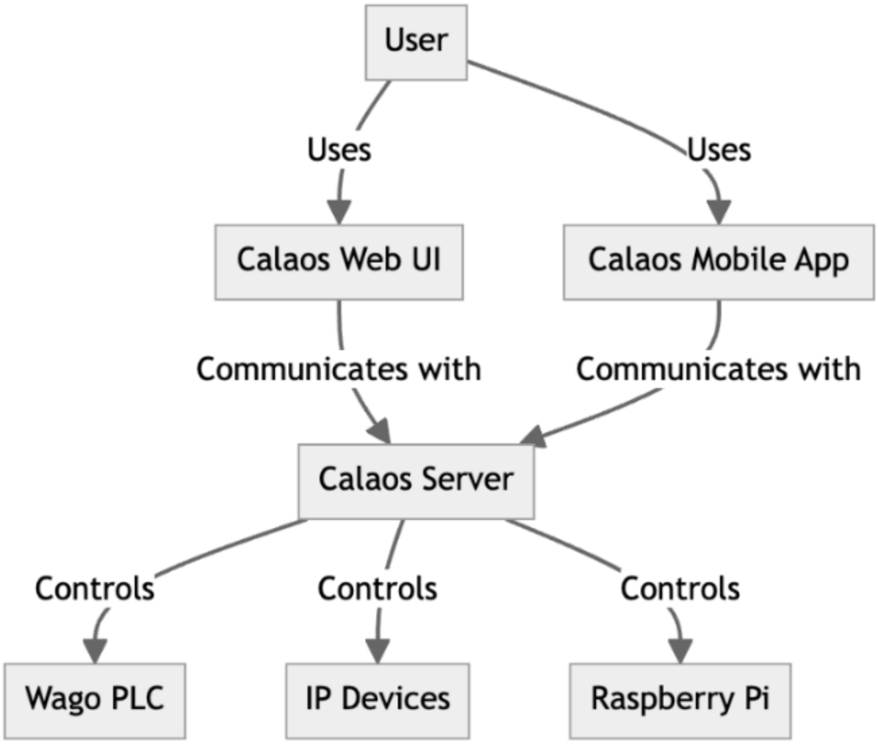

Figure 6. Calaos system architecture

3.6.1 Affordability

Domoticz is an open-source home automation platform, meaning the software itself is free to use. However, users should budget for hardware costs, such as a Raspberry Pi or dedicated server, as well as any smart home devices they wish to integrate with the system. There are no subscription fees associated with Domoticz.

3.6.2 Technical advantages and disadvantages

Advantages: Calaos is designed with ease of use in mind, featuring a user-friendly interface that caters to both novices and experienced users. It supports a wide range of devices and communication protocols such as KNX, X10, and others, facilitating flexible device integration. Being open-source, it allows for extensive customization and community-driven enhancements.

Disadvantages: While the platform is versatile, the reliance on community support can pose challenges in terms of finding immediate help or troubleshooting complex issues. The user interface, though straightforward, may not offer the same level of polish or integration as more commercially developed platforms like Google Nest or Apple HomeKit.

3.6.3 Security

Calaos offers basic security features that can be enhanced by savvy users who are capable of leveraging the open-source nature of the software to implement advanced security measures. However, like many open-source projects, the level of security will largely depend on the user's knowledge and ability to apply these enhancements effectively.

3.6.4 Privacy

Privacy is a strong suit for Calaos as it stores all data locally and does not depend on cloud services, which minimizes exposure to external vulnerabilities and unauthorized data access. Users maintain full control over their data, a significant advantage for those concerned with privacy.

3.6.5 Reliability

The reliability of Calaos depends on the specific hardware and network setup of the user. With proper installation and maintenance, it can be highly reliable, but it may require technical knowledge to optimize and troubleshoot, more so than some commercial alternatives.

3.6.6 Ease of use/intuitive

Calaos is straightforward to install and configure, with a focus on making home automation accessible to newcomers. The platform's interface is intuitive, providing clear navigation which enhances user experience and simplifies the management of connected devices. Calaos provides a user-friendly interface for managing devices, and adding new devices is usually straightforward through the interface. Removing devices can also be done through the Calaos interface with a few clicks.

3.6.7 Compatibility and Support

Calaos's compatibility with a broad range of protocols and devices enhances its adaptability in various home automation scenarios. Support is primarily community-driven, available through forums and documentation, where users can seek advice and share solutions.

3.7 OpenMotics(Renson)

OpenMotics (Renson)[7] is an open-source solution for both hardware and software automation, primarily targeting the European market. It emphasizes energy efficiency and integrates well with other systems, making it a solid choice for users looking for a comprehensive home automation system .

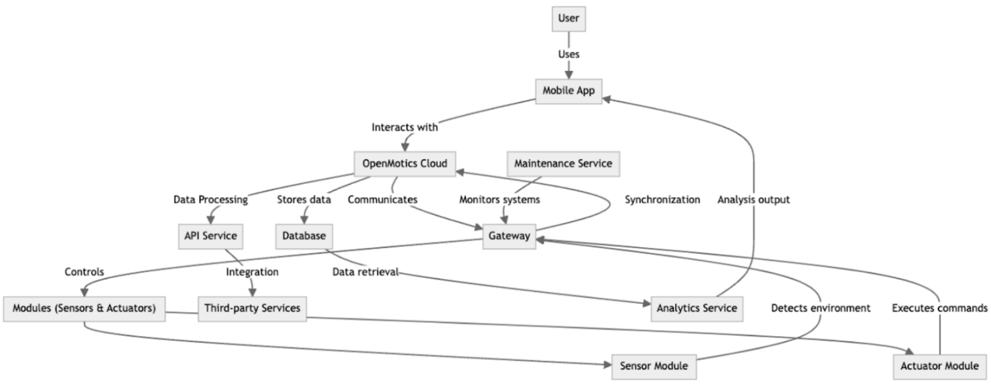

Figure 7. OpenMotics system architecture

The Figure 7 illustrates the architecture of the OpenMotics system, highlighting its comprehensive smart home management capabilities. The core of the system is the OpenMotics Cloud, which interfaces with a mobile app used by homeowners to control and monitor their environment. This cloud manages data storage, communication, and synchronization with the Gateway, which oversees system performance and maintenance. The architecture also features an API service for processing data and facilitating third-party integrations, enhancing functionality. Sensors and actuators detect conditions and execute commands, supported by a database and an Analytics Service that store, analyze, and provide insights from the data. This setup ensures seamless operation and integration across the system, effectively managing everything from user interactions to complex data processing.

3.7.1 Affordability

OpenMotics is a modular home automation platform that offers variable pricing based on the hardware components chosen by the user. This pricing structure allows for scalable solutions that can be tailored to fit budgetary constraints and specific needs, making it

[7] https://www.openmotics.com

a cost-effective choice for those looking to customize their home automation systems extensively.

3.7.2 Technical advantages and disadvantages

Advantages: OpenMotics emphasizes modularity and flexibility, supporting a wide array of communication protocols such as KNX and Modbus. This makes it highly adaptable for controlling various home functions like lighting and heating. The system's open-source nature allows for significant customization and integration with an extensive range of devices.

Disadvantages: The platform can face technical challenges such as maintaining compatibility across different devices and ensuring seamless integration within the network.

3.7.3 Security

OpenMotics takes a proactive approach to security, integrating advanced protocols and offering users the ability to heavily customize their security settings due to its open-source framework. However, like any system dependent on user configuration, the effectiveness of these security measures can vary significantly based on how they are implemented.

3.7.4 Privacy

Privacy is a cornerstone of OpenMotics' design, with all data handled locally and minimal reliance on cloud services, thereby reducing the risk of external breaches. The platform's open-source model further ensures that users have complete control over their data and its management.

3.7.5 Reliability

Due to its modular nature, the reliability of OpenMotics can depend greatly on the chosen hardware and the user's configuration. When set up with compatible and robust hardware, the system is highly reliable and capable of managing multiple automation tasks seamlessly.

3.7.6 Ease of use/intuitive

OpenMotics' platform, while powerful, is not necessarily user-friendly for those unfamiliar with home automation or without a technical background. The system requires a hands-on approach for installation and maintenance, which might challenge non-technical users. OpenMotics offers a web-based interface for managing devices, and adding new devices typically involves following the setup wizard or entering device details manually. Removing devices can usually be done through the interface with a few clicks.

3.7.7 Compatibility and Support

The platform's support for protocols like KNX and Modbus enhances its compatibility with a wide range of devices and systems, making it versatile for various home automation applications. Support is community-driven, provided through forums and documentation, where users can exchange insights and solutions.

3.8 HomeGenie

HomeGenie[8] is noted for its customizable options in smart home automation. This open-source platform offers a range of features that can be tailored to meet individual user preferences, providing a robust and flexible solution for home automation enthusiasts .

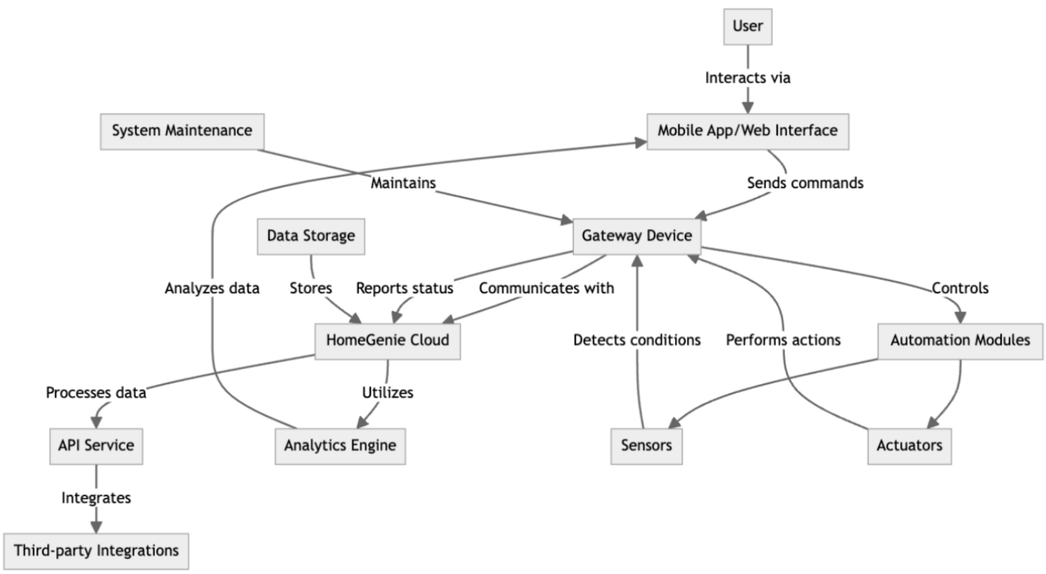

Figure 8. HomeGenie system architecture

The Figure 8 illustrates the architecture of the HomeGenie smart home system, showing how the various components interact to create an efficient and responsive smart home environment. At the user level, interaction is facilitated through a mobile app or web interface, allowing the user to send commands directly to the Gateway Device. This

[8] https://www.genielabs.github.io/HomeGenie

gateway is the core communication hub that connects with the HomeGenie Cloud for data storage and management, where data is stored, analyzed, and the system's status is reported back to the user. The Gateway Device also interfaces with various sensors and actuators, detecting environmental conditions and performing actions as needed, which are controlled by automation modules configured within the system. The HomeGenie Cloud utilizes an Analytics Engine to process the data collected, enhancing system intelligence and responsiveness. Additionally, the system includes an API Service that processes data and integrates third-party applications to extend the system's capabilities and flexibility. System maintenance is continually addressed to ensure operational integrity and reliability. Overall, the diagram aims to provide a clear visualization of the HomeGenie architecture, highlighting how each component contributes to a comprehensive smart home solution.

3.8.1 Affordability

HomeGenie is a free, open-source home automation server, making it an economical choice for individuals looking to enter the realm of home automation without incurring high startup costs. Its open-source nature not only ensures cost-effectiveness but also allows for extensive community-driven development and support.

3.8.2 Technical advantages and disadvantages

Advantages: HomeGenie features a user-friendly interface that simplifies the management and control of home automation devices, appealing to both novices and experienced users. It supports a variety of communication protocols including X10, Z-Wave, among others, facilitating compatibility with a broad range of devices and enhancing system flexibility.

Disadvantages: While HomeGenie is praised for its simplicity and broad protocol support, its open-source model may lead to variability in user experience, particularly with respect to reliability and support. The interface, while straightforward, may lack the depth of customization and advanced features provided by more developed, commercial platforms.

3.8.3 Security

HomeGenie provides basic security features that can be expanded through user customization, leveraging its open-source capabilities. Users are encouraged to implement additional security measures to enhance the system's defense against potential cyber threats, given the platform's reliance on community updates and patches.

3.8.4 Privacy

Privacy is a significant advantage of HomeGenie, as it processes and stores data locally without the need for cloud dependency. This local management of data not only speeds up operations but also significantly reduces the vulnerability of users' personal information to external breaches.

3.8.5 Reliability

The reliability of HomeGenie can vary depending on the hardware used, the user's technical skill in setup and maintenance, and the community's contributions to updates and fixes. Properly configured systems on compatible hardware are generally stable and reliable.

3.8.6 Ease of use/intuitive

HomeGenie's interface is designed to be intuitive and straightforward, removing barriers to entry for users new to home automation. This ease of use is a core feature that distinguishes it from more complex systems, making it accessible to a wider audience. Adding new devices to HomeGenie may require some manual configuration, but there are usually guides available to help with the process. Removing devices can be done through the HomeGenie interface with relative ease.

3.8.7 Compatibility and Support

Supporting protocols such as X10 and Z-Wave allows HomeGenie to manage a diverse set of devices, making it a versatile choice for comprehensive home automation setups. Community support, primarily available through forums and online documentation, plays a crucial role in assisting users with troubleshooting and system enhancements.

3.9 Samsung SmartThings

Samsung SmartThings[9] is a proprietary system by Samsung, renowned for its compatibility with a broad range of devices and its extensive third-party integrations. It provides a user-friendly interface and strong support, making it a popular choice among smart home users.

The Figure 9 illustrates the Samsung SmartThings ecosystem, focusing on how different components interact to manage a smart home efficiently. Central to the system is the SmartThings Hub, which coordinates local and cloud processing to ensure seamless operation of connected smart devices. Users interact with this system through a

[9] https://www.samsung.com/us/smart-home

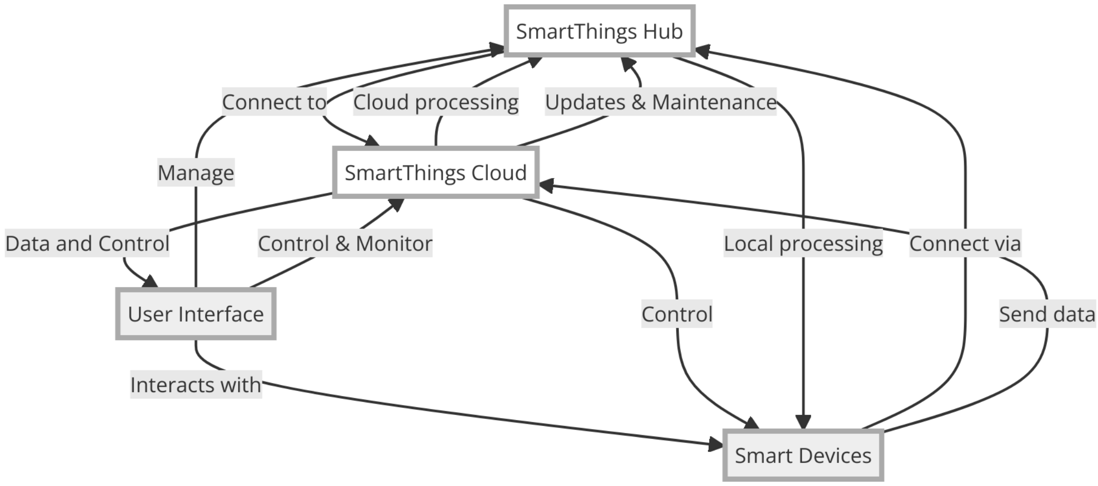

Figure 9. Samsung SmartThings system architecture

mobile app, providing an interface to control various devices such as lighting, security systems, and HVAC (heating, ventilation, and air conditioning) units directly from their smartphones. The SmartThings Cloud plays a critical role in this architecture, handling commands from the mobile app and pushing updates and maintenance to the hub, ensuring the system remains efficient and secure. It also facilitates third-party integrations, expanding the system's capabilities by allowing compatibility with a wider range of devices and services. The diagram aims to clearly demonstrate these relationships and how they contribute to a comprehensive smart home solution, showcasing the integrated and user-friendly nature of the Samsung SmartThings platform.

3.9.1 Affordability

Samsung SmartThings is a versatile smart home platform offering both a free tier with basic functionality and a paid subscription called SmartThings Premium, priced around $5 per month. It provides users with the ability to connect and control a wide range of smart devices, offering convenience and flexibility in home automation. With its competitive pricing and extensive device compatibility, SmartThings is a popular choice for those seeking an affordable and scalable smart home solution.

3.9.2 Technical advantages and disadvantages

Advantages: SmartThings provides a comprehensive and user-friendly platform that supports a wide array of smart devices. It primarily utilizes Zigbee and Z-Wave protocols, enhancing its compatibility with a vast ecosystem of products, which includes everything from sensors and cameras to light bulbs and locks. The platform is also noted for its robust automation capabilities, allowing users to create complex interaction rules between devices easily.

Disadvantages: While the platform is rich in features and supports extensive device integration, it may present challenges in stability and user experience inconsistencies across different devices. Additionally, reliance on a cloud-based infrastructure might raise concerns about connectivity and privacy.

3.9.3 Security

SmartThings employs stringent security measures including secure boot, hardware encryption, and optional two-factor authentication to protect user data and device functionality. These features aim to provide a secure environment for users to connect and manage their home devices.

3.9.4 Privacy

SmartThings processes significant amounts of user data to function effectively, which involves both device-generated data and user interactions that pass through Samsung's servers. While Samsung asserts commitment to user privacy, the scale of data collection and cloud dependency pose inherent privacy risks.

3.9.5 Reliability

SmartThings' reliability is generally high, thanks to Samsung's robust technical infrastructure and continuous software updates aimed at resolving bugs and enhancing functionality. However, performance can vary by device and the complexity of the user's setup.

3.9.6 Ease of use/intuitive

The SmartThings app is intuitive and simplifies the process of integrating and managing smart home devices. Its user-friendly interface is accessible on mobile devices and web browsers, offering flexibility in how users control their home environment. Adding devices to SmartThings is usually straightforward through the SmartThings app, especially for devices that are certified to work with SmartThings. Removing devices can also be done through the app with a few taps.

3.9.7 Compatibility and Support

Samsung SmartThings' compatibility is extensive, supporting a wide range of third-party devices in addition to Samsung products. This open compatibility is a key strength, allowing users to mix and match devices from various manufacturers. Support is provided directly through Samsung with ample resources such as guides, FAQs, and customer service channels.

3.10 Control4

Control4[10] offers proprietary high-end custom smart home systems and is popular among those looking for sophisticated home automation solutions. It provides extensive customization and integration options, often requiring professional installation and support to optimize its advanced capabilities.

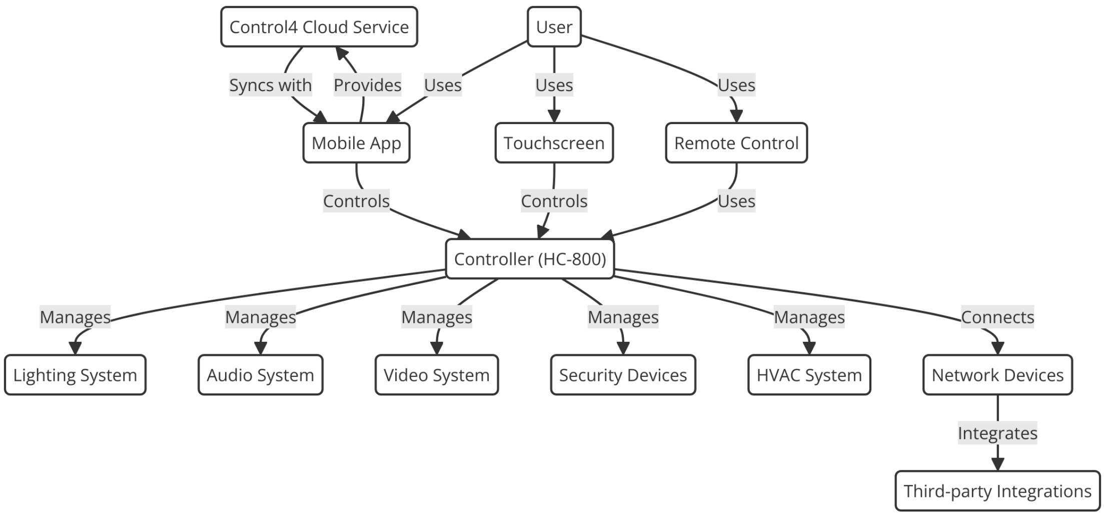

Figure 10. Control4 system architecture

The Figure 10 offers a clear and detailed view of the architecture for a Control4 smart home system. The system allows a user to interact with the home environment via multiple control interfaces, including a mobile app, touchscreen, and remote control. Each of these interfaces connects to the Control4 Cloud Service, which syncs with and provides services to the mobile app, ensuring all user commands and preferences are updated in real-time. The Controller (HC-800) manages several critical subsystems within the home, such as lighting, audio, video, security devices, and HVAC (heating, ventilation, and air conditioning) systems, providing a centralized point of control for these diverse functionalities. Each subsystem can interact with the controller to execute user commands efficiently and seamlessly. Furthermore, the Controller facilitates connections with network devices and integrates third-party integrations, enhancing the

[10] https://www.control4.com

system's capabilities and allowing for a broader range of services and device support. This setup emphasizes the system's modularity and versatility, illustrating how the Control4 architecture is designed to offer a comprehensive, integrated smart home solution.

3.10.1 Affordability

Control4 is a professionally installed smart home system, and pricing can vary significantly depending on the size and complexity of the installation, as well as the specific features and devices chosen. A basic Control4 setup for a small home might start at a few thousand dollars, while larger installations with extensive automation capabilities can cost tens of thousands of dollars or more. Control4 is generally considered a premium option and can be more expensive compared to do-it-yourself smart home solutions.

3.10.2 Technical advantages and disadvantages

Advantages: Control4 offers a highly advanced and integrated solution designed for comprehensive control over a wide array of home devices including lighting, security, entertainment, and more. Its use of a wired network infrastructure ensures reliable and fast communication between devices, which enhances the system's overall stability and performance.

Disadvantages: The platform's complexity can result in significant downtime during updates or system modifications.

3.10.3 Security

Control4 systems are designed with strong security protocols to protect against unauthorized access and to ensure the integrity of the home automation system. The professional installation further enhances security by ensuring that all components are correctly configured to safeguard user data and privacy.

3.10.4 Privacy

With professional installation and a closed network environment, Control4 provides enhanced privacy compared to many do-it-yourself systems. Data is handled within a secure network with limited exposure to external threats, ensuring a high degree of privacy for users.

3.10.5 Reliability

The use of a robust wired network infrastructure by Control4 ensures a highly reliable connection among all integrated devices. This setup minimizes downtime and maintains consistent performance across the system, which is a significant advantage in critical applications like security and climate control.

3.10.6 Ease of use/intuitive

Despite its complex setup, once installed, Control4 systems are user-friendly and can be controlled via smartphones, tablets, or wall-mounted panels. The interface is designed to be intuitive, providing users with straightforward, logical control over their entire home environment. Control4 systems are typically installed and configured by professional integrators, so adding and removing devices may require assistance from a trained technician.

3.10.7 Compatibility and Support

Control4 systems are compatible with thousands of third-party devices and are designed to work seamlessly with a variety of brands and technologies. This wide compatibility is supported by ongoing updates and professional support from certified technicians, which helps to maintain system performance and extend its capabilities over time.

3.11 Wink

Wink[11] is known for its user-friendly interface and broad compatibility with smart home devices. It offers a flexible and cost-effective solution for managing various smart home technologies, making it accessible to a wide range of users.

The Figure 11 of the Wink smart home system, as depicted in the provided diagram, clearly outlines how the system is orchestrated via the Wink Hub, which serves as the central command center. This hub communicates directly with a mobile app, allowing users to manage their smart home devices remotely. The Wink Hub is responsible for controlling a diverse array of devices across several categories, including lighting control systems, security devices, HVAC (heating, ventilation, and air conditioning) systems, and various smart appliances. Each of these device categories is synchronized with the Wink Cloud, ensuring that device states are updated in real-time and can be accessed remotely. The Wink Cloud plays a crucial role in this architecture, performing data analysis to enhance system performance and facilitate smarter home automation. Additionally, it interfaces with third-party services, expanding the system's functionality by incorporating external platforms and services. This comprehensive setup allows the Wink system to offer an integrated smart home solution that is both flexible and user-friendly, providing users with control and monitoring capabilities that enhance the convenience and efficiency of their home environments.

[11] https://www.wink.com

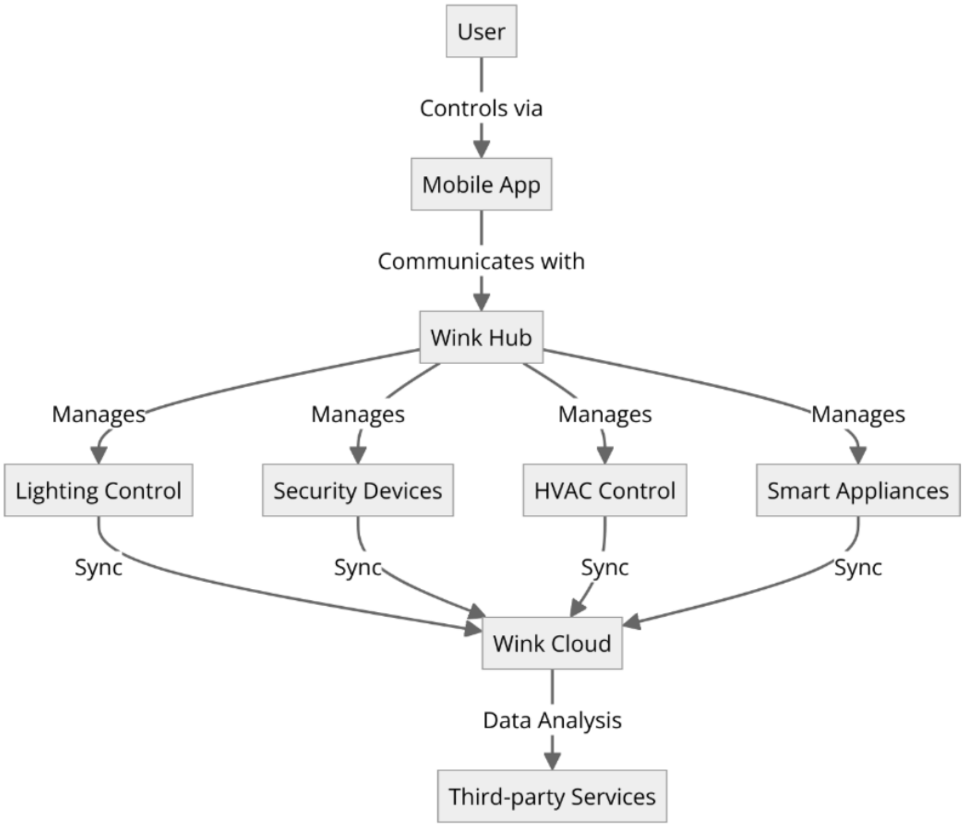

Figure 11. Wink system architecture

3.11.1 Affordability

Wink offers a cost-effective solution for home automation with its smart home hub priced to accommodate modest budgets. The pricing varies depending on the Wink-compatible devices chosen, allowing users to scale their system according to their financial capacity. Also Wink offers a subscription service called Wink Plus, which provided additional features and support for $5.99 USD per month.

3.11.2 Technical advantages and disadvantages

Advantages: Wink supports a variety of smart home devices using Wi-Fi and Zigbee protocols, providing reliable and extensive technical coverage for home automation.

Disadvantages: Wink has experienced some challenges, including reliability issues and a subscription model change that has impacted user trust and satisfaction. These factors may deter new users or those looking for a stable long-term investment.

3.11.3 Security

Wink incorporates standard security protocols, including advanced encryption and security measures to protect device communications. However, the platform has faced challenges with system outages and connectivity issues, which raise concerns about overall security and data integrity.

3.11.4 Privacy

Wink asserts a strong commitment to user privacy, ensuring that data is handled with care and not sold to third parties. Despite this, the use of cloud-based services means that users must trust Wink with their device data, which could be a point of concern for privacy-conscious individuals.

3.11.5 Reliability

While Wink offers a versatile and easy-to-use platform, its reliability has been questionable, evidenced by past system outages and delays in functionality updates. These issues could compromise the effectiveness of home automation routines and user confidence in the system.

3.11.6 Ease of use/intuitive

One of Wink's strongest features is its intuitive and simple interface, which enhances user experience and accessibility. Setting up and integrating devices is generally streamlined, making it easy for even non-technical users to build and manage their smart home environments. Adding devices to Wink is usually straightforward through the Wink app, especially for devices that are officially supported. Removing devices can also be done through the app with a few taps.

3.11.7 Compatibility and Support

Wink supports a wide range of devices through Wi-Fi and Zigbee, ensuring broad compatibility with a variety of smart home products. However, support has been a concern for some users, particularly with the transition to a subscription-based model, which has added a layer of complexity and cost to the user experience.

3.12 Home Assistant

Home Assistant[12] is a highly flexible, open-source platform popular among do-it-yourself enthusiasts for its extensive integration capabilities. It supports a wide array of devices

[12] https://www.home-assistant.io

and protocols, allowing for significant customization and control over home automation systems.

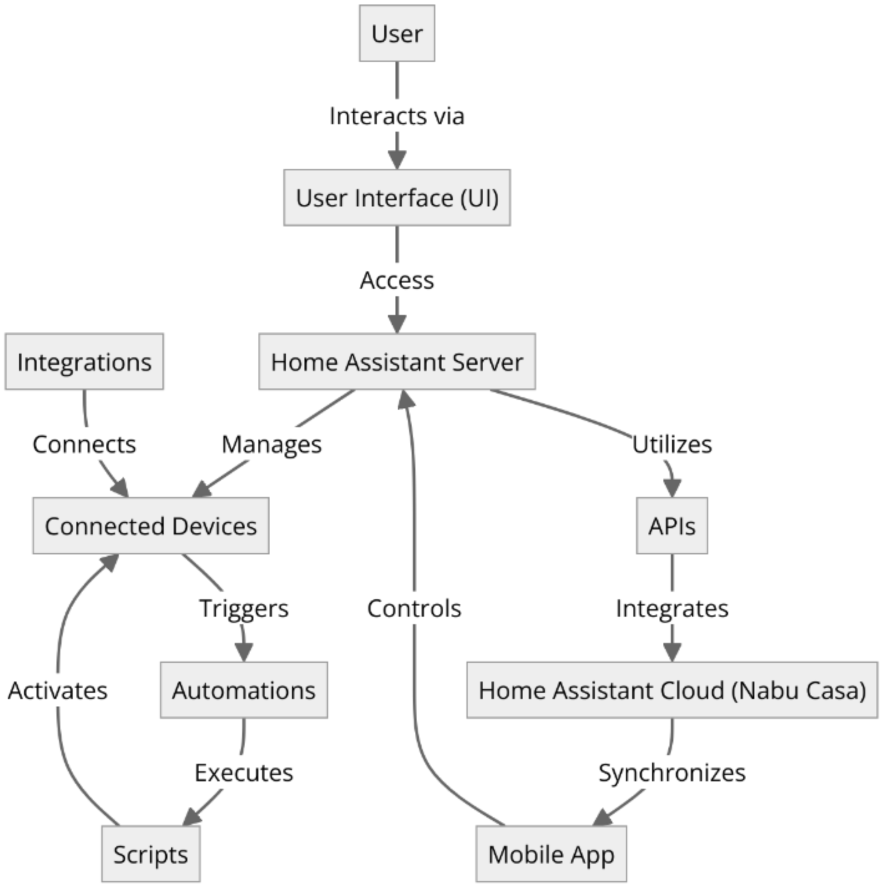

Figure 12. Home Assistant system architecture

The Figure 12 captures the architecture of Home Assistant, illustrating how this open-source home automation platform functions at both a local and remote level. It begins with the user, who interacts with the system via a web-based user interface. This interface is key for allowing users to control and monitor their smart home settings. At the core of the system is the Home Assistant Server, which handles various connected devices through integrations. These integrations enable the platform to interface with a diverse array of home automation devices, enhancing its versatility. The connected devices are shown to trigger automations that can execute scripts, automating specific actions based on user-defined conditions. The diagram also incorporates the Home Assistant Cloud (Nabu Casa), highlighting its role in enabling remote access and integration with voice assistants, and its synchronization with a mobile app for convenient remote management.

This connectivity is facilitated by APIs, which are essential for the seamless operation between the server and cloud services. The diagram aims to provide a comprehensive overview of how Home Assistant manages both local and remote interactions, showcasing the platform's extensive capabilities and connectivity.

3.12.1 Affordability

Home Assistant is open-source software, so there are no subscription fees. However, users may incur costs for compatible hardware and optional add-ons like Z-Wave or Zigbee dongles. Overall, Home Assistant is one of the most cost-effective options for those willing to invest time in setting up and customizing their smart home system.

3.12.2 Technical advantages and disadvantages

Advantages: Home Assistant excels in flexibility and the breadth of device support, including Wi-Fi, Zigbee, Z-Wave, and more, making it one of the most versatile home automation systems available. Its strong focus on local control enhances security and reliability, while community-driven updates continuously expand its capabilities and integrations without the need for subscription fees.

Disadvantages: Open-source nature can lead to inconsistent support and the need for frequent technical troubleshooting to maintain optimal performance.

3.12.3 Security

Home Assistant prioritizes privacy and security with its local processing approach—no personal data is sent to the cloud unless configured by the user. Regular updates and the ability to integrate secure communication protocols further strengthen its security stance.

3.12.4 Privacy

Privacy is a cornerstone of Home Assistant's design. The platform operates primarily locally, not relying on cloud services to store or process data, which significantly reduces the risk of external hacking attempts and data breaches. Users have full control over their data and can enhance privacy with additional configurations.

3.12.5 Reliability

The reliability of Home Assistant depends largely on the user's hardware and network setup but is generally high due to the local processing of tasks and commands. The active community quickly addresses bugs and issues through frequent updates, contributing to the system's overall stability.

3.12.6 Ease of use/intuitive

While highly customizable, Home Assistant can be complex to configure, especially for those without technical background. However, once set up, it offers a powerful interface that provides comprehensive control over all connected devices, with relatively straightforward day-to-day operation. Adding devices to Home Assistant can vary in difficulty depending on the device type and brand. However, there is usually extensive documentation and community support available. Removing devices can typically be done through the Home Assistant interface with relative ease.

3.12.7 Compatibility and Support

Home Assistant supports an extensive array of devices and protocols, making it highly compatible with almost any smart device in the market. Support is community-driven, provided through forums, social media, and detailed online documentation, helping users troubleshoot and optimize their setups.

4 Security and Privacy

As smart home technologies proliferate, securing these interconnected devices becomes paramount, not only to protect against unauthorized access but also to safeguard personal data privacy. This problem statement explores the multifaceted security and privacy issues currently impacting smart home platforms, focusing on their potential vulnerabilities and the robustness of the countermeasures in place.

4.1 Security challenges

In the realm of smart home security, several mechanisms are employed to safeguard devices and data against potential threats. Encryption and authentication serve as foundational security measures, with most platforms utilizing robust methods like AES for encryption and protocols such as TLS for authentication to protect sensitive data during transmission. However, the effectiveness of these measures can vary significantly across different platforms, sometimes leading to vulnerabilities in systems with weaker implementations.

For instance, in 2019, there were multiple reported incidents of hackers gaining unauthorized access to Ring security cameras installed in homes [51]. Weak or reused passwords were often cited as the cause, highlighting the importance of strong authentication measures like two-factor authentication.

To combat both physical and software threats, some platforms, including Samsung SmartThings, employ secure boot mechanisms and hardware-level encryption. These features are designed to ensure the integrity and confidentiality of device data from the point of booting the device and throughout its operation. Despite such efforts, vulnerabilities in smart locks have been exploited to gain unauthorized access to homes, underscoring the ongoing challenges in maintaining security. Nonetheless, regular security updates are critical for maintaining the security integrity of smart home platforms. Systems like Home Assistant and OpenHAB highlight the necessity for frequent updates to address new vulnerabilities and prevent potential cyberattacks. However, even with proactive measures, data breaches have occurred, Denning et al. (2013) detailed cases where attackers could hack smart home systems and gain control over connected devices, like unlocking doors or turning on appliances that could cause a fire hazard [52].

Dependence on consistent vendor support and proactive user involvement in applying updates plays a crucial role in mitigating risks, though it can sometimes lead to increased exposure if not diligently managed. Additionally, two-factor authentication (2FA) is increasingly being implemented to enhance security further. This method requires two forms of user verification to access smart home systems, significantly reducing the likelihood of unauthorized access. The effectiveness of 2FA hinges on users maintaining stringent security practices, underscoring the interactive relationship between system security measures and user behavior. Together, these mechanisms form a comprehensive security strategy for smart home platforms, each contributing to a layered defense system intended to protect against a variety of security threats.

4.2 Privacy Issues

In addressing privacy issues within smart home ecosystems, several mechanisms and strategies are crucial for safeguarding user data and enhancing privacy. Data localization, as seen with platforms like Home Assistant, focuses on local data processing and storage to minimize dependency on cloud services, which reduces the risk of breaches through external networks. Although local storage improves privacy by keeping data physically close to the user, it requires strong local security measures to prevent unauthorized physical access. Furthermore, open-source platforms often adopt a policy of minimal data retention to mitigate privacy risks, in contrast to many commercial platforms that store extensive user data for longer periods, potentially for processing or monetization purposes. By retaining only the minimal necessary data, these platforms reduce the potential impact of a data breach, aligning with the privacy preferences of security-conscious users.

Compliance with privacy regulations such as the General Data Protection Regulation (GDPR) is also crucial, particularly for platforms operating in or serving customers within the European Union. This involves a continuous effort from platform providers to monitor, adjust, and ensure transparency in how user data is handled, requiring platforms to engage in transparent data practices and to provide users with enhanced control over their personal information. Lastly, while cloud computing offers enhanced functionality and convenience, it introduces significant privacy challenges, as data stored in the cloud is potentially more susceptible to external breaches and surveillance.

This dependency complicates the privacy landscape by increasing the number of vectors through which unauthorized access to data may occur. Platforms leveraging cloud services must balance these benefits with the increased risks and ensure robust security measures are in place to protect data. Collectively, these mechanisms form the backbone of privacy protection in smart home platforms, aiming to balance functionality with the imperative of protecting user privacy and contributing to a comprehensive strategy intended to mitigate risks and enhance the trustworthiness of smart home technologies.

5 Communication Protocols

Smart home systems integrate various communication protocols to facilitate interaction between devices. These protocols vary in range, capacity, stability, and popularity, influencing their suitability for specific applications in smart homes. This document assesses the widely used [53] communication protocols—Wi-Fi, Zigbee, Z-Wave, and Bluetooth.

5.1 Wi-Fi

Wi-Fi is a prevalent communication technology that offers a substantial range, typically up to about 150 feet indoors, though this can vary based on obstacles and barriers present. It supports the number of devices but may degrade the performance, depending on the router's model, for each additional device or for users on older routers and more congested networks. Wi-Fi is fairly reliable [54] but can be influenced by any other device within a household and other networks and can sometimes be unstable. The main reason for its popularity is that the protocol is available, and data rates are high, therefore making it the obvious choice for smart home devices requiring high bandwidth. Devices supported are devices like Amazon Echo, Google Nest products, most of the smart TVs, and home security systems, all of which need a strong and consistent high-speed internet connection to be operable.

5.2 Zigbee

Zigbee is known for its effective communication range, typically offering up to 300 feet in open air, a distance that can be significantly extended through its mesh networking capabilities. This technology is particularly well-suited for low-power, low-data-rate applications and can support thousands of devices over a mesh network, making it ideal for extensive smart home setups. Zigbee's stability is one of its standout features [55]; it experiences low interference with other household electronics and boasts a mesh network structure that can reroute or continue transmission even if one node fails, ensuring reliable connectivity. Its popularity in home automation can be attributed to its scalability, energy efficiency, and robustness, which are critical for creating large networks of devices. Among the vendors and devices that utilize Zigbee are Philips Hue lighting systems, Samsung SmartThings, and Yale smart locks, all of which benefit from the strong and stable connectivity that Zigbee provides.

5.3 Z-wave

Z-Wave technology, like Zigbee, communicates up to 300 feet in open air and supports mesh networking. A Z-Wave network supports a little more limited number of devices—up to 232—but that is still enough for most of the home automation systems. It is highly notable that one of the major advantages and the main reason for the popularity of Z-Wave home automation systems is high stability and very low risk of interference [56], which is ensured due to its frequency of 908.42 MHz in the U.S. Products like smart locks, lighting, thermostats, and more from companies such as Fibaro, Aeotec, and Honeywell have developed a stable and absolutely secure basis in the area of smart home technology by using Z-Wave devices.

5.4 Bluetooth

Bluetooth typically offers a communication range of about 30 feet, making it more suited to smaller environments unless extenders or additional technologies are used to increase its reach. In terms of connectivity, Bluetooth can support up to seven active devices within a piconet, with the capability for devices to switch between inactive and active statuses to effectively manage connections [57]. While Bluetooth offers a strong connection within a personal-area network, it can be quite susceptible to interference due to other devices on the 2.4 GHz frequency. Bluetooth has been widely adopted because it is supported by virtually every mobile gadget, allowing for easy control and connectivity of compatible smart-home gadgets. Among the supported devices are smart speakers, wearable technology, and some smart home appliances that rely on Bluetooth for quick, short-range communication.

Table 4. Technical Comparison of Network Protocols

Protocol	Wi-Fi	Zigbee	Z-wave	Bluetooth
Range	Up to 150 ft	Up to 300 ft	Up to 300 ft	Up to 30 ft
Device Capacity	Many	Thousands	Up to 232	Up to 7
Stability	High	Very High	Very High	Moderate
Popularity	Very High	High	Moderate	High
Frequency band	2.4 GHz, 5.0 GHz, 6.0 GHz (for Wi-Fi 6E)	2.4 GHz, 0.915 GHz (915 MHz), 0.868 GHz (868 MHz)	0.90842 GHz (908.42 MHz) 0.86842 GHz (868.42 MHz)	2.4 GHz
Latency	2-10 ms	20-100 ms	40 ms	100 ms
Data rate	Up to 9.6 Gbps (Wi-Fi 6)	Up to 250 Kbps	Up to 100 Kbps	Up to 3 Mbps (Bluetooth 4.x)
Power consumption	High for most devices	Very low (sleep mode capable)	Low	Moderate to low
Security	WPA2, WPA3	AES-128 encryption	AES-128 encryption	AES-CCM encryption (Bluetooth 5.x)

The table 4 in the thesis serves as a fundamental resource for understanding the technical specifications and comparative merits of the principal network protocols utilized in smart home technologies—Wi-Fi, Zigbee, Z-Wave, and Bluetooth. This technical comparison is instrumental for developers, manufacturers, and consumers in making informed decisions about which communication protocols might best suit their specific needs for home automation projects. By detailing attributes such as range, device capacity, stability, and security features, the table underscores the unique advantages and limitations of each protocol, facilitating a deeper comprehension of how these technologies can be optimized for different smart home environments. For instance, while Wi-Fi offers substantial data rates suitable for high-bandwidth applications, Zigbee and Z-Wave provide superior device handling and stability, crucial for expansive smart home networks. Bluetooth, with its ubiquitous presence in mobile devices, presents a convenient option for simpler, localized control. This comprehensive technical insight aids stakeholders in strategically selecting or combining these protocols to achieve a balance of performance, efficiency, and security in their smart home systems.

6 Extensibility

Smart home systems are designed to be inherently flexible and adaptable, allowing for the integration of new devices and technologies as they become available. Extensibility is a critical factor in smart home systems, impacting their longevity and adaptability to future needs and innovations [58]. In the main section on Extensibility within the realm of smart home technologies, it is crucial to consider several factors that determine how effectively a platform can adapt to evolving technological landscapes and user needs. These factors include Hardware Integration, Software Adaptability, API Support, and User Interface Scalability.

- Hardware integration is important in explaining the capability of a platform to enable the integration of new devices while maintaining compatibility with different system protocols. This will ensure that the smart home system can handle a wide array of devices being released from the different manufacturers and technologies. Proper hardware integration will keep the platform relevant in the long run, making expansions in the functionality possible without the necessity of overhauling the whole system.

- Software Adaptability refers to the ability of the platform's software to not only integrate new features but also maintain compatibility with updates. This is essential for security and functionality, as software that cannot adapt may become vulnerable to attacks or fail to support newer device functionalities. A platform with high software adaptability can thus provide a more durable and future-proof service to its users.

- API support is another important factor, where the scope of APIs supported by any given platform is directly related to the way it can interface with current and future devices. More API support will mean wider flexibility with integration, and it will be linked to a wider ecosystem of devices and services in an easy manner. This allows not only for a smarter home system but also guarantees functionality with novel technologies that are developed later on.

- User Interface Scalability is essential for maintaining the usability of the smart home system as more devices and functionalities are added. A scalable user interface adapts to increased complexity without becoming cumbersome, thereby preserving the user experience and ensuring that the system remains accessible and manageable, regardless of how extensive it becomes.

Together, these factors form the cornerstone of a smart home platform's extensibility. They determine not just the current effectiveness but also the long-term viability and adaptability of the platform in the face of rapid technological advancements and changing user demands.

The Table 5 provides a comparative analysis of twelve prominent smart home platforms based on four key extensibility criteria: Hardware Integration, Software Adaptability, API Support, and User Interface Scalability. These criteria are essential for evaluating the ability of each platform to adapt and scale in response to advances in smart home technology and user requirements. The table aims to offer a clear overview of how each platform performs in terms of integrating new hardware, accommodating software updates, supporting a range of APIs, and maintaining a user-friendly interface as the system expands.

Table 5. Extensibility Comparison of Smart Home Platforms

Platform	**Hardware Integration**	**Software Adaptability**	**API Support**	**User Interface Scalability**
openHAB	High	High	Extensive	High
Domoticz	Moderate	High	Moderate	Moderate
Calaos	Moderate	Moderate	Limited	Moderate
OpenMotics (Renson)	High	Moderate	Moderate	High
HomeGenie	High	High	Extensive	High
Home Assistant	High	High	Extensive	High
Amazon Alexa	High	Moderate	High	High
Google Nest	Moderate	Moderate	High	Moderate
Apple HomeKit	Moderate	High	High	High
Samsung SmartThings	High	High	High	High
Control4	High	Moderate	Moderate	Moderate
Wink	Moderate	Moderate	Moderate	Moderate

The Table 5 sheds light on the broader implications for users and developers aiming to build or expand their smart home systems. The findings indicate that platforms like openHAB, HomeGenie, and Home Assistant offer robust support across all four criteria, making them potentially more versatile and future-proof for a rapidly evolving market. On the other hand, platforms such as Calaos and Wink show more limitations, which might hinder their adaptability to new technologies and user demands. Such disparities underscore the importance of choosing a smart home platform that not only meets current needs but also has the potential to adapt to future developments in smart home technology. This analysis is crucial for stakeholders to make informed decisions that align with long-term goals for scalability and adaptability, ensuring that investments in smart home technology remain viable and beneficial as new challenges and opportunities arise within the field.

7 Conclusion

In this thesis, a detailed comparative analysis of twelve major smart home platforms was conducted to understand their architectural differences, functionality, and user interface designs. The study involved evaluating each platform against a set of criteria including adaptability, security features, ease of use, and integration capabilities with other systems and devices. Through rigorous analysis, the research provided a clear snapshot of the current landscape of smart home technologies.

The results of this study revealed significant variability across the different platforms. Some systems excelled in user-friendliness and intuitive design, while others offered superior security features or better integration with broader smart home ecosystems. However, the study also highlighted a common issue among many platforms: a lack of adaptability and customization options, which can hinder their effectiveness in meeting diverse user needs. This points to a gap in the market for more flexible and customizable smart home solutions.

Furthermore, the thesis identified several areas for future work. One key area is the development of more robust security measures that can be easily integrated into existing and new platforms without compromising usability. Another important area for future research is the exploration of more advanced machine learning algorithms to improve the automation capabilities of smart home systems, making them more adaptive and responsive to individual user patterns.

Additionally, there is a need for further investigation into the interoperability of different smart home technologies. As homes become increasingly connected, the ability for various devices and systems to work seamlessly together becomes more crucial. Future studies could explore the development of universal standards or protocols that enhance the compatibility across different platforms and devices.

This thesis contributes to the field of smart home technology by providing a comprehensive overview of the current state of smart home platforms, offering insights that can guide consumers, developers, and researchers. It lays the groundwork for future innovations that prioritize functionality, security, and user experience, paving the way for smarter and more efficient living environments. This work not only enriches our understanding of smart home technologies but also highlights the importance of continued research and development in this area to address emerging challenges and opportunities.

References

[1] Statista, “Smart home - worldwide.” `https://www.statista.com/outlook/cmo/smart-home/worldwide`, 2024. Online; accessed 13.05.2024.

[2] OpenAI, “Chatgpt (gpt-4).” `https://chatgpt.com`, 2024. (April 2024 version) [large language model].

[3] M. Schiefer, “Smart home definition and security threats,” in *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, pp. 114–118, 2015.

[4] A. Babakura, M. N. Sulaiman, N. Mustapha, and T. Perumal, “Hmm-based decision model for smart home environment,” *International Journal of Smart Home*, vol. 8, no. 1, pp. 129–138, 2014.

[5] K. Gram-Hanssen and S. J. Darby, "“home is where the smart is”? evaluating smart home research and approaches against the concept of home," *Energy Research & Social Science*, vol. 37, pp. 94–101, 2018.

[6] Y. Shi, R. Taib, and S. Lichman, “Gesturecam: A smart camera for gesture recognition and gesture-controlled web navigation,” pp. 1 – 6, 01 2007.

[7] O. Ayan and B. Turkay, “Iot-based energy efficiency in smart homes by smart lighting solutions,” in *2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA)*, pp. 1–5, IEEE, 2020.

[8] A. Shaout and M. Theisen, “State of the art-smart doorbell systems,” in *2021 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1–8, IEEE, 2021.

[9] J. Baikerikar, V. Kavathekar, N. Ghavate, R. Sawant, and K. Madan, “Smart door locking mechanism,” in *2021 4th Biennial International Conference on Nascent Technologies in Engineering (ICNTE)*, pp. 1–4, IEEE, 2021.

[10] M. A. Hoque and C. Davidson, “Design and implementation of an iot-based smart home security system,” *International Journal of Networked and Distributed Computing*, vol. 7, no. 2, pp. 85–92, 2019.

[11] Y. Zhai and X. Cheng, “Design of smart home remote monitoring system based on embedded system,” in *2011 IEEE 2nd International Conference on Computing, Control and Industrial Engineering*, vol. 2, pp. 41–44, IEEE, 2011.

[12] A. Wilde, O. Ojuroye, and R. Torah, "Prototyping a voice-controlled smart home hub wirelessly integrated with a wearable device," in *2015 9th International Conference on Sensing Technology (ICST)*, pp. 71–75, IEEE, 2015.

[13] T. Liu, D. Zhang, H. Dai, and T. Wu, "Intelligent modeling and optimization for smart energy hub," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 12, pp. 9898–9908, 2019.

[14] R. Zhong, M. Ma, Y. Zhou, Q. Lin, L. Li, and N. Zhang, "User acceptance of smart home voice assistant: a comparison among younger, middle-aged, and older adults," *Universal Access in the Information Society*, vol. 23, no. 1, pp. 275–292, 2024.

[15] I. Alam, S. Khusro, and M. Naeem, "A review of smart tv: Past, present, and future," in *2017 International Conference on Open Source Systems & Technologies (ICOSST)*, pp. 35–41, IEEE, 2017.

[16] O. Schwartz, E. A. Habets, and S. Gannot, "Low complexity nlms for multiple loudspeaker acoustic echo canceller using relative loudspeaker transfer functions," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 446–450, IEEE, 2020.

[17] D. Natapov, S. J. Castellucci, and I. S. MacKenzie, "Iso 9241-9 evaluation of video game controllers," in *Proceedings of Graphics Interface 2009*, pp. 223–230, Citeseer, 2009.

[18] L. Jiang, D.-Y. Liu, and B. Yang, "Smart home research," in *Proceedings of 2004 international conference on machine learning and cybernetics (IEEE Cat. No. 04EX826)*, vol. 2, pp. 659–663, IEEE, 2004.

[19] M. Ständer, A. Hadjakos, N. Lochschmidt, C. Klos, B. Renner, and M. Mühlhäuser, "A smart kitchen infrastructure," in *2012 IEEE International Symposium on Multimedia*, pp. 96–99, IEEE, 2012.

[20] J. Ojha, Shikha, A. Nayak, V. Goyal, K. Sharma, and S. Reddy, "An analysis of smart kitchen gadgets and a smartphone application for the smart cooker," in *International Conference on Smart Trends for Information Technology and Computer Communications*, pp. 823–837, Springer, 2023.

[21] S. Domnitcheva, "Smart vacuum cleaner–an autonomous location-aware cleaning device," in *Proceedings of the 6th International Conference on Ubiquitous Computing, Tokyo, Japan*, pp. 844–856, Citeseer, 2004.

[22] Y. Zhu, G. Jia, G. Han, Z. Zhou, and M. Guizani, "An nb-iot-based smart trash can system for improved health in smart cities," in *2019 15th International Wireless*

Communications & Mobile Computing Conference (IWCMC), pp. 763–768, IEEE, 2019.

[23] A. Umek, A. Kos, and S. Tomažič, "Smart equipment design challenges for feedback support in sport and rehabilitation," 2017.

[24] Tempo, "Tempo website." `https://tempo.fit/studio`, 2024. Online; accessed 13.05.2024.

[25] T. Meyer and G. Hancke, "Design of a smart sprinkler system," in *TENCON 2015-2015 IEEE Region 10 Conference*, pp. 1–6, IEEE, 2015.

[26] K. Baluprithviraj, R. Harini, M. Janarthanan, and C. Jasodhasree, "Design and development of smart lawn mower," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, pp. 1215–1219, IEEE, 2021.

[27] N. Shaowei, Z. Minling, Z. Zhiwei, L. Xia, L. Zifei, and K. Yuhui, "Design and implementation of smart curtains," in *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)*, pp. 718–722, IEEE, 2023.

[28] F. Shaikh, F. Shaikh, K. Sayed, N. Mittha, and N. Khan, "Smart toilet based on iot," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 248–250, IEEE, 2019.

[29] M. Shaik, A. Mohammed, and G. Sailaja, "Smart water purifier and dispenser for averting spread of covid-19 infection—machine learning approach," in *Contactless Healthcare Facilitation and Commodity Delivery Management During COVID 19 Pandemic*, pp. 95–102, Springer, 2021.

[30] T. Khan, "Design of an autonomous smart shower with sensors and actuators," *Int. J. Embed. Syst. Appl*, vol. 8, pp. 1–17, 2018.

[31] J. Frija-Masson, J. Mullaert, E. Vidal-Petiot, N. Pons-Kerjean, M. Flamant, and M.-P. d'Ortho, "Accuracy of smart scales on weight and body composition: observational study," *JMIR mHealth and uHealth*, vol. 9, no. 4, p. e22487, 2021.

[32] J.-W. Lee, K.-H. Lee, K.-S. Kim, D.-J. Kim, and K. Kim, "Development of smart toothbrush monitoring system for ubiquitous healthcare," in *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 6422–6425, IEEE, 2006.

[33] H. A. Özkan and A. Aybar, "A smart air conditioner in smart home," in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, pp. 1–6, IEEE, 2016.

[34] Y. Wang, W. Wang, Z. Zhang, P. Zhou, and H. Jiang, "Design and research of intelligent air purifier system," in *2020 IEEE International Conference on Mechatronics and Automation (ICMA)*, pp. 1822–1826, IEEE, 2020.

[35] A. S. Musleh, M. Debouza, and M. Farook, "Design and implementation of smart plug: An internet of things (iot) approach," in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pp. 1–4, IEEE, 2017.

[36] L. Özgür, V. K. Akram, M. Challenger, and O. Dağdeviren, "An iot based smart thermostat," in *2018 5th International Conference on Electrical and Electronic Engineering (ICEEE)*, pp. 252–256, Ieee, 2018.

[37] M. Laurino, L. Arcarisi, N. Carbonaro, A. Gemignani, D. Menicucci, and A. Tognetti, "A smart bed for non-obtrusive sleep analysis in real world context," *Ieee Access*, vol. 8, pp. 45664–45673, 2020.

[38] M. M. Yusri, S. Kasim, R. Hassan, Z. Abdullah, H. Ruslai, K. Jahidin, and M. S. Arshad, "Smart mirror for smart life," in *2017 6th ICT International Student Project Conference (ICT-ISPC)*, pp. 1–5, IEEE, 2017.

[39] A. Alexa, "Amazon alexa website." `developer.amazon.com/alexa`, 2024. Online; accessed 13.05.2024.

[40] GoogleNest, "Google nest website." `https://store.google.com/gb/category/connected_home?hl=en-GB`, 2024. Online; accessed 13.05.2024.

[41] AppleHomeKit, "Apple homekit website." `https://www.developer.apple.com/homekit`, 2024. Online; accessed 13.05.2024.

[42] Domoticz, "Domoticz website." `https://www.domoticz.com`, 2024. Online; accessed 13.05.2024.

[43] Calaos, "Calaos website." `https://www.calaos.fr`, 2024. Online; accessed 13.05.2024.

[44] OpenMotics(Renson), "Openmotics (renson) website." `https://www.openmotics.com`, 2024. Online; accessed 13.05.2024.

[45] HomeGenie, "Homegenie website." `https://www.genielabs.github.io/HomeGenie`, 2024. Online; accessed 13.05.2024.

[46] SamsungSmartThings, "Samsung smartthings website." `https://www.samsung.com/us/smart-home`, 2024. Online; accessed 13.05.2024.

[47] Control4, "Control4 website." https://www.control4.com, 2024. Online; accessed 13.05.2024.

[48] Wink, "Wink website." https://www.wink.com, 2024. Online; accessed 13.05.2024.

[49] HomeAssistant, "Home assistant website." https://www.home-assistant.io, 2024. Online; accessed 13.05.2024.

[50] MarketsandMarkets, "Smart home market size, share, statistics industry growth analysis report by product (lighting control, security access control, hvac control, smart speaker, smart kitchen and smart furniture), software and services, sales channel and region - global forecast to 2028." https://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html, 2023. Online; accessed 13.05.2024.

[51] ABCnews, "Ring security camera hacks see homeowners subjected to racial abuse, ransom demands." https://abcnews.go.com/US/ring-security-camera-hacks-homeowners-subjected-racial-abuse/story?id=67679790, 2019. Online; accessed 13.05.2024.

[52] G. Vojkovic, M. Milenkovic, and T. Katulić, "Iot and smart home data breach risks from the perspective of croatian data protection and information security law," 09 2019.

[53] A. N. Gollu and J. Kumar, *Wireless Protocols: Wi-Fi SON, Bluetooth, ZigBee, Z-Wave, and Wi-Fi*, pp. 229–239. 01 2019.

[54] N. A. N. M. Ashril, D. P. Dahnil, and S. Abdullah, "Wi-fi based smart home prototype development," in *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, pp. 540–543, 2019.

[55] S. Zhihua, "Design of smart home system based on zigbee," in *2016 International Conference on Robots Intelligent System (ICRIS)*, pp. 167–170, 2016.

[56] C. K. Nkuba, S. Kim, S. Dietrich, and H. Lee, "Riding the iot wave with vfuzz: Discovering security flaws in smart homes," *IEEE Access*, vol. 10, pp. 1775–1789, 2022.

[57] T. M. Triet Pham and J. Yang, "Exploring bluetooth communication protocols in internet-of-things software development," in *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pp. 792–793, 2020.

[58] C.-H. Lu, “Improving system extensibility via an iot-interoperable platform for dynamic smart homes,” in *2017 International Conference on Applied System Innovation (ICASI)*, pp. 1300–1303, 2017.

Appendix

I. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Aleksandra Sergeeva**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Comprehensive survey of smart home technologies,

   supervised by Chinmaya Kumar Dehury.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Aleksandra Sergeeva
15/05/2024