Evaluation of a concrete IoT System: Apple Homekit and Amazon Echo with Alexa IoT Framework

Keyshav Mor(1237978)
Anoop Krishna Ravattu(1336444)
For the course : 2IMN15 Internet of Things(Q2)
Department of Mathematics and Computer Science
Eindhoven University Technology
Academic Year 2018-2019

***Abstract*—The following report discusses Internet of Things (IoT), their role in Home automation and two relevant technologies namely the Apple Homekit and Amazon Echo and Alexa based IoT systems. The different aspects like componets, their functionalities, deployment views, control and data flows, failure models, privacy and security concerns are also studied and presented. Finally, a case study of a possible interaction interface between these two technologies and its implications are presented.**

Keywords—IoT,Home Automation, Apple Homekit, Amazon Echo, Amazon Alexa, Siri, MFi, Alexa skills server, iCloud, WiFi, IP, Zigbee, bridges, gateway, functionalities, life cycles, privacy,security.

I. Internet of Things:What is it?

The IEEE defines Internet of Things as follows: "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet using standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration."[1]

II. Internet of Things in Home Automation

Advent of faster and more efficient communication protocols like WiFi, 4G and 5G along with the reduction in power consumption, space and cost requirements of data storage in data farms has resulted in development of more intelligent and aware Artificial intelligence systems. This has prompted major technology companies like Google, Amazon and Apple have launched their own IoT Home Automation platforms namely Nest, Alexa and Homekit respectively. In this article, our focus would be upon Amazon's Alexa and Apple's Homekit Automation systems.

III. Apple Homekit: What is it and how does it work?

Apple Homekit is the flagship home automation framework developed by Apple Inc. for providing home automation features for iOS and Mac OS device users. The devices which are compatible with Apple Homekit are marketed under the classification "Works with Apple Homekit". The voice assistant "Siri" can be used to execute voice commands which have a wakeup command "Hey, Siri!" These commands can be of the type "Hey Siri, please turn on the ceiling bulb in my bedroom." Here, "Ceiling Bulb" is an accessory in the room called "Bedroom" which could be located in the zone "Upstairs" in the one of Homekit configured home called "Amsterdam Home". Homekit API is used by accessory manufacturers to develop devices compatible with Homekit and Homekit Accessory Protocol (HAP). [10][11]

Multiple Homes, Zones, Rooms and Accessories with unique names and Apple certified MFi (Made for iPhone/iPad/iPad) ID's can be configured in the Home app of single Apple ID. As mentioned above, one can either use Siri or the "Home" App on iOS and Mac OS to control the accessories. Siri can be controlled via Mac computers, iOS devices like iPhone, iPad, Apple TV and Homepod, which is a smart speaker with Siri.To control the accessories remotely from outside of the house, one has to configure a "Home Hub" which can be either an iPad, a Homepod or an Apple TV. The controlling device (iPhone,iPad, Mac) has to be connected to the WiFi access point to which the accessories or the accessories gateways and bridges are also connected for Zigbee accessories. Accessories with Bluetooth can be controlled BLE from Apple devices. [10][11]

It is possible to set "Scenes" based on certain events like Morning, Evening, Night, Summer, Winter etc. can be set to simultaneously activate and control a group of accessories. Similarly, "Automations" based on location of primary user(s), time and certain triggers for ex. Opening and closing the door, occupancy, activating certain accessory etc. can be set to ensure optimized accessory performance and energy consumption. Home(s) in Homekit is divided into zones, rooms and accessories in a hierarchal manne [10][11]

A. Apple Homekit Ecosystem, its components and their functionalities

The Apple Homekit ecosystem consists of various components which help in fulfilling its functions. These are mentioned below along with their functional capabilities.

Apple Devices (iPhone/iPad/Apple TV/Homepod/Mac): The Apple devices are central to controlling Apple Homekit based home automations through the Home application or Siri.

Home Hub (Apple TV/iPad/Homepod): Home hubs are again Apple iOS devices which have to be connected to WiFi network same as accessories and must have internet to help primary and guest users to control the home remotely.

Home App: The Home app is set up in one of the audio-visually interactive Apple devices along with its zones, rooms, accessories, scenes and automations, such that all the devices sharing that device's Apple ID can control the accessories remotely or in the house.

Siri: Siri is the voice assistant which activates accessories, scenes and automations which care configured in the Home app. Activated by the wake phrase "Hey Siri!", it uses the data stored in the iCloud to fulfill the tasks demanded of it.

iCloud: iCloud, configured uniquely for each Apple ID stores the unique name and MFi licensed ID of each Homekit device along with the different homes, zones, rooms, scenes and automations configured in the Home App. All the voice and touch-screen commands are routed here over IP for processing and back to generate tangible actions. Analytics can also be generated through the data stored in the iCloud.

WiFi Access Point: The WiFi Access point is the WiFi router placed within the house and to which all your Apple devices, accessories, bridges and gateways are connected. The communication with the cloud is facilitated through this router which transfers the encrypted data packets from Apple devices and accessories to the iCloud for processing over the IP and also helps in communicating the encrypted data from iCloud to Apple devices and accessories.

Siri Shortcuts: Siri Shortcuts is an application on top of the Siri framework which makes it easier to trigger multiple accessories, scenes, automations in sequence or event-triggered manner through just a single voice command.

Homekit API: The Homekit API is the API provided by Apple for third party developers to develop software applications for accessories to be made compatible with Homekit framework.

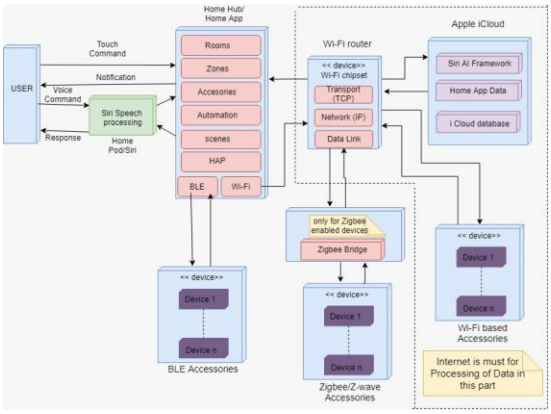
Homekit Accessory Protocol (HAP): Apple's proprietary communication protocol stack to communicate with third party accessories which is implemented over BLE and IP.

MFi Certification: MFi certification is the license required by third party accessory developers in order to ensure that their devices comply with the Apple security, privacy and encryption standards. Initially a hardware coprocessor based certification, now it is available as a software API for third-party developers to make the devices Homekit compatible.

Accessories: Accessories are the devices being controlled through the Homekit interface. These accessories can be anything like Smart Locks, Smart Curtains, brightness and colour controllable smart bulbs, thermostats etc. These could also be smart switches to control incompatible or differently communicating accessories. These accessories can connect either via Bluetooth, WiFi, ZigBee or Z-Wave and sometimes require bridges between the WiFi router and them.

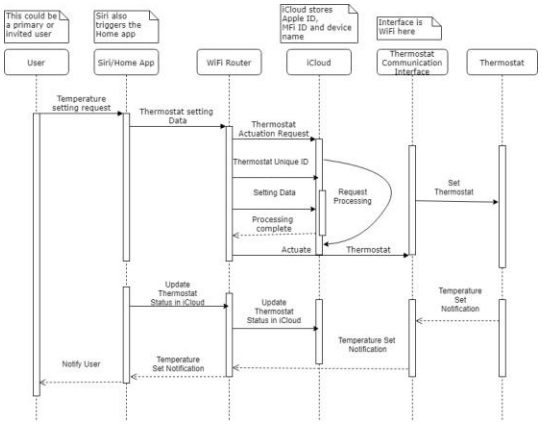
Zigbee Bridges & Gateways: Bridges and gateways are needed when Apple devices wish to control incompatible or differently communicating devices. These can either for single accessories or a bunch of accessories mapped on the Home app, but using a different communication protocol other than WiFi like Zigbee.

B. Apple Homekit Deployment View and its Control & Data Flow

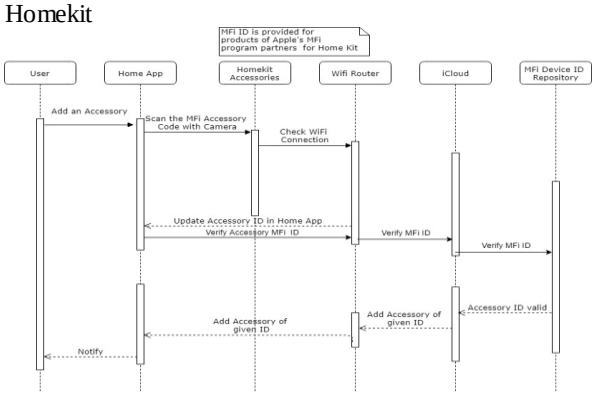


APPENDIX A. Deployment View of Apple Homekit Home Automation System.

It should be noted here that the Zigbee bridge does require a WiFi connection but no internet.



APPENDIX B. Sequence diagram explaining control and data flow for a Thermostat application based on Apple Homekit



APPENDIX C. Sequence Diagram explaining the process of adding an accessory in the Apple Homekit network

C. Apple Homekit Fault Analysis

Internet Connection goes down: The Apple Homekit implements the HAP for communication with its accessories. HAP is built on top of IP and BLE. The IP

support is provided through WiFi which enables data exchange between the automated home and iCloud. If the internet connection goes down, there is no single hop or remote communication between the Home Hub or Apple devices, the iCloud and the accessories. In such cases, nothing much can be done except for preparing for such a scenario by buying Bluetooth, Zigbee and Z-Wave supported accessories like Elgato Eve weather sensor, Kwikset 916 Electronic Deadbolt Lock, Elgato Eva room sensor, Elgato wireless door and window sensor, Elgato Eve aqua water controller, Philips Hue Bridge, Fibaro Bridge and Homee Bridge etc. This will ensure that these accessories can be controlled in absence of internet, however seriously imparing additional features like fine grained control and data analytics.

A Device goes down: Home automation systems like Apple Homekit do not have a single point of failure, they have multiple points of failure because of multiple components present in their ecosystem. Thus we have to consider multiple device failure and their implications.

- **Home Hub (Apple Tv/iPad/Homepod):** The Home Hub is extremely critical for remote access. If these devices malfunction, have virulent software or have no internet connection, one cannot access their home remotely or even possibly shut out from their house by hackers. They must be repaired or replaced.
- **iCloud:** iCloud can either be inaccessible due to lack of internet as mentioned previously or its servers in data farms could be inaccessible for some software/hardware fault or its data could be corrupted. This could possibly delete existing data, derail home automation by not allowing processing of input commands or cause incorrect data processing. This could also expose data for malignant activities.
- **Siri and Home App software:** Siri depends on iCloud for data and its overlying AI algorithm for accurate command processing. Same is the case with the Home App. If their local or cloud based software malfunctions, incorrect processing of commands, deletion of data and possibly passive reactions to commands may occur. Service request to development center must be forwarded.
- **WiFi Router:** Malfunction of Wi-Fi router cuts off Internet connection and connection to bridges or accessories. Thus, for successful operations they must be repaired or replaced.
- **Zigbee Bridge:** Malfunction of the Zigbee bridges cuts off the accessories and their connection with the WiFi router, Home Hub and other Apple devices. Thus, for successful operations they must be repaired or replaced.
- **Accessories:** When accessories malfunction, the purpose of home automation is defeated. Getting accurate data and actuating is hampered. This could be due to lack of power supply or hardware/software faults associated with the accessory. Servicing and replacement are possible options.

Conflicting commands to Siri/Home App: Conflicting commands to Siri/Home app can be classified in two ways: a) Multiple people speaking to Siri b) Contradicting commands to Home App.

a) **Multiple people speaking to Siri:** If multiple people are speaking to Sir, the first person uttering the wake up phrase “Hey Siri!” is considered to be primary user and his/her voice is processed. The other person is ignored. If the commands given are contrary to preset scenes, automation settings for ex. Turning on heater in a Summer “scene” , Home App prompts for confirmation by the user, and the request is processed and scene/automation is deactivated and overridden to fulfill the request.

b) **Contradicting commands to Home App:** Contradicting commands to Home App and Home Hub are processed in the same way as mentioned above

D. Privacy and Security Analysis of Homekit

Privacy: HomeKit uses iCould and iOS for safely synchronizing data.Apple claims that is uses end-to-end encryption between all the communications between its devices and its iCloud which stores data for Homekit only for a period of 6 months. It also claims that it does not share data with third party apps but it uses an unidentified data pool in assessing how its users use the services to improve its services particularly Siri. Only apps for configuration and automation are allowed. Apple does not know which devices we are controlling from where and when. Siri only associates our devices with some unique ID that is not our Apple ID. Data of the home is stored in a keychain encrypted between devices even remotely. Location-based automations are triggered only through Homekit. 2 factor authentication is a must to access Homekit remotely and is also recommended while accessing iCloud.

When we invite another user into our HomeKit the same security mechanisms just like when adding a HomeKit accessory are used. The original home user authenticates the new user with the devices so that the accessories can accept the new user. Siri receives anonymous information from our voice to process HomeKit voice commands. HomeKit IP cameras also follow the encryption mechanism mentioned above. The camera viewing apps follow a special decryption policy so that they cannot access, store the stream capture or even capture screenshots from the video stream.

Home Hubs allows us to remotely access our HomeKit and iCloud with a 2factor authentication. When we access our homes remotely through iCloud, information on which devices we control and these notifications are opaque to even Apple.

On enabling Siri, a random ID is generated tied to our Apple device. Once we disable Siri, this ID is replaced by a new ID and all data is deleted on the device. [6][7][8]

Security: Authentication between Homekit and iOS devices is based on Ed25519 17 public-private key signature. For each user and accessory in the HomeKit framework, an ed25519 key pair is generated for authentication purposes. In the authentication process, keys are exchanged using Secure Remote Password protocol, in which a 8-digit code from the manufacturer must be entered by the user. Keys are encrypted using ChaCha20-Poly1305 AEAD with HKDF-SHA-512-derived keys. The accessory's MFi certification is also verified during setup. These are long- term keys. For each communication session, a temporary key is encrypted with HKDF-SHA-512 derived keys based on per-session Curve25519 keys. Applications must user's permissions to get access to their home data. Only trusted code can run in Apple devices. AES 256 encryption protocol is included in an engine on the DMA path between flash and processor to provide highly efficient encryption. Each Apple device has a unique device Id which is AES 256-bit key which allows data to be identified with one device only. All other cryptographic keys are created by the system's random number generator using an algorithm like CTR_DRBG. TL S/DTL S with AES-128-GCM and SHA-256 are used to secure HTTP communication. In HomeKit, the long-term keys, used for secure communications are stored in user's devices which cannot be seen by even Apple. [6][7][8]

E. Lifecycle of Apple Homekit

Lifecycle of Apple Homekit components and system can be divided into three parts: physical devices, software components and the systemas a whole.

Physical Devices: Physical devices like Apple Devices iPhone, iPad, Homepod, Apple TV or devices like Wi-Fi router and accessories all follow a particular life cycle. All these components go through the phases of requirement evaluation, specification formalization, design, manufacturing, testing and deployment through marketing of these products. Their respective manufacturers are responsible for these stages including deployment. Accessories compatible with Homekit also have an additional process of being compliant with MFi licensing certification. This is an additional stage for them. The customers buying them forms the part of deployment followed by installment and configuration as per the requirements of the user to connect them to the network, adding ID's to devices in case of accessories and adding them to the Apple ID based cloud network. Repair and maintenance is responsibility of manufacturer or its partners if warranty is valid else it is the responsibility of the user. After arrival of a new and better similar devices or after malfunctioning outside warranty, these physical devices are decommissioned for newer devices. The stakeholders are manufacturers, retailers, regulators, servicing agencies and the users.

Software Components: Software components for the likes of Apple products iPhone, iPad, Siri, Homepod, Apple TV, iCloud, Home App, iOS, Mac and accessories all follow a different life cycle than physical components. All these components go through the phases of requirement evaluation, specification formalization, design, software deveopment, testing and deployment through marketing of these products but also through updates and revisions. Their respective developing organisations and users are responsible for updates. Accessories compatible with Homekit also have an additional process of being compliant with MFi licensing certification which is a combination of both software and hardware encryption processes. This is an additional stage for them. The customers may buy the software and download/subscribe to it for services requiring voluntary participation but sometimes these software come as a part of a system like accessories or WiFi router and one does not need to buy such software but only their devices. Home App is the central app with no extra applications needed and this comes as a part of Apple iOS and Mac devices. Execution of these services provided by the software are triggered by the user, which provide the service or display an error in case of inability and go back to to dormant state. Services are provided as long as the software is valid and compatible with its environment like the accessories or the devices. Updates are regularly provided by the developer or the manufacturer. A new software or an updates replaces the old software or end in the old software's termination. The stakeholders are software designers and developers, testers, users and update managers.

Applications: Applications follows a combination of the aspects of software and physical components' life cycle along with some additions. In addition to the aspects the software and physical component lifecycle, the Homekit application lifecycle involves addition of devices, services, scenes and automations to its framework, commissioning services and devices, requesting services out of them and decommissioning these services. Addition of services and applications in the Homekit is a part of deployment which has to be configured by the user. Execution is also carried out by the user like switching on and off of an application. Reconfiguration of a Homekit accessory, scenes and automations are also carried out by the user. Termination of an application happens either due to incompatibility with the software, physical device malfunction or decommissioning by the user. The stakeholders are users, power providers, cloud managers, network providers and installation agencies.

IV. AMAZON ECHO WITH ALEXA : WHAT ISIT AND HOW DOES IT WORK?

Amazon Alexa, is an intelligent digital personal assistant which can be accessed by using a wide range of Amazon devices like Amazon's Echo, Dot and Show. These devices are used to register the user's voice command and convey them to the Alexa service whereupon Alexa service gives an appropriate response back. Using this service an user can perform a variety of useful tasks like streaming music, retrieving real-time weather and traffic information, purchasing products through Amazon, controlling the smart-home devices and a lots of other tasks. However this report mainly aims at using Alexa for controlling the smart-home devices.

A. Amazon Echo based Home Automation, its components and functionalites

When Alexa voice service is accessed via Echo, there are a number of system components that work together to produce a meaningful response for a given voice command. These include the user controlled devices like Echo, Echo Plus or a

Smart Phone. In addition to these we have hubs which can be one of the above mentioned device or a Zigbee hub. The accessories can be smart home devices like Light or Thermostat which acts like sensors and actuators for the system. Alexa cloud is the cloud storage which helps in storing the encrypted data and it also acts as the processing unit for the entire system. Amazon skill server is used to enable a default skill or a third party skill. The Wi-Fi router is connected to user controlled device and provides an IP uplink to Alexa Cloud. As Alexa is an open source platform, Bridges and gateways helps in communication among the devices. Smart plugs can also be used which can convert a normal device into smart device by enabling internet.

Echo: Echo is the device which basically provides the speech-based interface to the user. The user gives an instruction/command in form of speech with a wake word ("Alexa'') and it responds back with an appropriate response. So the main functionality of Echo is *communication (UI as well***)** between the user and the smart-home system.

Alexa Application: Amazon provides a mobile application which is used for changing the Alexa setting like language, preferences. Whenever a user interacts with Alexa, the cloud service updates the information relevant to the interaction and an audio recording here. Moreover, the user can have access to all the previous interactions here and can delete the interaction if he wishes to. This is used for both *Vertical and Horizontal Analytics* of the system.

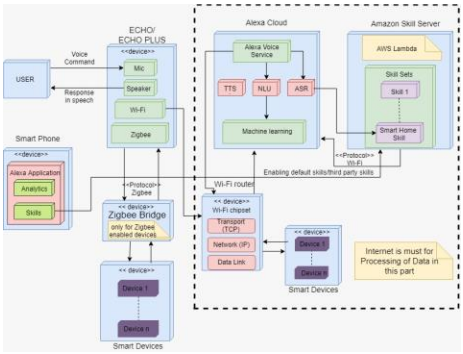
Alexa Voice Service (AVS): Alexa voice service is a (software component) provided by Amazon which helps in forwarding the instructions given by a user.

Alexa Cloud: Alexa Cloud receives the voice from the Echo and is responsible Automatic Speech Recognition (ASR), Natural Language Understanding (NLU) and Machine learning. Machine learning is used to improve the performance of Alexa by feeding the audio clips to the neural networks of Alexa so that it can analyze the patterns and thereby making Alexa more smarter (providing more accurate results) for the User. Moreover Text To Speech (TTS) is also performed in Alexa cloud which is responsible for the response (in speech) for a given command. Once the given instruction is analyzed properly in the cloud, it is then given to the Amazon skill server. And when the cloud service receives response from this skill server, it conveys the message back to the Echo device. Moreover, Cloud is the place where every Audio recordings of the interaction with Alexa is stored and therefore Alexa cloud is acting as both *Storage* and *Application Logic*.

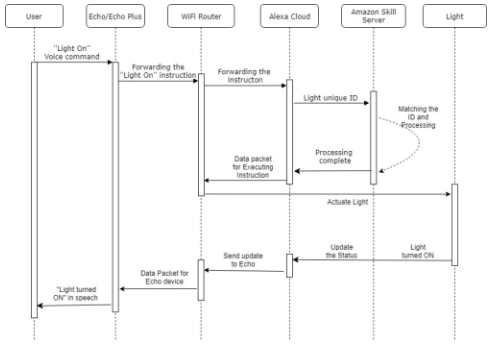
Skill Server: After the command/instruction is processed in the cloud it is then sent to the Amazon skill server where the appropriate skills are searched for and then selected. For functioning of Smart-Home the smart home skill should be enabled and this can be done using the Alexa Application mentioned above. Once the skill set is found and based on the data packet (device ID) that has been received, it is then redirected to the specific Smart device cloud. One big advantage of Amazon Skill server is that if you want an additional skill which is not in the default skills provided by Amazon, You can create your own skill using AWS Lambda and this can be added to the skill server. The Skill server acts as *application logic with Data/information*

Zigbee Bridge: Zigbee Bridge is mainly used for *communication* between Echo and Zigbee enabled devices.

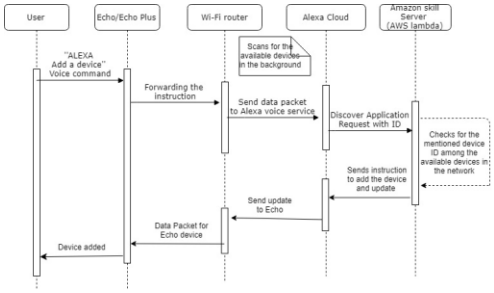
B. Amazon Echo Home Automation Deployment View and its Control & Data Flow



APPENDIX D. Deployment view of Amazon Echo based Home Automation system



APPENDIX E Sequence Diagram explaining the application of light activation in Alexa Home Automation



APPENDIX F Sequence diagram demonstrating addition of an accessory in Amazon Alexa's IoT framework via Amazon Echo

C. Amazon Echo with Alexa based Home Automation Fault Analysis

When the internet connection is lost:

As shown in deployment view, Echo (in particular Alexa) needs internet to perform any actions. If there is no internet, the command cannot reach Alexa cloud and therefore it can't be executed. However, with Echo Plus (latest line of devices for Alexa), a local voice control will take its Zigbee element and link it with other Smart devices (Zigbee enabled) and lets you perform the basic functions (like turning on/off) even when there is no internet.

Users giving conflicting commands:

Whenever Alexa receives conflicting commands, it sets priority (using the concept of beam forwarding). For example, Let us consider 2 users, An adult and his child.

When the adult is trying to order something on Amazon and his kid suddenly says "Alexa order 10000 Legos", It will ignore the Kid's command as the adult was the first to give instruction, However, It will later ask about kid's instruction as well.

When the device goes down:

For this, a full fault model analysis is done for the each component that is mentioned in the deployment diagram and the solution for it is also mentioned below.

Echo and Alexa: As Echo is the device with which you are operating the smart home system and if it goes down you can't do much about it except resetting the device or calling the Technician. But, Thanks to Amazon, Alexa is made available for Smart Phones and PC's. Once we login with the Alexa in your PC, you can perform most of the functions. If Alexa goes down as well, we have the backup option of using the original Smart Hub which is designed for the devices.

Wi-Fi Router: When the Wi-Fi router is not working (which is the same case when the internet is lost) Alexa takes control of Zigbee enabled device by creating a local bridge and can function.

Alexa Cloud: Even though when the internet is available and the Alexa Cloud is not working, smart home system functionalities cannot work its full capacity and the solution for this is same as the Wi-Fi router.

Zigbee Bridge: Even though when the Zigbee hub is not working, the Smart home system functionalities does not get affected as long as there is internet.

Mobile Application: When the Application (of Alexa) goes down, it really doesn't affect that much because it is mainly used for analytics and the application can be easily re-installed.

Skill Server: Most of the time, The Amazon Skill server is never down as there are a lot of technical teams working 24/7 to troubleshoot a problem if it arises. However if the Skill Server is down, the solution is same as the Wi-Fi router.

Smart Device: If the device is down (or not responding), when given a command, Alexa will simply say the device is not responding and you can repair the device or get a new one based on its condition.

D. Privacy and Security Analysis of Amazon Echo Home Automation System

Security emphasizes on Alexa taking commands/instructions only from *registered* user's for that particular account whereas privacy is concerned with the third party not having the user's personal data (like daily routine, interests etc.).

When it comes to the security, Alexa is not up to the mark because of its usage of single factor authentication method (the password being just saying ''Alexa'') [2]. Alexa does not actually need a user (in person) saying the command, So an Echo device can be activated by simply hearing the wake word (even from an anonymous source). This results in a high level security issue. If the local (home) network is compromised i.e. when an third party device is connected to the network he can simply connect to the TV or a Bluetooth speaker and instruct the Alexa to perform some tasks and Alexa does these tasks without any hesitation, this is clearly explained in [2], where an experiment has been setup in a controlled environment and an anonymous user gives command through a Bluetooth speaker to (Echo) Alexa and the Echo executes the instruction. This is the same case for purchasing products through Amazon where an anonymous user can order the product with the actual User's credentials. However, the technical team at Amazon tried to come up with a solution by using a 4-digit pin but it was not effective because the order does not get cancelled after a number of wrong attempts [3] . So, the best way to secure an Echo device is to turn off the microphone of Echo when leaving or make sure that the Home/Home network is secured so that an intruder may not gain access to it. The additional step for security is by using a Virtual Security (VS button) so that the Echo can't activate unless a user is present in the room and this is clearly explained in [2]

Coming to the privacy issues, It is a good thing that the Echo device doesn't store the data locally. In fact it sends the data in the form of HTTP request to the Amazon cloud for processing so it will be difficult for the third party's to hack into the cloud and get the personal information. However if the device is not secured properly (if a person can gain physical access to the device) they can perform a ***physical root access***[5] and can get control over the personal data and even can install malware without any evidence. Again the solution for this is to make the home secure so that no one can physically access the Echo. But what if Amazon was forced to hand over your personal data? This is what happened in Kansas case [5]. Amazon was forced to hand over personal data in a legal case. However Amazon refused to hand over the personal data but eventually it gave in which is a violation of privacy. Amazon keeps track of the voice recordings so that it can be given to the neural network of Alexa and by using the concept of machine learning so that it becomes more user friendly. These audio clips can't be accessed by anyone without your consent because they are encrypted by Secured Socket Layers (SSL) when sent to the cloud [5]. However, if one can still feel that his/her privacy might be violated, the audio clips from the cloud can be deleted through the Alexa application.

E. Lifecycle of Amazon Echo Home Automation Components

When compared to the lifecycle of Apple Homekit, the lifecycle of Alexa and Echo is somewhat typical because of its accessibility to third party devices. Lifecycle of Alexa and Echo can be divided into three parts: physical devices, software components and the Applications

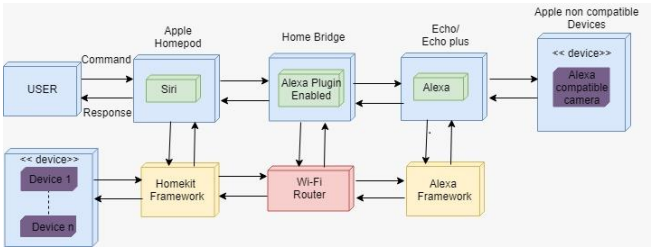
Physical Devices: Devices like Echo/Echo plus, Wi-Fi router, smart phone, smart home devices , PC's (Alexa can be accessed through personal computers), are the crucial physical devices in working of Alexa and Echo. These devices more or less follow the same pattern in life cycles. All of these devices have to go through the phases of specification, design, production, testing and deployment. The main stake holders are the manufacturers for their respective stages. Once the deployment is done it is system integrator who has to take care of mapping the functionalities. The stakeholders differ in each case. For example, it is not the manufacturer who is responsible for the Wi-Fi router once it is deployed. The data provider is the

main stakeholder who is responsible for providing the internet. Although, Repair and Maintenance is the responsibility of the manufacturer if the devices were given a warranty else is the responsibility of the user. With the rapid advancement in technology, there are high chances of new devices or the same devices with the better performance made available. Then these physical devices are decommissioned for new devices. The policy regulators and the manufacturers are the main stake holders at this stage.

Software Components: Most of the physical devices are associated with the software components like Alexa for Echo and OS for smart phone. Software components Alexa cloud, Amazon skill server follow a slightly different life cycle than the physical components. All these components go through the phases of requirement evaluation, specification formalization, design, software development, testing and deployment. In addition this, it also has to go through certification for certain standards. The customers can buy software or download, it but most of the time physical device comes with software component. For example, if you buy an Echo, it comes pre-loaded with Alexa. There are cases where we have to download the software as well (downloading Alexa for smart phone). The respective developing organization and users are responsible for software updates. Updates are regularly provided by the manufacturer or administrator but it is the responsibility of the consumer to update the software in time. The main stake holders are software developers, testers, users and administrators.

Applications: For an application to happen, it requires both physical and software components to function accordingly and hence it follows both the life cycles of physical devices and software components. In addition to the aspects of the software and physical components, Echo life cycle involves addition of devices, services and automation to its framework. Addition of these services can be considered as deployment but the main stake holders is user as he has to decide which device has to be added. Execution of the actions like switching ON and OFF are also handled by the user. Termination of an application happens either due to incompatibility with the software or device malfunctioning. The main stake holders are data providers, users and technicians.

F. Interaction between Apple Homekit and Amazon Alexa



APPENDIX G. Deployment view of a combined Apple Homekit and Amazon Echo+Alexa based Home Automation system using a Homebridge to control an Alexa based IP Camera

Apple Homekit and Amazon Echo+Alexa based IoT systems are mutually incompatible. Apple considers that the privacy of user data is of paramount importance, a philosophy inconsistent with Amazon and Google who actively provide user data to third party apps. Apple Homekit is closed to developers as they must be a part of MFi program to utilize Apple encryptions, HAP and Apple Homekit APIs, whereas Alexa skills are open-source. Since the philosophies do not match, most of the accessories used in Alexa framework are not compatible with "Works with Homekit" framework.

In order to use these technologies such that they communicate with each other, an open-source server called Homebridge[9][10] with an Alexa plug-in is used which converts Homekit messages to Alexa Skills compatible instruction to control an Alexa compatible accessory, in this case an IP Camera. It can be implemented on a PC, A laptop or even a Raspberry Pi connected to the Internet via a WiFi access point shared between Homekit, Echo and the Raspberry Pi.

The Homebridge ensures that the privacy and security aspects of Homekit are maintained while controlling an incompatible accessory meant for Alexa framework. Naturally, an additional hardware is needed. It must be noted that the lifecycle of the individual Homekit and Alexa framework remains unchanged.

The data privacy status of the Alexa compatible IP camera is also unchanged same as that of Homekit's privacy and security. The camera remains susceptible to attack while the Homebridge shielding the Homekit if it implements encryptions enabled in Apple devices. There could be security issues between Homebridge and Alexa which should be studied in detail.

The stake holders in this application are the users, the open-source Homebridge repository developers, Alexa and Homekit framework developers and managers and network security managers.

Homebridge should be added both in the Home App and also as an Alexa skill. Although it does not require Echo, Echo connected to Homebridge provides an easy mechanism to control the IP Camera. Control from Alexa to Homekit is not possible as Alexa is configured as an "Accessory" of Homekit framework. Because of this, accessories in Alexa domain can be controlled via Homekit using keywords specific to Alexa, usually via Siri.

Functionality of the application is to integrate Homekit and Alexa frameworks without the user having to spend extra money on either Apple or Amazon compatible products. Fine grained control is possible depending on the Siri but the accessory by itself is not visible on the Home app as only Alexa appears as an accessory.

Control and Data flow involves both the iCloud and Alexa skills server. This means that there will be latency in the application as it involves multiple nodes. Also it is not clear if the stream of the camera will be visible on an Apple device however the part of controlling the IP camera or other such accessories is well defined.

CONCLUSION

Thus, we have studied Amazon Echo based Home Automation system supported by Amazon Alexa framework and the Apple Homekit home automation system along with their respective functionalities, components, lifecycles, deployment views, control flows, data flows. Their fault models were also covered along with their privacy and security features. In the end, we studied interaction between Amazon Alexa and Apple Homekit in a home automation environment and looked at how it affects theirs life cycles and functionalities.

REFERENCES

[1] Steiner, W., Bonomi, F., & Kopetz, H. (2014). Towards synchronous deterministic channels for the Internet of Things. 2014 IEEE World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2014.6803205

[2] Xinyu Lei_, Guan-Hua Tu_, Alex X. Liu_, Kamran Ali_, Chi-Yu Liy, Tian Xie_' The Insecurity of Home Digital Voice Assistants– Amazon Alexa as a Case Study'.

[3] William Haack, Madeleine Severance, Michael Wallace, Jeremy Wohlwend 'Security Analysis of the Amazon Echo'.

[4] Amazon Echo vs. Google Home: Which Voice Controlled Speaker Is Best for You? (n.d.). Retrieved from https://thewirecutter.com/reviews/amazon-echo-vs-google-home/

[5] Jackson, C. And Orebaugh, A. (2018) 'A study of security and privacy issues associated with the Amazon Echo', *Int. J. Internet of Things and Cyber-Assurance*, Vol. 1, No. 1, pp.91–100.

[6] Apple and Your Security and Privacy. (2018, August 06). Retrieved from https://www.smartenlight.com/apple-and-your-security-and-privacy/

[7] Internet of Things (IoT): Security Analysis & Security Protocol CoAP. (2017). *International Journal of Recent Trends in Engineering and Research*, *3*(3), 417-425. doi:10.23883/ijrter.2017.3126.6ibua

[8] Sturgess, Jack & Nurse, Jason & Zhao, Jun. (2018). A capability-oriented approach to assessing privacy risk in smart home ecosystems. 10.1049/cp.2018.0037.

[9] Sargent, M. (2017, April 07). How to connect incompatible accessories to HomeKit using Homebridge. Retrieved from https://www.imore.com/how-connect-non-homekit-devices-homekit-using-homebridge

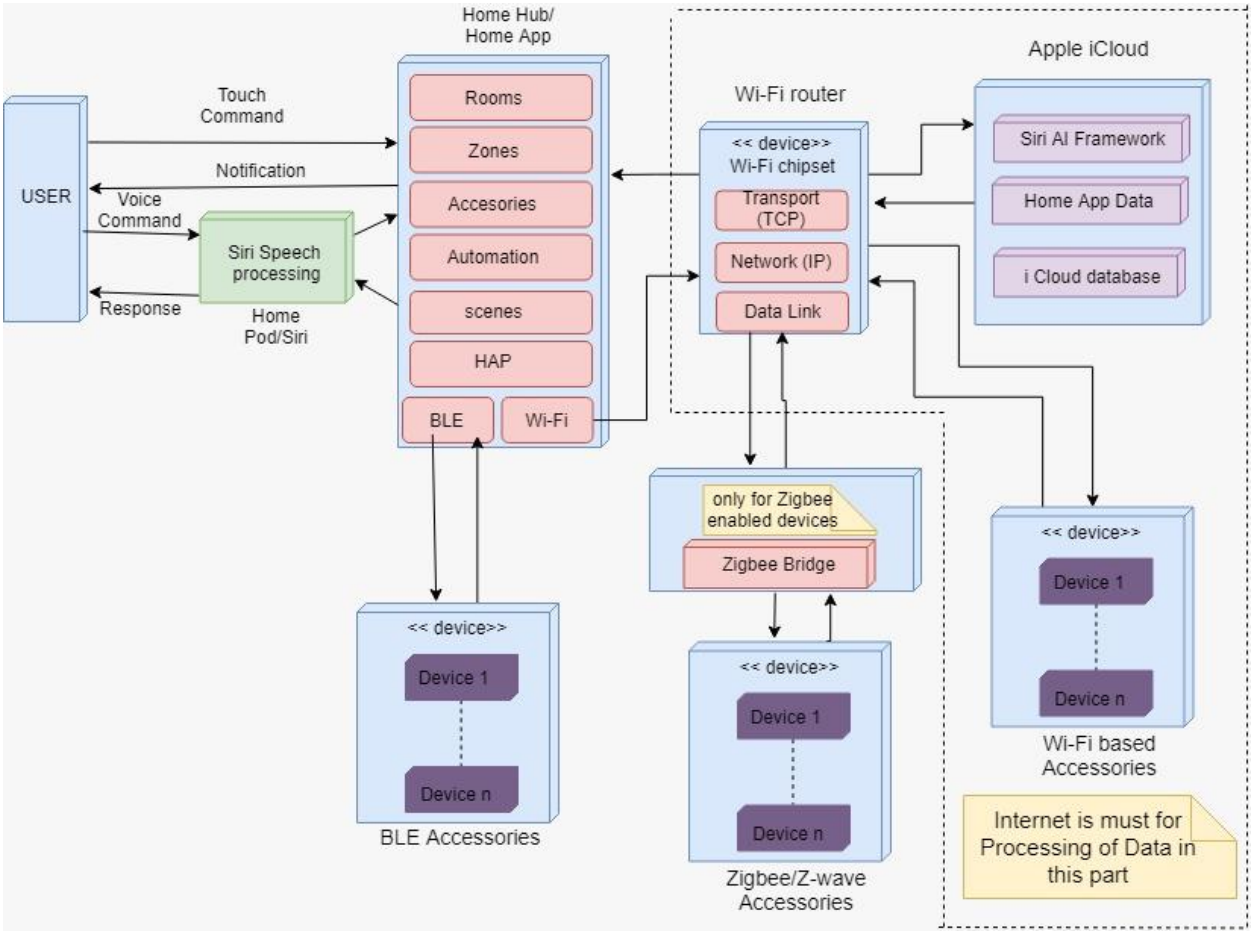
[10] Nfarina. (2018, November 26). Homebridge GitHub Repository. Retrieved from https://github.com/nfarina/homebridge

[11] Stables, J. (2018, August 09). Apple HomeKit: Everything you need to know about living in an Apple Home. Retrieved from https://www.the-ambient.com/guides/apple-homekit-complete-guide-194

[12] Feiler, J. (2016). *Learn Apple HomeKit on iOS: A home automation guide for developers, designers, and homeowners*. New York: Apress.

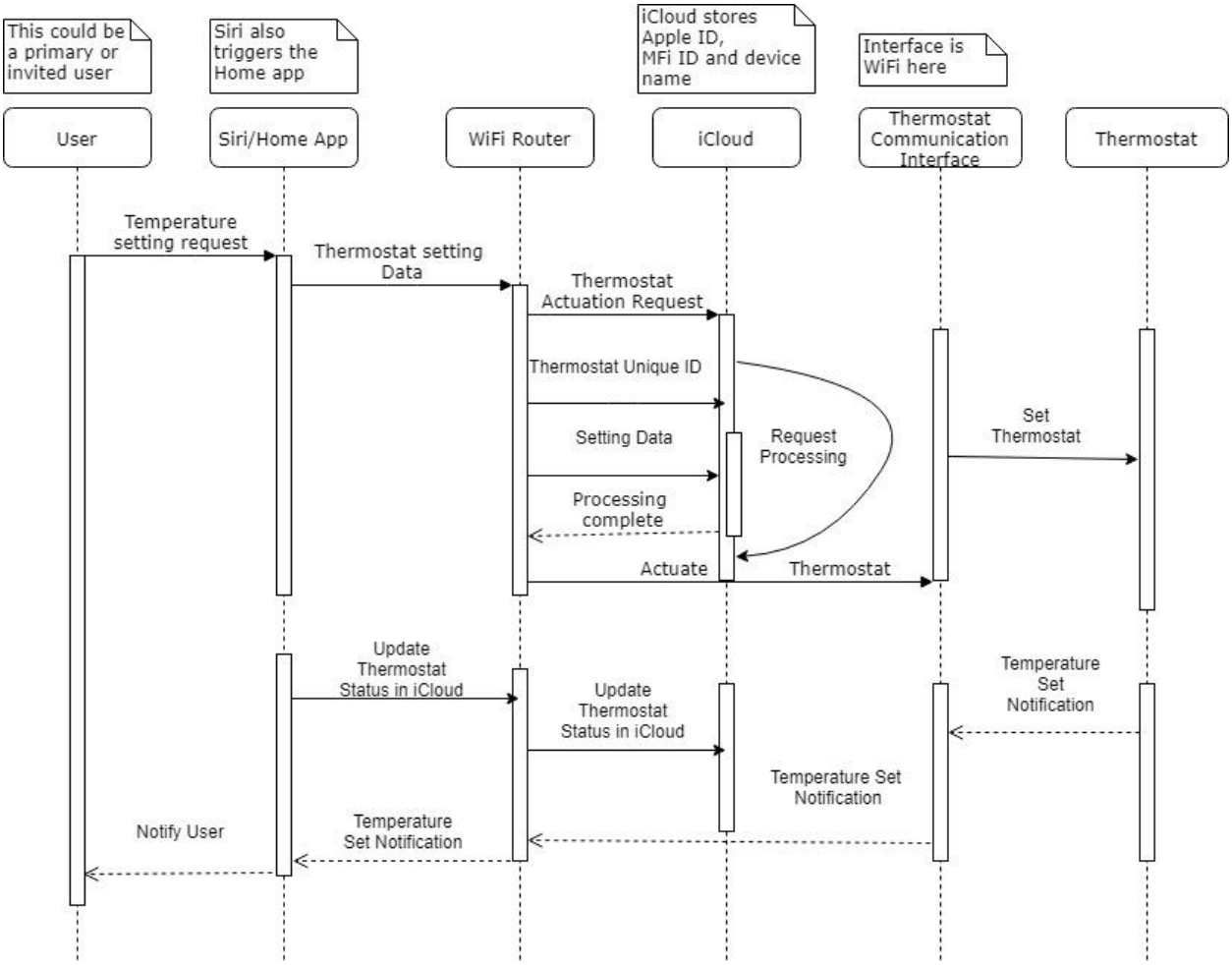
[13] Lei, X., Tu, G., Liu, A. X., Li, C., & Xie, T. (2018). The Insecurity of Home Digital Voice Assistants - Vulnerabilities, Attacks and Countermeasures. *2018 IEEE Conference on Communications and Network Security (CNS)*. doi:10.1109/cns.2018.8433167

APPENDIX A



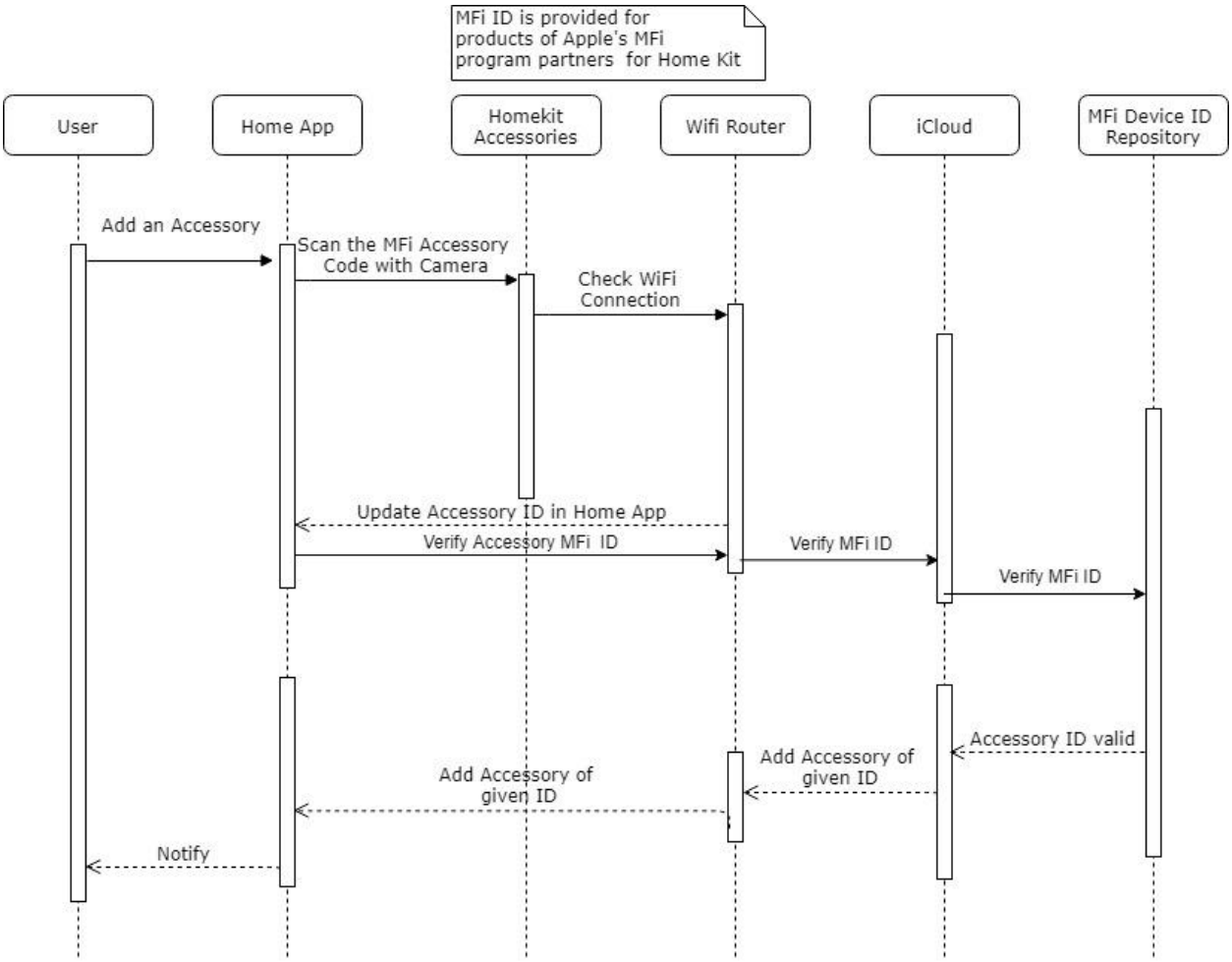
Deployment View of Apple Homekit Home Automation System

APPENDIX B



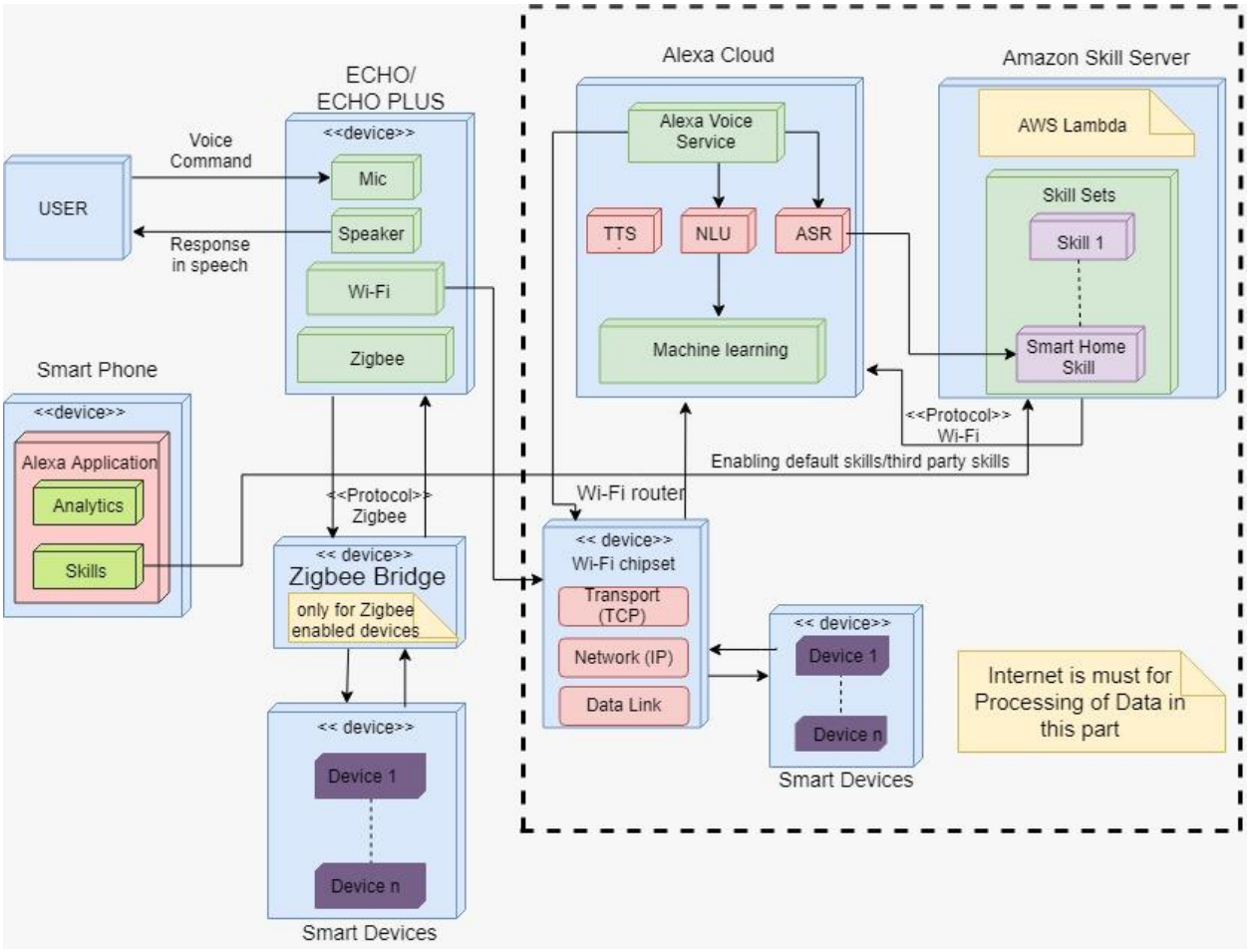
Sequence diagram explaining control and data flow for a Thermostat application based on Apple Homekit

APPENDIX C



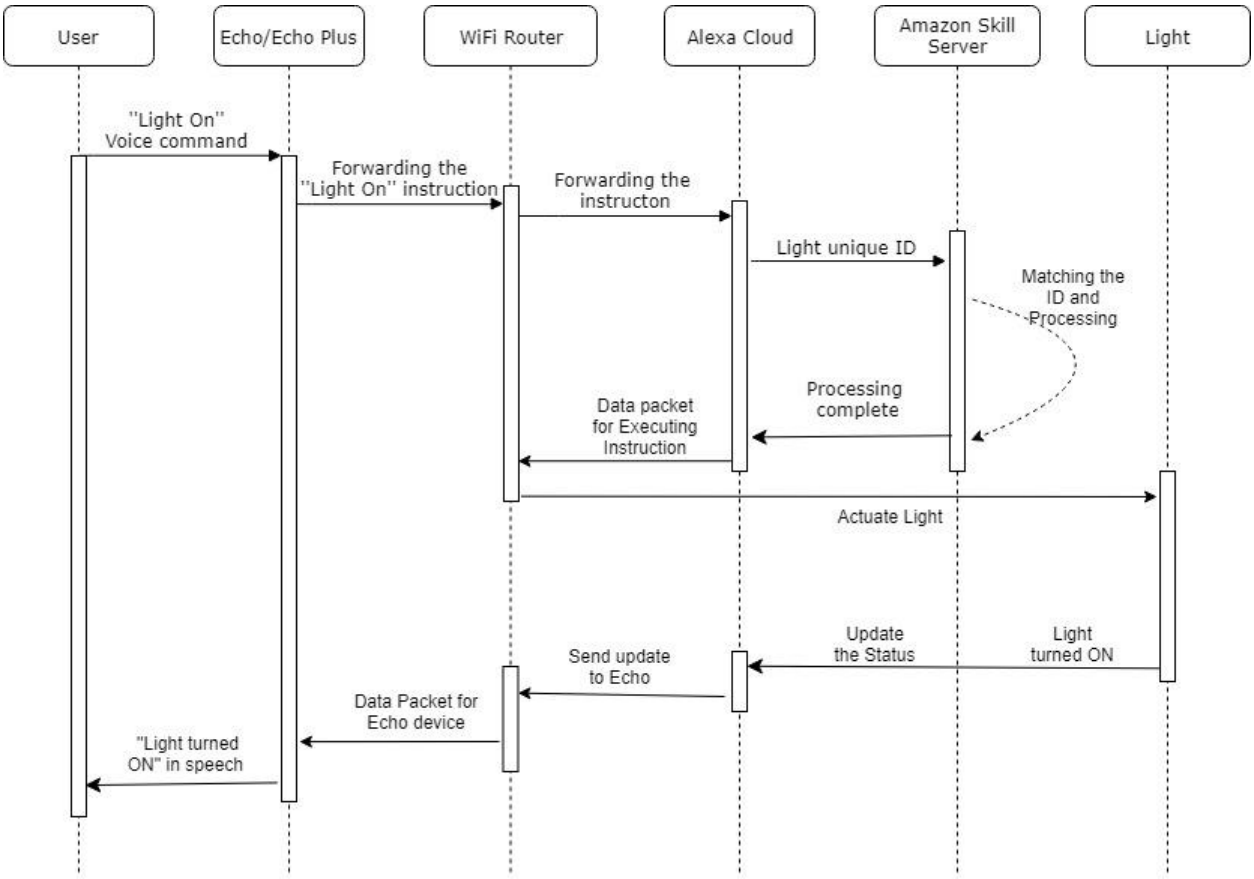
Sequence Diagram explaining the process of adding an accessory in the Apple Homekit network

APPENDIX D



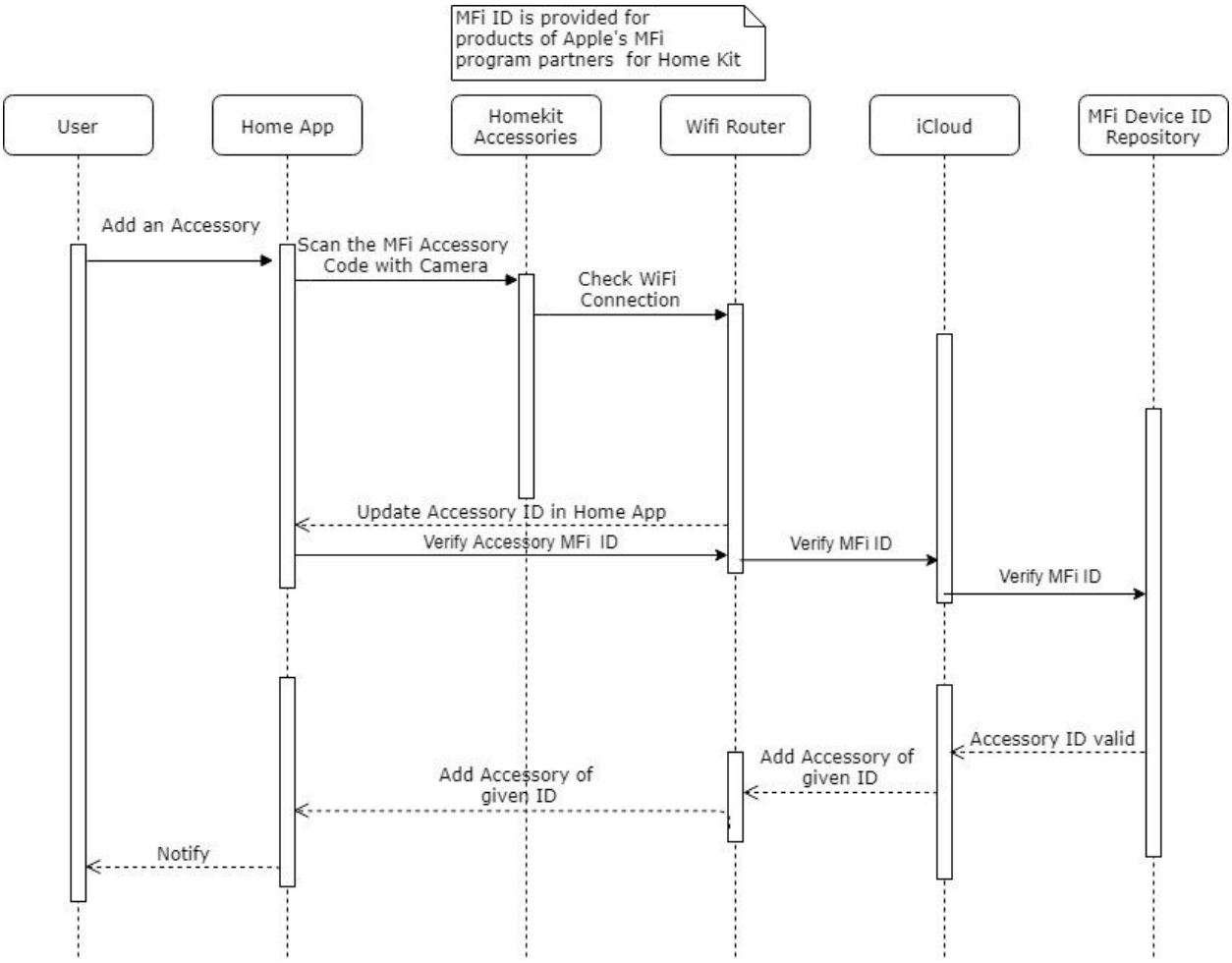
Deployment view of Amazon Echo based Home Automation system

APPENDIX E



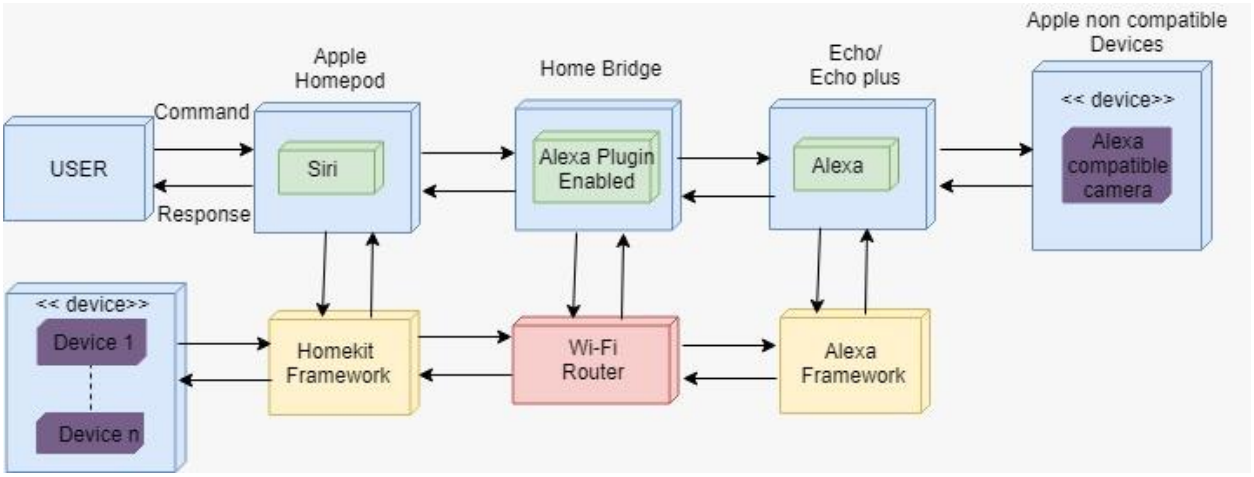
Sequence Diagram explaining the application of light activation in Alexa Home Automation

APPENDIX F



Sequence diagram demonstrating addition of an accessory in Amazon Alexa's IoT framework via Amazon Echo

APPENDIX G



Deployment view of a combined Apple Homekit and Amazon Echo+Alexa based Home Automation system using a Homebridge to control an Alexa based IP Camera