IOT-Assignment1

Snorri Stefansson, Sai Krishna Kalluri
Department of Mathematics and Computer Science,Eindhoven University of Technology
[s.stefansson, s.k.kalluri]@student.tue.nl

I. INTRODUCTION

Two separate IoT platforms from different companies will be analyzed with the main focus on their overview and architecture. Moreover, their deployment view, control system and their data flow.

The two projects are from the two largest technology rivals, namely Google nest (Nest 2016) and Apple Homekit (Apple 2016). Although in these two use cases, the companies are not competing for the exact same goals and thus their architectures are not comparable in that way. Performance wise but their efficiency and security protocol can be compared.

These project will be covered individually and with respect to their developers, users and use cases.

II. APPLE HOMEKIT

Apple Homekit is an economical home automation product for everyone wanting to have digital control over their home. It consists of various products by different vendors who integrate their products, through an API, into this project in collaboration with Apple. To ensure the user has complete control, Apple developed an iOS App called Home which can control all devices inside the platform and with great horizontal analyses and high level automation based on weather, time of day and even the users location.

To name a few of the Homekit's possible automation aspects; lighting, locks, security cameras, electricity control and measurements, temperature control, air quality control, doorbell and other sensors and actuators offered by Apple's collaborators.

Apple diversifies itself from other IoT platforms in the largest way that they do not produce any of the devices used for sensing and actuating. They reduced their time to market and save resources on the development of these new devices. This strategy involves other companies, and their invites them to a highly advances infrastructure, but only as the lowest leaf in their tree. Apple makes use of their user based devices to gather information, such as the iPhone, if the user is at home accompanying the devices. The iPad and Apple TV can act as a remote for all devices when the user is not home. This strikes as a security vulnerability, devices being accessible over the internet, but the the communication is end-to-end encrypted, via iCloud, and not by the low power IoT devices but by a plugged in powerful apple device. This procedure creates a way for vendors with low power communication protocols that utilize Bluetooth or Wi-Fi to forget about high level security protection and focus on functionality. The diagram in Figure 1 explains the basic functionality of the Homekit where Apple devices can collect data from vendor sensors and send data to their actuators as well. This is done through bridges if the vendor does not utilize the Homekit API straight on the device.

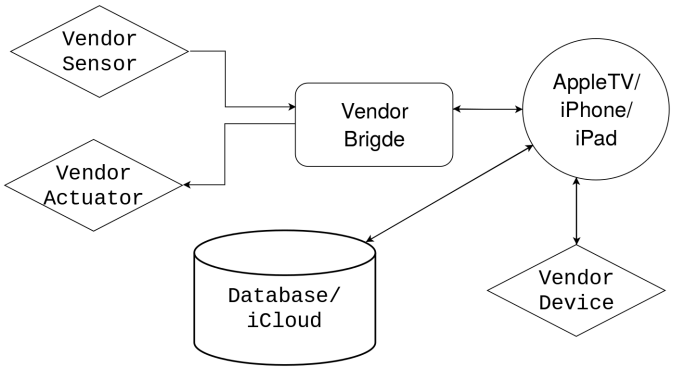

Fig. 1: A simplified functional diagram of the Homekit. Data from devices and user settings is centrally stored in a database. Device data-flow directions are shown and device specialized functionality is hidden and will discussed later on.

All data from devices in the Homekit is stored in iCloud which allows Apple to horizontally analyze it as well as it being available to any user, anywhere, with the correct permission of course. iCloud will update information cross devices, even for different user registered to this certain home. Thus iCloud updates as close as possible to real time to ensure all users see the correct information.

A. Deployment View

The Homekit's IoT devices are deployed by the user after purchase. The deployment process is simplified to the extent that a user can set up the device within minutes. When describing the architecture, different view have to be taken into account. Namely, the user can have setups depending two factors: Firstly, if the user chooses to have a remote access via an Apple TV or an iPad and secondly if the user is home or not.

The two cases function the same when the user is at home. Otherwise there is an iPad or an Apple TV that is constantly connected to all other devices and will be internet connected. The first case is more extensive and will thus be focused on when describing the architecture seen in Figure 2.

With the architecture in mind, there are three main architectures that vendor follow when embedding into the Homekit platform.

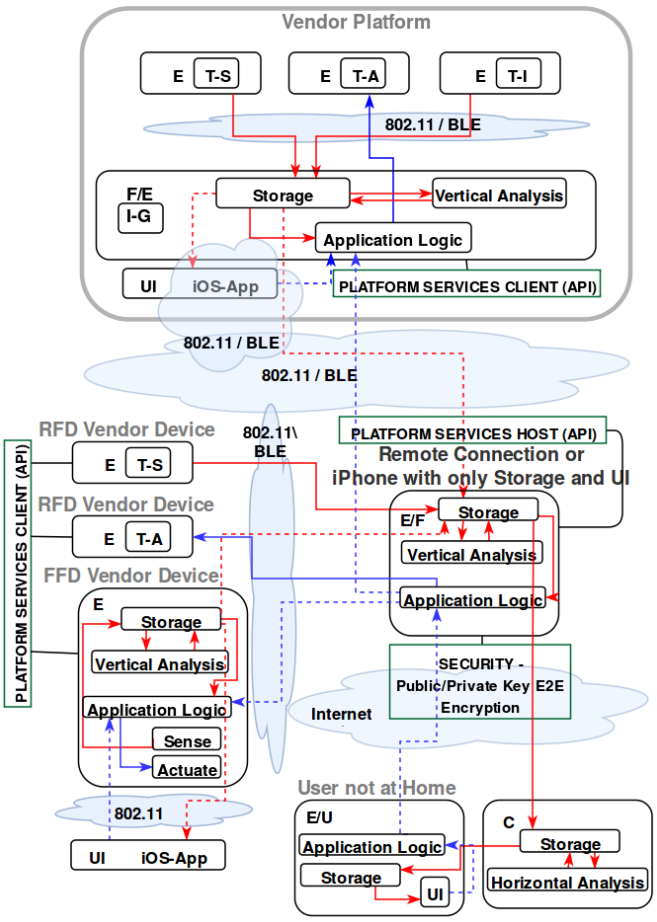

Fig. 2: Architectural diagram of the Homekit describing connections and dataflow between devices and platforms. This diagram focuses on the case were the user has remote access via an Apple TV/iPad, which is the most extensive use of the Homekit. The diagram can be simplified for the other case, only user device for total system overview without remote access.

1) **Vendor Platform**. A (IEEE 802.11 connected) vendor bridge acts as a storage and automation unit for one or more devices from the this vendor, creating a vendor platform inside the Homekit. The bridge can also be operated without the Homekit with an UI, app or physical unit, but the extra functionality such as location based operation and a higher level automation through a single platform is provided through Homekit.
2) **Full-function device (FFD) by vendor**. A device that can be fully functional on its own without a bridge. These devices are capable of fulfilling their main purpose without control from the Homekit but they need either a manual user input from a UI or an iOS app. Despite that the devices integrates into the Homekit directly with through Apple's API and IEEE 802.11 or BLE. An example of this device is a thermostat that can set the temperature from an input and a Smoke and Gas Alarm.
3) **Reduced-function device (RFD) by vendor**. These devices cannot function without human interference through the Home App or the vendors app. Despite that, the device can directly communicate to the API without any bridge or other setup. A good example is a switch that can be turned on or off or a sensor that can stream data and able other devices to act on.

B. *Privacy and Fault analysis*

Nothing is perfect in the sense of being unbreakable. All systems and architectures involving personal details and behavioral information is incredibly delicate and should always be handles carefully. The Homekit utilized security thoroughly and to be able to hack it, internal knowledge from Apple is required were the details about the systems are never reviled to the public as was learned when gathering information about this architecture. The main weakness of the architectures without much investigation is the third party devices that apple invites to this network. Third party devices collect some information from at a users home. Thus if someone with the intention of gathering information about people could make and sell a Homekit enabled product online for a low price and including some scripts to send the data to another external API. The user would have to join the device to the Homekit network and maybe also ignore some security warning that his might not be a secure device authenticated be Apple. This could be done with a Raspberry pi for instance. This is maybe a far fetched fault and not a concern for observant users.

C. *Life cycle*

The Homekit's infrastructure is advanced and developed in with self sustainability in mind. Although self sustainability is the goal, the wireless devices require battery changing and all of the devices require for example firmware upgrade at some point. Not only the devices need attention but also the main software and communication methods, namely the API. All these components need maintained by Apple, the vendor or the user. To clarify the main categories defining the life cycle, see Figure 3, were these physical objects are linked with their associated handlers.

III. Google Nest

Nest consists of following products.1.Thermostat 2.Protect and 3.Camera Multiple products of the same or different type can be used to form a Nest network. These products communicate within themselves using IEEE 802.15.4 while they connect to the internet using Wi-fi(IEEE 802.11).Data from the network is sent to Nest Cloud using Internet Protocol(IP).

The main objective of Nest Thermostat is to optimize the energy consumed by the heating and cooling systems of the environment. It does it with the help of a machine learning algorithm, where it studies the schedules of desired needs based on data from the sensors and user inputs. In other words, it performs horizontal analyzes on the data and uses this information to take necessary actions. Nest Protect offers

Stage	Vendor Device	API	Apple TV/ iPad/iPhone
Analysis	Device specific covering home automation as a whole, defined by Apple	Apple	Apple
Design, Implementation, Testing,	Vendor	Apple in collaboration with vendors	Apple
Deployment	Purchase and configured in Home App (User)	Apple	Purchased by user
Configuration	User, Vendor and/or Apple	Apple and vendors	User (and Apple if needed)
Operation	Automated (partly by Apples algorithms) and User	Apple and vendor	User
Update	Vendor	Apple	Apple

Fig. 3: A link between the physical objects of the Homekit and the relying stages on each object is described; Creating the life cycle and responsibilities of maintenance and up keeping.

protection from smoke and CO emissions. Nest Cam is used to monitor activities in the installed location (indoor or outdoor). The user can remotely monitor and control these products using remote applications via Nest cloud. Nest also supports incorporating other manufacturers smart devices to the Nest network. These devices are integrated into nest network via Vendor bridge connected to Wi-Fi router. All the devices in the nest network exchange required (limited) information to take necessary actions in accordance with the collective state of the environment. Figure 4 shows a rough outline of various possible devices that can installed in the network along with corresponding protocols used for communication.

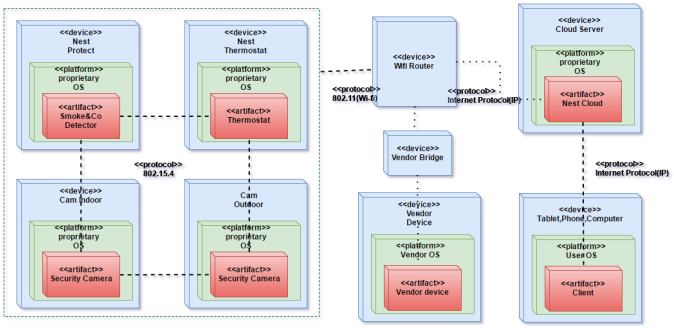

Fig. 4: A functional diagram of the Nest. Data from devices and user settings is centrally stored in a database.

A. Deployment View

Figure 5 shows the deployment view of the functionality of various devices in nest the network in detail along with data and control flow throughout the network.

B. Privacy and Fault analysis

Security is a serious concern in home automation. And some flaws that can be pointed out just by comparing the two home automation platforms, Nest and Homekit, are that the Homekit utilized E2EE on all components. Nest labs utilize the same function for the cameras which is important were that is one of the major privacy factors, real time footage. Nest Labs do

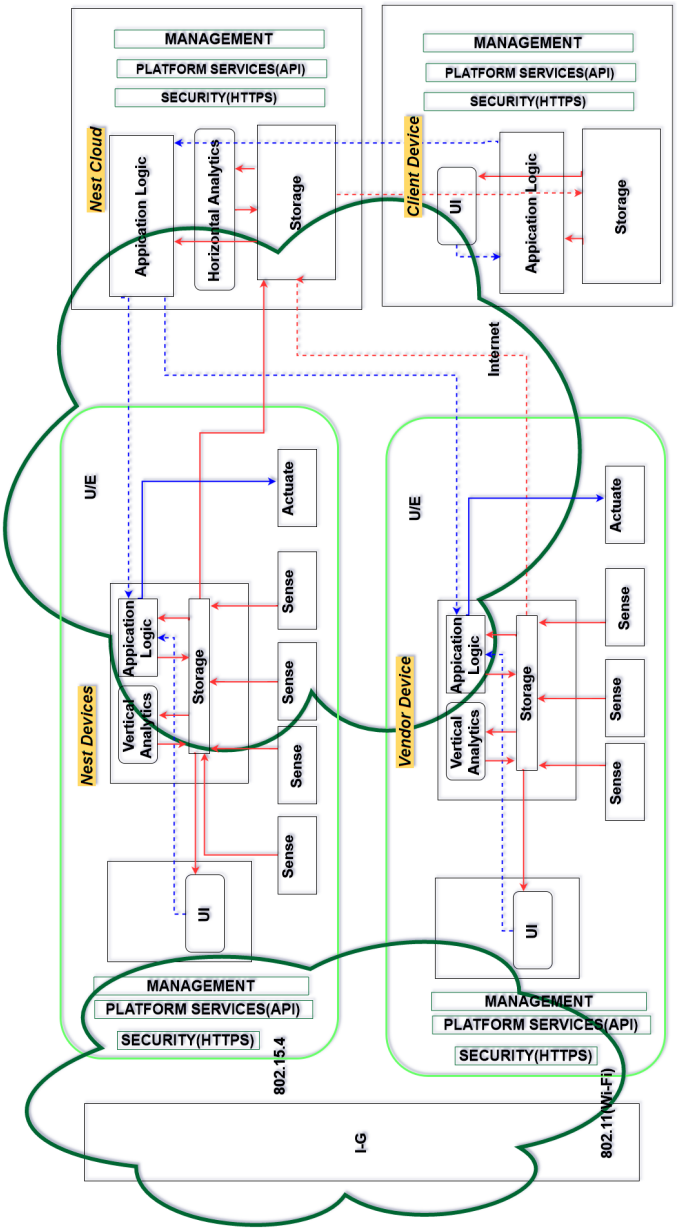

Fig. 5: Deployment view of the Nest along with the Data Flow.

not implement a encryption with 2048-bit RSA private keys on the other gadgets of the home, but rather Transport Layer Security TLS, which could lead to man-in-the-middle attacks where the attacker might be able to inject plain text into the protocol stream (Employee n.d.) which could lead to problems with the communication. This is not a major issue but still something that might be referred to as a minor security issue.

C. Life cycle

The life cycle of the Nest depends on different devices, software and vendors. First of all Nest can only assure that the product developed by Nest will fit their standard. The Vendors developing hardware and home gadgets are inclined to make

their products the best they can be by integrating them into a smart home platform such as the Nest. The Vendors are then responsible to keep their products up to date and working with the latest changes from nest or the user requirements. Other from the vendor, Nest Labs are mostly responsible for keeping the life cycle of the Nest as long as possible with renewability as easy as possible. The firmware has to be able to update without interference of the user but configurations and setup can be done by the user to maintain low cost and simplicity. See Figure 6 for a detailed review of the Nests's life cycle stages.

Stage	Thermostat	Protect	Cam	Vendor Device
Analysis	Need for smart device to optimize energy consumptions	Need for smart device to monitor smoke and CO emissions	Need for monitoring activities in a given location	Device Specific
Design, Implementation, Testing, Commissioning, Software Install,	Nest Labs	Nest Labs	Nest Labs	Vendor
Deployment	Purchase and integrating to nest network using Nest App (User).	Purchase and integrating to nest network using Nest App (User).	Purchase and integrating to nest network using Nest App (User).	Purchase and integrating to nest network using Nest App (User).
Configuration	User, Nest Labs	User, Nest Labs	User, Nest Labs	User,Vendor
Operation	Automatic and manual with high priority for manual operation	Automatic	Automatic	Application specific. Can be manually controlled through vendor apps.
Update	NestLabs	NestLabs	NestLabs	Vendor

Fig. 6: Life Cycle of products in nest network

REFERENCES

Apple (2016). *The Smart Home Just Got Smarter*. URL: www.apple.com/ios/home/.

Employee, Adrian Pisarczyk - Symantec. *Transport Layer Security Issues*. URL: https://www.symantec.com/connect/blogs/transport-layer-security-issues.

Nest, Google (2016). *Nest is home*. URL: https://nest.com/.