Chapter

Smart Home Systems Based on Internet of Things

Menachem Domb

Abstract

Smart home systems achieved great popularity in the last decades as they increase the comfort and quality of life. Most smart home systems are controlled by smartphones and microcontrollers. A smartphone application is used to control and monitor home functions using wireless communication techniques. We explore the concept of smart home with the integration of IoT services and cloud computing to it, by embedding intelligence into sensors and actuators, networking of smart things using the corresponding technology, facilitating interactions with smart things using cloud computing for easy access in different locations, increasing computation power, storage space and improving data exchange efficiency. In this chapter we present a composition of three components to build a robust approach of an advanced smart home concept and implementation.

Keywords: smart home, IoT, cloud computing, event processing, home appliances, rule-based event processing

1. Introduction

Classic smart home, internet of things, cloud computing and rule-based event processing, are the building blocks of our proposed advanced smart home integrated compound. Each component contributes its core attributes and technologies to the proposed composition. IoT contributes the internet connection and remote management of mobile appliances, incorporated with a variety of sensors. Sensors may be attached to home related appliances, such as air-conditioning, lights and other environmental devices. And so, it embeds computer intelligence into home devices to provide ways to measure home conditions and monitor home appliances' functionality. Cloud computing provides scalable computing power, storage space and applications, for developing, maintaining, running home services, and accessing home devices anywhere at anytime. The rule-based event processing system provides the control and orchestration of the entire advanced smart home composition.

Combining technologies in order to generate a best of breed product, already appear in recent literature in various ways. Christos Stergioua et al. [1] merge cloud computing and IoT to show how the cloud computing technology improves the functionality of the IoT. Majid Al-Kuwari [2] focus on embedded IoT for using analyzed data to remotely execute commands of home appliances in a smart home. Trisha Datta et al. [3] propose a privacy-preserving library to embed traffic shaping in home appliances. Jian Mao et al. [4] enhance machine learning algorithms to play a role in the security in a smart home ecosystem. Faisal Saeed et al. [5] propose using sensors to sense and provide in real-time, fire detection with high accuracy.

In this chapter we explain the integration of classic smart home, IoT and cloud computing. Starting by analyzing the basics of smart home, IoT, cloud computing and event processing systems. We discuss their complementarity and synergy, detailing what is currently driving to their integration. We also discuss what is already available in terms of platforms, and projects implementing the smart home, cloud and IoT paradigm. From the connectivity perspective, the added IoT appliances and the cloud, are connected to the internet and in this context also to the home local area network. These connections complement the overall setup to a complete unified and interconnected composition with extended processing power, powerful 3rd party tools, comprehensive applications and an extensive storage space.

In the rest of this chapter we elaborate on each of the four components. In Section 1, we describe the classic smart home, in Section 2, we introduce the internet of things [IoT], in Section 3, we outline cloud computing and in Section 4, we present the event processing module. In Section 5, we describe the composition of an advanced smart home, incorporating these four components. In Section 6, we provide some practical information and relevant selection considerations, for building a practical advanced smart home implementation. In Section 7, we describe our experiment introducing three examples presenting the essence of our integrated proposal. Finally, we identify open issues and future directions in the future of advanced smart home components and applications.

2. Classic smart home overview

Smart home is the residential extension of building automation and involves the control and automation of all its embedded technology. It defines a residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment systems, big home appliances such as washers/dryers and refrigerators/freezers, security and camera systems capable of communicating with each other and being controlled remotely by a time schedule, phone, mobile or internet. These systems consist of switches and sensors connected to a central hub controlled by the home resident using wall-mounted terminal or mobile unit connected to internet cloud services.

Smart home provides, security, energy efficiency, low operating costs and convenience. Installation of smart products provide convenience and savings of time, money and energy. Such systems are adaptive and adjustable to meet the ongoing changing needs of the home residents. In most cases its infrastructure is flexible enough to integrate with a wide range of devices from different providers and standards.

The basic architecture enables measuring home conditions, process instrumented data, utilizing microcontroller-enabled sensors for measuring home conditions and actuators for monitoring home embedded devices.

The popularity and penetration of the smart home concept is growing in a good pace, as it became part of the modernization and reduction of cost trends. This is achieved by embedding the capability to maintain a centralized event log, execute machine learning processes to provide main cost elements, saving recommendations and other useful reports.

2.1 Smart home services

2.1.1 Measuring home conditions

A typical smart home is equipped with a set of sensors for measuring home conditions, such as: temperature, humidity, light and proximity. Each sensor is

dedicated to capture one or more measurement. Temperature and humidity may be measured by one sensor, other sensors calculate the light ratio for a given area and the distance from it to each object exposed to it. All sensors allow storing the data and visualizing it so that the user can view it anywhere and anytime. To do so, it includes a signal processer, a communication interface and a host on a cloud infrastructure.

2.1.2 Managing home appliances

Creates the cloud service for managing home appliances which will be hosted on a cloud infrastructure. The managing service allows the user, controlling the outputs of smart actuators associated with home appliances, such as such as lamps and fans. Smart actuators are devices, such as valves and switches, which perform actions such as turning things on or off or adjusting an operational system. Actuators provides a variety of functionalities, such as on/off valve service, positioning to percentage open, modulating to control changes on flow conditions, emergency shutdown (ESD). To activate an actuator, a digital write command is issued to the actuator.

2.1.3 Controlling home access

Home access technologies are commonly used for public access doors. A common system uses a database with the identification attributes of authorized people. When a person is approaching the access control system, the person's identification attributes are collected instantly and compared to the database. If it matches the database data, the access is allowed, otherwise, the access is denied. For a wide distributed institute, we may employ cloud services for centrally collecting persons' data and processing it. Some use magnetic or proximity identification cards, other use face recognition systems, finger print and RFID.

In an example implementation, an RFID card and an RFID reader have been used. Every authorized person has an RFID card. The person scanned the card via RFID reader located near the door. The scanned ID has been sent via the internet to the cloud system. The system posted the ID to the controlling service which compares the scanned ID against the authorized IDs in the database.

2.2 The main components

To enable all of the above described activities and data management, the system is composed of the following components, as described in **Figure 1**.

a. Sensors to collect internal and external home data and measure home conditions. These sensors are connected to the home itself and to the attached-to-home devices. These sensors are not internet of things sensors, which are attached to home appliances. The sensors' data is collected and continually transferred via the local network, to the smart home server.

b. Processors for performing local and integrated actions. It may also be connected to the cloud for applications requiring extended resources. The sensors' data is then processed by the local server processes.

c. A collection of software components wrapped as APIs, allowing external applications execute it, given it follows the pre-defined parameters format. Such an API can process sensors data or manage necessary actions.

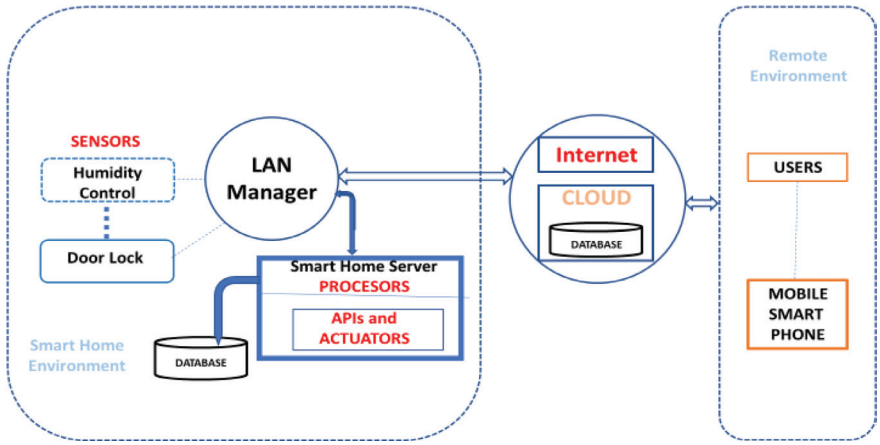

Figure 1.
Smart home paradigm with optional cloud connectivity.

d. Actuators to provision and execute commands in the server or other control devices. It translates the required activity to the command syntax; the device can execute. During processing the received sensors' data, the task checks if any rule became true. In such case the system may launch a command to the proper device processor.

e. Database to store the processed data collected from the sensors [and cloud services]. It will also be used for data analysis, data presentation and visualization. The processed data is saved in the attached database for future use.

3. Internet of things [IoT] overview

The internet of things (IoT) paradigm refers to devices connected to the internet. Devices are objects such as sensors and actuators, equipped with a telecommunication interface, a processing unit, limited storage and software applications. It enables the integration of objects into the internet, establishing the interaction between people and devices among devices. The key technology of IoT includes radio frequency identification (RFID), sensor technology and intelligence technology. RFID is the foundation and networking core of the construction of IoT. Its processing and communication capabilities along with unique algorithms allows the integration of a variety of elements to operate as an integrated unit but at the same time allow easy addition and removal of components with minimum impact, making IoT robust but flexible to absorb changes in the environment and user preferences. To minimize bandwidth usage, it is using JSON, a lightweight version of XML, for inter components and external messaging.

4. Cloud computing and its contribution to IoT and smart home

Cloud computing is a shared pool of computing resources ready to provide a variety of computing services in different levels, from basic infrastructure to most sophisticated application services, easily allocated and released with minimal efforts or service provider interaction [6, 7]. In practice, it manages computing, storage, and communication resources that are shared by multiple users in a virtualized and isolated environment. **Figure 2** depicts the overall cloud paradigm.

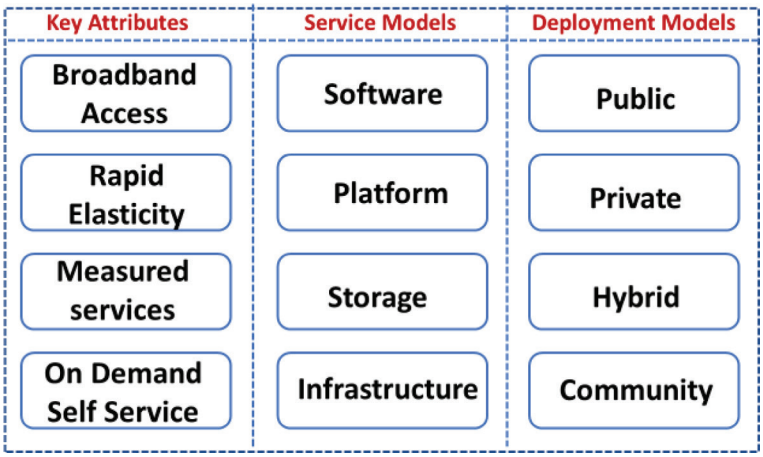

Figure 2.
Cloud computing paradigm.

IoT and smart home can benefit from the wide resources and functionalities of cloud to compensate its limitation in storage, processing, communication, support in pick demand, backup and recovery. For example, cloud can support IoT service management and fulfillment and execute complementary applications using the data produced by it. Smart home can be condensed and focus just on the basic and critical functions and so minimize the local home resources and rely on the cloud capabilities and resources. Smart home and IoT will focus on data collection, basic processing, and transmission to the cloud for further processing. To cope with security challenges, cloud may be private for highly secured data and public for the rest.

IoT, smart home and cloud computing are not just a merge of technologies. But rather, a balance between local and central computing along with optimization of resources consumption. A computing task can be either executed on the IoT and smart home devices or outsourced to the cloud. Where to compute depends on the overhead tradeoffs, data availability, data dependency, amount of data transportation, communications dependency and security considerations. On the one hand, the triple computing model involving the cloud, IoT and smart home, should minimize the entire system cost, usually with more focus on reducing resource consumptions at home. On the other hand, an IoT and smart home computing service model, should improve IoT users to fulfill their demand when using cloud applications and address complex problems arising from the new IoT, smart home and cloud service model.

Some examples of healthcare services provided by cloud and IoT integration: properly managing information, sharing electronic healthcare records enable high-quality medical services, managing healthcare sensor data, makes mobile devices suited for health data delivery, security, privacy, and reliability, by enhancing medical data security and service availability and redundancy and assisted-living services in real-time, and cloud execution of multimedia-based health services.

5. Centralized event processing, a rule-based system

Smart home and IoT are rich with sensors, which generate massive data flows in the form of messages or events. Processing this data is above the capacity of a human being's capabilities [8–10]. Hence, event processing systems have been developed and used to respond faster to classified events. In this section, we focus

on rule management systems which can sense and evaluate events to respond to changes in values or interrupts. The user can define event-triggered rule and to control the proper delivery of services. A rule is composed of event conditions, event pattern and correlation-related information which can be combined for modeling complex situations. It was implemented in a typical smart home and proved its suitability for a service-oriented system.

The system can process large amounts of events, execute functions to monitor, navigate and optimize processes in real-time. It discovers and analyzes anomalies or exceptions and creates reactive/proactive responses, such as warnings and preventing damage actions. Situations are modeled by a user-friendly modeling interface for event-triggered rules. When required, it breaks them down into simple, understandable elements. The proposed model can be seamlessly integrated into the distributed and service-oriented event processing platform.

The evaluation process is triggered by events delivering the most recent state and information from the relevant environment. The outcome is a decision graph representing the rule. It can break down complex situations to simple conditions, and combine them with each other, composing complex conditions. The output is a response event raised when a rule fires. The fired events may be used as input for other rules for further evaluation. Event patterns are discovered when multiple events occur and match a pre-defined pattern. Due to the graphical model and modular approach for constructing rules, rules can be easily adapted to domain changes. New event conditions or event patterns can be added or removed from the rule model. Rules are executed by event services, which supply the rule engine with events and process the evaluation result. To ensure the availability of suitable processing resources, the system can run in a distributed mode, on multiple machines and facilitate the integration with external systems, as well. The definition of relationships and dependencies among events that are relevant for the rule processing, are performed using sequence sets, generated by the rule engine. The rule engine constructs sequences of events relevant to a specific rule condition to allow associating events by their context data. Rules automatically perform actions in response when stated conditions hold. Actions generate response events, which trigger response activities. Event patterns can match temporal event sequences, allowing the description of home situations where the occurrences of events are relevant. For example, when the door is kept open too long.

The following challenges are known with this model: structure for the processed events and data, configuration of services and adapters for processing steps, including their input and output parameters, interfaces to external systems for sensing data and for responding by executing transactions, structure for the processed events and data, data transformations, data analysis and persistence. It allows to model which events should be processed by the rule service and how the response events should be forwarded to other event services. The process is simple: data is collected and received from adapters which forward events to event services that consume them. Initially the events are enriched to prepare the event data for the rule processing. For example, the response events are sent to a service for sending notifications to a call agent, or to services which transmit event delay notifications and event updates back to the event management system.

5.1 Event processing languages

Event processing is concerned with real-time capturing and managing predefined events. It starts from managing the receptors of events right from the event occurrence, even identification, data collection, process association and activation

of the response action. To allow rapid and flexible event handling, an event processing language is used, which allows fast configuration of the resources required to handle the expected sequence of activities per event type. It is composed of two modules, ESP and CEP. ESP efficiently handles the event, analyzes it and selects the appropriate occurrence. CEP handles aggregated events. Event languages describe complex event-types applied over the event log.

5.2 Rediscovering workflow from events

In some cases, rules relate to discrepancies in a sequence of events in a workflow. In such cases, it is mandatory to precisely understand the workflow and its associated events. To overcome this, we propose a reverse engineering process to automatically rediscover the workflows from the events log collected over time, assuming these events are ordered, and each event refers to one task being executed for a single case. The rediscovering process can be used to validate workflow sequences by measuring the discrepancies between prescriptive models and actual process executions. The rediscovery process consists of the following three steps: (1) construction of the dependency/frequency table. (2) Induction of dependency/frequency graphs. (3) Generating WF-nets from D/F-graphs.

6. Advanced smart home

In this section, we focus on the integration of smart home, IoT and cloud computing to define a new computing paradigm. We can find in the literature section [11–14] surveys and research work on smart home, IoT and cloud computing separately, emphasizing their unique properties, features, technologies, and drawbacks. However, our approach is the opposite. We are looking at the synergy among these three concepts and searching for ways to integrate them into a new comprehensive paradigm, utilizing its common underlying concepts as well as its unique attributes, to allow the execution of new processes, which could not be processed otherwise.

Figure 3 depicts the advanced smart-home main components and their interconnectivity. On the left block, the smart home environment, we can see the typical

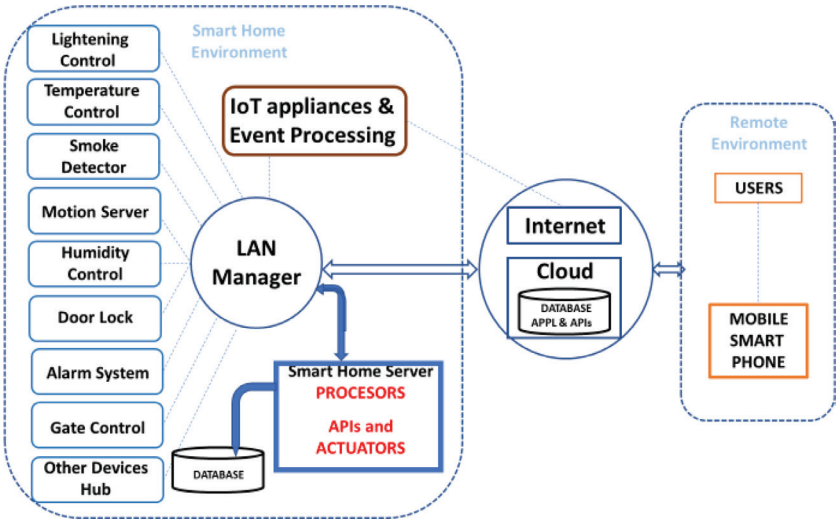

Figure 3.
Advanced smart home—integrating smart home, IoT and cloud computing.

devices connected to a local area network [LAN]. This enables the communication among the devices and outside of it. Connected to the LAN is a server and its database. The server controls the devices, logs its activities, provides reports, answers queries and executes the appropriate commands. For more comprehensive or common tasks, the smart home server, transfers data to the cloud and remotely activate tasks in it using APIs, application programming interface processes. In addition, IoT home appliances are connected to the internet and to the LAN, and so expands smart home to include IoT. The connection to the internet allows the end user, resident, to communicate with the smart home to get current information and remotely activate tasks.

To demonstrate the benefits of the advanced smart home, we use RSA, a robust asymmetric cryptography algorithm, which generates a public and private key and encrypts/decrypts messages. Using the public key, everyone can encrypt a message, but only these who hold the private key can decrypt the sent message. Generating the keys and encrypting/decrypting messages, involves extensive calculations, which require considerable memory space and processing power. Therefore, it is usually processed on powerful computers built to cope with the required resources. However, due to its limited resources, running RSA in an IoT device is almost impossible, and so, it opens a security gap in the Internet, where attackers may easily utilize. To cope with it, we combine the power of the local smart home processors to compute some RSA calculations and forward more complicated computing tasks to be processed in the cloud. The results will then be transferred back to the IoT sensor to be compiled and assembled together, to generate the RSA encryption/decryption code, and so close the mentioned IoT security gap. This example demonstrates the data flow among the advanced smart home components. Where, each component performs its own stack of operations to generate its unique output. However, in case of complicated and long tasks it will split the task to sub tasks to be executed by more powerful components. Referring to the RSA example, the IoT device initiates the need to generate an encryption key and so, sends a request message to the RSA application, running in the smart home computer. The smart home computer then asks the "prime numbers generation" application running on cloud, to provide p and q prime numbers. Once p and q are accepted, the encryption code is generated. In a later stage, an IoT device issues a request to the smart home computer to encrypt a message, using the recent generated RSA encryption key. The encrypted message is then transferred back to the IoT device for further execution. A similar scenario may be in the opposite direction, when an IoT device gets a message it may request the smart home to decrypt it.

To summarize, the RSA scenarios depict the utilization of the strength of the cloud computing power, the smart home secured computing capabilities and at the end the limited power of the IoT device. It proves that without this automatic cooperation, RSA would not be able to be executed at the IoT level.

A more practical example is where several detached appliances, such as an oven, a slow cooker and a pan on the gas stove top, are active in fulfilling the resident request. The resident is getting an urgent phone call and leaves home immediately, without shutting off the active appliances. In case the relevant IoTs have been tuned to automatically shut down based on a predefined rule, it will be taken care at the IoT level. Otherwise, the smart home realizes the resident has left home [the home door has been opened and then locked, the garage has been opened, the resident's car left, the main gate was opened and then closed, no one was at home] and will shut down all active devices classified as risk in case of absence. It will send an appropriate message to the mailing list defined for such an occasion.

7. Practical aspects and implementation considerations for IoT and smart home

Smart home has three components: hardware, software and communication protocols. It has a wide variety of applications for the digital consumer. Some of the areas of home automation led IoT enabled connectivity, such as: lighting control, gardening, safety and security, air quality, water-quality monitoring, voice assistants, switches, locks, energy and water meters.

Advanced smart home components include: IoT sensors, gateways, protocols, firmware, cloud computing, databases, middleware and gateways. IoT cloud can be divided into a platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS). **Figure 4** demonstrates the main components of the proposed advanced smart home and the connection and data flow among its components.

The smart home application updates the home database in the cloud to allow remote people access it and get the latest status of the home. A typical IoT platform contains: device security and authentication, message brokers and message queuing, device administration, protocols, data collection, visualization, analysis capabilities, integration with other web services, scalability, APIs for real-time information flow and open source libraries. IoT sensors for home automation are known by their sensing capabilities, such as: temperature, lux, water level, air composition, surveillance video cameras, voice/sound, pressure, humidity, accelerometers, infrared, vibrations and ultrasonic. Some of the most commonly used smart home sensors are temperature sensors, most are digital sensors, but some are analog and can be extremely accurate. Lux sensors measure the luminosity. Water level ultrasonic sensors.

Float level sensors offer a more precise measurement capability to IoT developers. Air composition sensors are used by developers to measure specific components in the air: CO monitoring, hydrogen gas levels measuring, nitrogen oxide measure, hazardous gas levels. Most of them have a heating time, which means that it requires a certain time before presenting accurate values. It relies on detecting gas

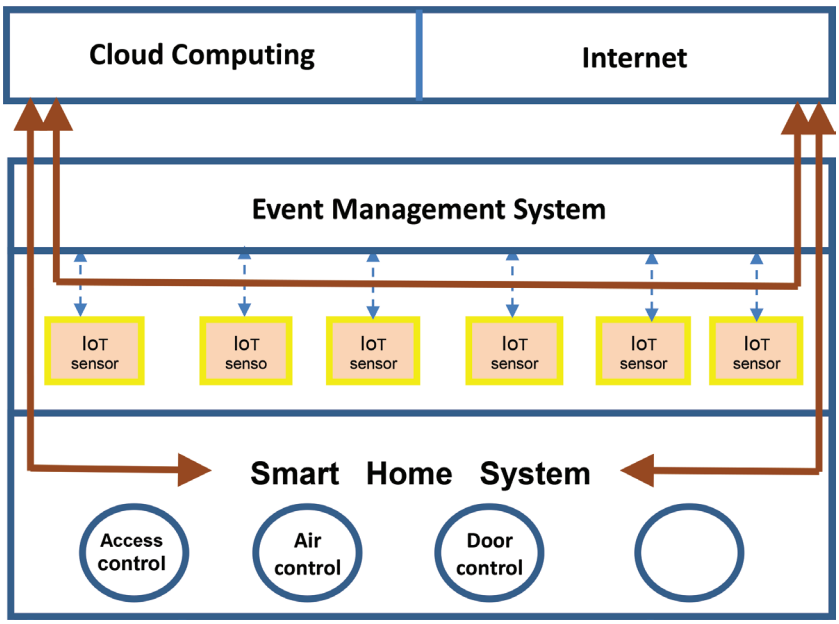

Figure 4.
Advanced smart home composition.

components on a surface only after the surface is heated enough, values start to show up. Video cameras for surveillance and analytics. A range of cameras, with a high-speed connection. Using Raspberry Pi processor is recommended as its camera module is very efficient due to its flex connector, connected directly to the board.

Sound detectors are widely used for monitoring purposes, detecting sounds and acting accordingly. Some can even detect ultra-low levels of noise, and fine tune among various noise levels.

Humidity sensors sense the humidity levels in the air for smart homes. Its accuracy and precision depend on the sensor design and placement. Certain sensors like the DHT22, built for rapid prototyping, will always perform poorly when compared to high-quality sensors like HIH6100. For open spaces, the distribution around the sensor is expected to be uniform requiring fewer corrective actions for the right calibration.

Smart home communication protocols: bluetooth, Wi-Fi, or GSM. Bluetooth smart or low energy wireless protocols with mesh capabilities and data encryption algorithms. Zigbee is mesh networked, low power radio frequency-based protocol for IoT. X10 protocol that utilizes powerline wiring for signaling and control. Insteon, wireless and wireline communication. Z-wave specializes in secured home automation. UPB, uses existing power lines. Thread, a royalty-free protocol for smart home automation. ANT, an ultra-low-power protocol for building low-powered sensors with a mesh distribution capability. The preferred protocols are bluetooth low energy, Z-wave, Zigbee, and thread. Considerations for incorporating a gateway may include: cloud connectivity, supported protocols, customization complexity and prototyping support. Home control is composed of the following: state machine, event bus, service log and timer.

Modularity: enables the bundle concept, runtime dynamics, software components can be managed at runtime, service orientation, manage dependencies among bundles, life cycle layer: controls the life cycle of the bundles, service layers: defines a dynamic model of communication between various modules, actual services: this is the application layer. Security layer: optional, leverages Java 2 security architecture and manages permissions from different modules.

OpenHAB is a framework, combining home automation and IoT gateway for smart homes. Its features: rules engine, logging mechanism and UI abstraction. Automation rules that focus on time, mood, or ambiance, easy configuration, common supported hardware:

Domoticz architecture: very few people know about the architecture of Domoticz, making it extremely difficult to build applications on it without taking unnecessary risks in building the product itself. For example, the entire design of general architecture feels a little weird when you look at the concept of a sensor to control to an actuator. Building advanced applications with Domoticz can be done using OO based languages.

Deployment of blockchain into home networks can easily be done with Raspberry Pi. A blockchain secured layer between devices and gateways can be implemented without a massive revamp of the existing code base. Blockchain is a technology that will play a role in the future to reassure them with revolutionary and new business models like dynamic renting for Airbnb.

8. Smart home and IoT examples

We can find in the literature and practical reports, many implementations of various integrations among part of the main three building blocks, smart home, IoT and cloud computing. For example, refer to [12–14]. In this section we outline three implementations, which clearly demonstrate the need and the benefits of interconnecting

or integrating all three components, as illustrated in **Figure 5**. Each component is numbered, 1–6. In the left side, we describe for each implementation, the sequence of messages/commands among components, from left to right and from bottom up. Take for example the third implementation, a control task constantly runing at the home server (2) discovers the fact that all residents left home and automatically, initiates actuators to shut down all IoT appliances (3), then it issues messages to the relevant users/residents, updating them about the situation and the applied actions it took (6).

The use of (i) in the implementations explanation, corresponds to the circled numbers in **Figure 5**.

8.1 Discovery of water leaks and its prevention

First step is deploying water sensors under every reasonable potential leak source and an automated master water valve sensor for the whole house, which now means the house is considered as an IoT.

In case the water sensor detects a leak of water (3), it sends an event to the hub (2), which triggers the "turn valve off" application. The home control application then sends a "turn off" command to all IoT (3) appliances defined as sensitive to water stopping and then sends the "turn off" command to the main water valve (1). An update message is sent via the messaging system to these appearing in the notification list (6). This setup helps defending against scenarios where the source of the water is from the house plumbing. The underlying configuration assumes an integration via messages and commands between the smart home and the IoT control system. It demonstrates the dependency and the resulting benefits of combining smart home and IoT.

8.2 Smoke detectors

Most houses already have the typical collection of smoke detectors (1), but there is no bridge to send data from the sensor to a smart home hub. Connecting these sensors to a smart home app (2), enables a comprehensive smoke detection system. It is further expanded to notify the elevator sensor to block the use of it due to fire condition (1), and so, it is even further expanded to any IoT sensor (3), who may be activated due to the detected smoke alert.

In [5] they designed a wireless sensor network for early detection of house fires. They simulated a fire in a smart home using the fire dynamics simulator and a language program. The simulation results showed that the system detects fire early.

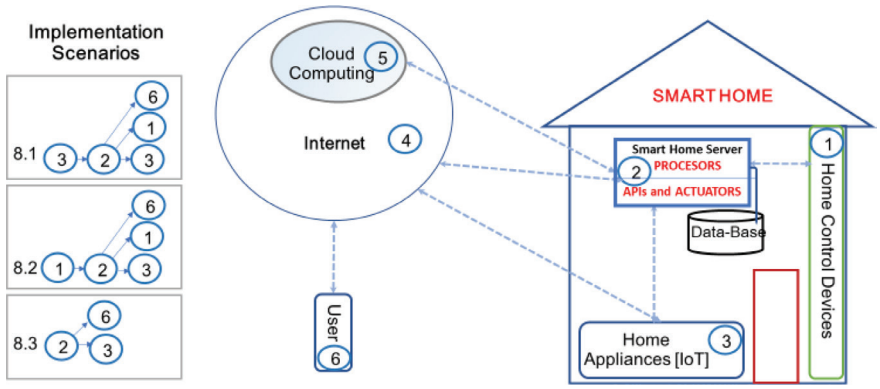

Figure 5.
Advanced smart home implementations chart.

8.3 Incident management to control home appliances

Consider the scenario where you leave home while some of the appliances are still on. In case your absence is long enough, some of the appliances may over heat and are about to blowout. To avoid such situations, we connect all IoT appliances' sensors to the home application (2), so that when all leave home it will automatically adjust all the appliances' sensors accordingly (3), to avoid damages. Note that the indication of an empty home is generated by the Smart Home application, while the "on" indication of the appliance, is generated by IoT. Hence, this scenario is possible due to the integration between smart home and IoT systems.

9. Conclusions and summary

In this chapter we described the integration of three loosely coupled components, smart home, Iot, and cloud computing. To orchestrate and timely manage the vast data flow in an efficient and balanced way, utilizing the strengths of each component we propose a centralized real time event processing application.

We describe the advantages and benefits of each standalone component and its possible complements, which may be achieved by integrating it with the other components providing new benefits raised from the whole compound system. Since these components are still at its development stage, the integration among them may change and provide a robust paradigm that generates a new generation of infrastructure and applications.

As we follow-up on the progress of each component and its corresponding impact on the integrated compound, we will constantly consider additional components to be added, resulting with new service models and applications.

Author details

Menachem Domb
Computer Science Department, Ashkelon Academic College, Ashkelon, Israel

*Address all correspondence to: dombmnc@edu.aac.ac.il

References

[1] Stergioua C, Psannis KE, Kimb B-G, Gupta B. Secure Integration of IoT and Cloud Computing. Elsevier, Future Generation Computer Systems, Vol. 78. Part 3. January 2018. pp. 964-975

[2] Al-Kuwari M, Ramadan A, Ismael Y, Al-Sughair L, Gastli A, Benammar M. Smart-Home Automation Using IoT-Based Sensing and Monitoring Platform, IEEE. 2018. Available from: ieeexplore.ieee.org

[3] Datta T, Apthorpe N, Feamster N. Developer-friendly library for smart home IoT privacy-preserving traffic obfuscation, IoT S&P 18. In: Proceedings of the 2018 Workshop on IoT Security and Privacy. ACM; 2018. pp. 43-48

[4] Mao J, Lin Q , Bian J. Application of Learning Algorithms in Smart Home IoT System Security. American Institute of Mathematical Sciences; 2018. DOI: 10.3934/mfc.2018004

[5] Saeed F, Paul A, Rehman A, Hong WH, Seo H. IoT-based intelligent modeling of smart home environment for fire prevention and safety. Journal of Sensor and Actuator Networks. 2018;**7**(1):11. DOI: 10.3390/jsan7010011

[6] Botta A, de Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: A survey. Future Generation Computer Systems. 2016;**56**:684-700

[7] Soliman M, Abiodun T, Hamouda T, Zhou J, Lung C-H. Smart home: Integrating internet of things with web services and cloud computing. In: International Conference on Cloud Computing Technology and Science; IEEE. 2013

[8] Paschke A, Kozlenkov A. Rule-Based Event Processing and Reaction Rules. London: Betfair Ltd; 2009. DOI: 10.1007/978-3-642-04985-9_8

[9] Khan NS, Ghani S, Haider S. Real-time analysis of a sensor's data for automated decision making in an IoT-based smart home. Sensors. 2018;**18**:1711. DOI: 10.3390/s18061711

[10] Malik R, Parameswaran N, Ghose U. Rule based event management systems. In: Proceedings of the 25th International Florida Artificial Intelligence Research Society Conference. Association for the Advancement of Artificial Intelligence; 2012

[11] Vinodhan D, Vinnarasi A. IOT based smart home. International Journal of Engineering and Innovative Technology (IJEIT). 2016;**5**(10):35-38

[12] Jian MS, Wu JY, Chen JY, Li YJ, Wang YC, Xu HY. IOT Base Smart Home Appliances by Using Cloud Intelligent Tetris Switch; 19-22 February 2017; ICACT, ISBN 978-89-968650-9-4, 2017

[13] Risteska Stojkoska BL, Trivodaliev KV. A review of internet of things for smart home: Challenges and solutions. Journal of Cleaner Production. Part 3. 2017 January 1;**140**(3):1454-1464

[14] Lia B, Yub J. Research and application on the smart home based on component technologies and internet of things. Elsevier, Procedia Engineering; Vol. 15. 2011. pp. 2087-2092. 2011:1877-7058. DOI: 10.1016/j.proeng.2011.08.390