Lessons and Experiences of a DIY Smart Home

Raef Abdallah
Wayne State University
Detroit, Michigan, USA
raef.abdallah@gmail.com

Lanyu Xu
Wayne State University
Detroit, Michigan, USA
xu.lanyu@wayne.edu

Weisong Shi
Wayne State University
Detroit, Michigan, USA
weisong@wayne.edu

ABSTRACT

As our daily lives become busier and more complicated, owning a smart home is increasingly becoming a necessity rather than a luxury. Surveillance systems are heavily utilized by police departments to assist in solving crimes. People rely on surveillance systems to provide them with real-time events taking place inside and outside properties they own. The probability that a smart homeowner can act sooner than later when emergencies arise provides the homeowner a sense of security. In an emergency, time is of the essence and a smart home equipped with the right tools and devices can give a smart homeowner an edge over his/her non-smart home counterpart. Therefore, it is important that the process of converting a home to a smart one is not a complex one. The ease of installation, operation, and maintenance of smart home devices unarguably plays an important role in the wide spread use of smart homes around us. This paper mainly discusses early experiences related to the installation of a surveillance system, the challenges faced during installation, problems encountered after installation, and a glimpse into future work. It presents areas and issues in a smart home that require more investigation in the hope of intriguing researchers to further study smart homes and tackle existing issues.

CCS CONCEPTS

• **Networks** → **Wireless access networks**; • **Human-centered computing** → **Ubiquitous computing**; • **Hardware** → *Wireless devices*;

KEYWORDS

Surveillance systems, smart homes, Do-It-Yourself

ACM Reference format:
Raef Abdallah, Lanyu Xu, and Weisong Shi. 2017. Lessons and Experiences of a DIY Smart Home. In *Proceedings of SmartIoT'17, San Jose / Silicon Valley, CA, USA, October 14, 2017,* 6 pages.
https://doi.org/10.1145/3132479.3132488

1 INTRODUCTION

The smart home epoch is approaching. Allied Market Research predicts that the smart home market revenue of $4.8 billion in 2012 will go up to $35.3 billion by 2020 [3]. Given the flourishing of the Internet of Things (IoT), low cost of electronic devices accompanied with the image sensors and image processing allowed the spread of camera surveillance systems on privately owned properties [5–7, 17]. A homeowner (will be referred to as user) relies on such a system to check on people, events, and property [10, 13]. Police departments reach out to homeowners with surveillance cameras to register their cameras with the department. Information acquired by surveillance systems can significantly aid in solving crimes quickly. The installation, operation, and maintenance cost of a surveillance system can be high. One of the main reasons that a homeowner shies away from installing a surveillance system is due to the cost associated with the installation and maintenance of such a system. In the last decade, many smart home products have been introduced to the market. A product like Amcrest allows users to enhance their smart homes through do-it-yourself (DIY) projects [19]. The easier the installation and maintenance of smart home devices are, the more people will utilize DIY products to convert their homes to smart ones. Because setup and installation fall on the homeowner's shoulders, in a DIY smart home project, the homeowner is prone to face technical challenges during installation, operation, and maintenance of smart home devices.

Smart home devices include many features such as sending email or SMS message to a mobile device when motion is detected using built-in sensors. Despite all the challenges that a homeowner can sometimes experience during installation and configuration of a DIY smart home project, the benefits are worth the effort. One benefit is lower cost in comparison to systems installed, configured, and maintained by professionals. Another benefit is the learning experience that a homeowner gains by from the DIY project opening the doors to continuously improve and add devices and features to the smart home. Also, the DIY project enables one to take responsibility when something goes wrong rather than relying on a professional to rectify the problem. In some cases, this will decrease the downtime of the smart home devices.

In this paper, we will discuss the DIY experience of a home owner installing and setting up a wireless surveillance system. The paper makes the following contributions: *1) Identify the common problems that an average user encounters when configuring and maintaining smart home devices. 2) Highlight major smart home issues post-configuration. 3) Present potential solutions to these issues.*

The remainder of this paper is organized as follows. First section is the introduction. Section 2 describes the home participants, toolkits, and architecture. Section 3 discusses the configuration of a wireless camera surveillance system. Section 4 mainly focuses on the technical challenges faced by the smart homeowner after the system has been set up and in operation. Section 5 discusses data management and storage of the surveillance system and some of the issues associated with that. Section 6 is the maintenance

SmartIoT'17, October 14, 2017, San Jose / Silicon Valley, CA, USA

ACM ISBN 978-1-4503-5528-5/17/10…$15.00
https://doi.org/10.1145/3132479.3132488

and backup of the surveillance system and how that affects the reliability of the system. Section 7 and 7.4 point out observed smart home issues and possible solutions. Section 8 concludes this paper and provides suggestions on how a DIY smart home project can become less of a hassle and more of a success for an average user, as well as open issues for the community to address.

2 RESEARCH METHODS

In order achieve the task on hand, we utilized several DIY commercial products available on the market. Some of those are wireless IP cameras, a wireless router, and a range extender. The experiment took place in a residential environment. The size of the main experimental facility size does not exceed 1100 square feet. Our experiments relied mainly on a wireless connection to collect data and analyze results.

2.1 Participants

In a DIY project like this, the knowledge and skill level of participants in the experiment play an important role in the successful implementation of a smart home. One of the two participants involved in this experiment is somewhat familiar with smart home products and has developed an interest in smart homes. The other participant does not have knowledge in smart homes and is neutral to the whole experiment.

2.2 Experiment Toolkits

It is important that the commercial products chosen for this experiment are reliable, easy-to-configure, and compatible with services such as email and SMS messaging. We decided on Cisco for the wireless router and on six Foscam for wireless IP cameras. For the range extender, we utilized Amped wireless range extender, and WeMo for the switch smart plug. All of the devices used in this experiment provide simple user interfaces for an average user to navigate through and configure.

2.3 The DIY Smart Home Architecture

The experimental smart home is approximately 1040 square feet excluding the detached garage. As mentioned above, the experiment consists of six cameras, one wireless router, wireless range extender, and a smart plug. After the participants completed the camera setup (next section), they proceeded with installing the devices in different locations inside and outside the smart home. Three cameras were installed on the front porch. One camera was installed facing west (driveway). The second camera is pointed east (driveway and street), and the third one faced south (entrance). The fourth camera is located in the living room. The fifth camera was installed in the backyard and the last one was positioned in the garage. In order to extend the WiFi coverage area and provide a boosted signal to the two cameras in the garage and the backyard, the participants installed the wireless range extender in the back part of the smart home (Figure 1).

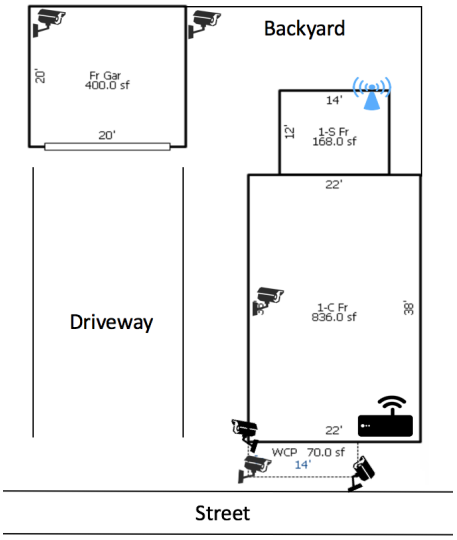

Figure 1: The DIY smart home architecture.

3 CONFIGURATION OF A WIRELESS SURVEILLANCE SYSTEM

In this experiment, the participants worked on the setup of a smart home surveillance system consisting of six Foscam cameras. Five of the cameras are Foscam FI8910W model, and remaining one is Foscam FI8905W model. Each camera was configured initially using a wired connection with a web interface. After each camera has been successfully configured by the homeowner, the cameras were then connected wirelessly to the home network. The six cameras were then installed inside and outside the experimental residence. The participants in our scenario are not smart home professionals. This was the first time the participants attempt to configure and install such a system. The participants utilized the software that ships with each camera to complete the setup process. The setup process was completed in a short time not exceeding 15 minutes by following the installation steps. The user accepted the default settings for each camera.

4 SURVEILLANCE SYSTEM TROUBLESHOOTING

The surveillance system worked without issues for few days until problems arose. The surveillance cameras stopped capturing images or recording video. Although the participants initially did not encounter any significant issues during the setup and software installation process, the participants faced technical difficulties a few days later by accepting the default installation settings.

4.1 Camera Configuration Settings

During the camera setup phase, the participants configured each camera to obtain its IP address from a DHCP server. The DHCP server in the experimental residence is part of the wireless router, which we will discuss in further detail later in this paper. In such a configuration, when each camera requests an IP address, the DHCP server assigns each camera with an unassigned IP address. This

type of an IP assignment is an address lease. A DHCP IP address lease has a fixed duration. Once the lease expires, a new IP address will be assigned by the DHCP server. There is a high probability that the cameras receive different IP addresses when the IP lease expires. When the participants utilized this camera setup configuration, the participants unknowingly were introducing three main issues with the default surveillance system setup:

- The participants were only able to access the surveillance system from within the home network. The participants did not change any of the router settings and therefore the cameras could not be accessed from outside of the smart home network. The participants fixed this issue by using port forwarding on the wireless router. This is discussed in more detail in the router configuration settings subsection.
- The internal access of the surveillance system was interrupted when the DHCP server IP address lease expired. If the router reboots due to temporary power loss or scheduled maintenance, a new IP address might be assigned and therefore the camera could not be accessed with the previously assigned IP address. The user rectified this issue by assigning an internal IP address to each camera and not relying on the DHCP server for IP address assignments.
- This type of configuration may cause IP address conflicts where a camera and another device on the network like a laptop compete for the same IP address.

4.2 Router Configuration Settings

The router used in this smart home experiment is a Linksys EA4500 model. As mentioned previously, the participants did not change any of the router configurations when the cameras were initially set up, which consequently led to the issue described in A.1. The participants resolved this issue by configuring port forwarding on the router. The new port forwarding configuration allowed the participants to access the surveillance system using a web browser or a mobile application from anywhere (Figure 2).

Figure 2: Accessing camera via a mobile application.

5 DATA MANAGEMENT AND STORAGE

Data management and storage are essential to any surveillance system. Initially, the participants recorded data locally. They utilized Blue Iris software to configure schedules, motion detection, notifications and other features. The participants indicated that they experienced network slow down when collecting data from the six surveillance cameras. This network slow-down could be due to the wireless environment. Such an environment is a shared environment, and all smart devices will compete for bandwidth. Other factors that have an impact on storage are the type of recording the participants choose. They can choose among continuous recording, motion detection recording or a combination of both strategies (Figure 3). The first option clearly fills up storage space at a faster rate than the second option. The second option conserves storage space compared to the two other options but the number of recordings depends on the sensitivity setting of the camera sensors. Depending on how the sensitivity of the sensor is configured, the surveillance system can record video that does not provide valuable information to the user. In this smart home experiment, the Foscam camera motion sensor activates when a slight change in light is detected. Then, the participants receive notifications via a text message or email indicating that motion has been detected. This results in many false alarms that will use storage space and send bogus alerts to the homeowner. The participants eventually lowered the sensor sensitivity level to decrease the number of false alarms.

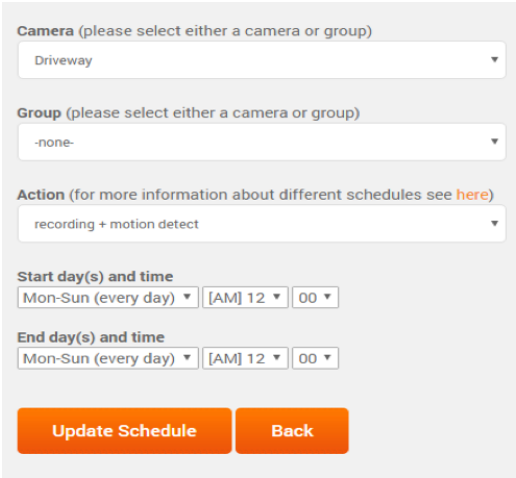

Figure 3: Motion detection and continuous recording Strategy.

Accessing data collected by the Blue Iris software proved to be a challenge for the participants when not on the same network as the surveillance system. It is important that the surveillance data collected can be accessed from anywhere. The participants opted to cloud storage for data management and storage. In this experiment, the participants utilized Mangocam for cloud storage solution. Cloud storage resolves the accessibility problem but introduces data privacy concerns. Our participants did not feel secure using the cloud to store video surveillance and images from cameras inside the smart home. Instead, they utilized the local software (Blue Iris) to perform that task and relied on the cloud to store surveillance outside the smart home. Even with that approach, data privacy is still a major concern.

6 MAINTENANCE OF SMART DEVICES

Maintenance of smart devices can prevent smart device service interruptions and fix potential problems. One type of maintenance is software and firmware updates. One must be prepared to have a backup plan if the update procedure fails and the smart device becomes nonoperational. The participants in our smart home experiment faced another technical challenge when two of the cameras malfunctioned (Figure 4). The participants spent considerable amount of time troubleshooting the problem. They attempted to determine if the failure was a result of network, hardware or software failure. When asked about this issue, one of the participants indicated that troubleshooting was more challenging than the initial configuration of the camera. They also indicated that after spending time troubleshooting the camera, they resorted to resetting the camera to its factory settings. They also confirmed that this approach did not restore the camera to its previous working state.

This experiment emphasizes that the ease of setting up a backup smart device without having to go through the initial installation and setup will make preparing a backup smart device a noncumbersome task for the user. Backing up the configuration settings of all devices will ensure that replacements inherit the same configurations from the original devices. In our scenario, the participants encountered problems with only one of the surveillance cameras and they were physically present. Imagine another scenario where the nonoperational camera is in one location and the participants are at another. This will add another level of challenges to the participants. They have to troubleshoot the device remotely and this could prove to be a very difficult task. Therefore, it is critical that there is a simple and straightforward procedure that the user can follow to maintain and backup smart home devices. This will help improve the overall performance of the smart devices and consequently make smart homes more reliable. Increasing the reliability of a smart home device plays an important role in ensuring the operation of other devices. For example, a surveillance camera would verify that a Wemo light switch is functioning. The camera will capture an image before and after a state change in the Wemo light switch. The initial state is when the Wemo light switch is off, and the final state is when the switch is turned on. This corresponds to change in the room light from an off to an on state.

7 LESSONS AND EARLY EXPERIENCES

7.1 Security and Privacy

Although smart homes are becoming more popular and advances in the smart home technologies have flourished in recent decades and early complicated device deployment systems have been improved into more friendly ones, security and privacy are still major concern and threat to the smart home environment [5, 9, 14, 16, 18]. Smart homes are vulnerable to outside attacks and therefore user privacy threats are real. Recently, it was announced that millions of IoT devices were hit by a bug in an open source code library. The flaw in widely-used code library has exposed Axis Communications security cameras to remote attacks. The flaw in the open source code library enables hackers to continually reboot security cameras and block the owner from viewing the video feed. This is an extremely dangerous scenario because the attacker is able to reset the security camera to its factory settings and then change its credentials. The attacker now has complete control of the device and is able to view and record the video feed. Axis Communications confirmed that over 99% of its surveillance camera models were affected by the flaw [4]. Such security flaws are not restricted to open source software. The Foscam cameras used in our experiment had their share of security flaws. F-Secure researchers discovered that some camera models cannot be protected by just changing their default credentials. F-secure has identified over a dozen vulnerabilities in the cameras that will allow a hacker to take control of the camera. In this case, researches identify how companies neglect software hardening [1].

Figure 4: Nonoperational cameras.

7.2 Latency

In a smart home, response time is an important criterion to determine whether a smart home experience is satisfactory or not. Back in 1968, Miller described computer mainframe responsiveness in three different orders of magnitude [12]: (1) 100 ms is perceived as instantaneous; (2) 1 second or less is fast enough for the user to interact with the system in a free way; (3) 10 seconds or more reduces the user's interest. Generally speaking, controlling the response time under 1 second is sufficient for the satisfactory functionality of the smart home implementation, and meeting user expectations. The participants in our home smart experiment complained about latency. Those complaints are shared with many smart home users. In one instance, a smart home user talked about her experience with a wireless IP camera. She briefly discussed how easy the initial setup was and talked about her experience afterwards. This was similar to the experience our smart home participants encountered. When commenting on latency, she labeled latency as dreadful by explaining how it was faster to walk into the room where the camera is than viewing the camera feed of the same room on her smartphone

using WiFi. To resolve this issue, she powered the camera on and off. This solution was feasible when she was inside the house [2].

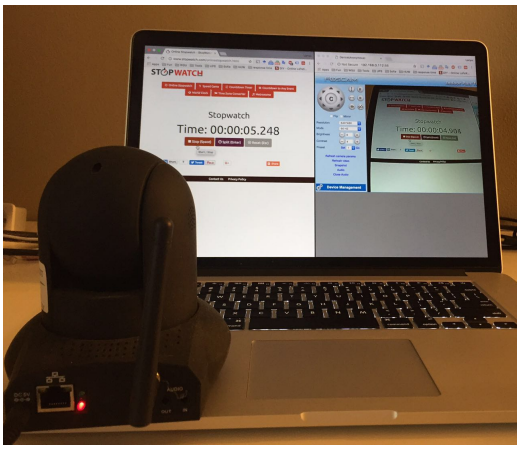

Figure 5: Camera latency measurement.

To provide better understanding of latency in a smart home environment, we ran an experiment in the environment similar to the one that our participants were involved in. The approximate network download and upload speeds are 21 Mbps and 6 Mbps respectively. We employed Foscam FI8910W to measure latency in two different scenarios: (1)*Baseline*: No significant network activities, such as camera video upload, Online video streaming, Large file downloads and so on, take place; (2)*Video Stream Upload*: Five Foscam cameras uploading video stream to the cloud; As an alternative of intrusive programming, we positioned one camera in front of a laptop display observing an online stopwatch. The same computer was used to display both the stopwatch and the stopwatch video stream as shown in Figure 5. This ensures accuracy in timing the delay between the stopwatch and its video feed. The time between the images being displayed and detected was recorded. The same process can be used to analyze a variety of configurations including different camera models, different image sizes and compression levels, where the camera supports these, and different network configurations [8]. If we assume T_1 is the stopwatch time and T_2 is the stopwatch time from the video feed, then latency is ΔT ($|T_1 - T_2|$). Table 1 shows measurements for running the stopwatch experiment for Foscam camera. For each scenario, we recorded a 30 second video, then played back the video to record T_1 and T_2. The latency is calculated in milliseconds by averaging ΔT ($latency = \frac{\sum_{i=1}^{N} \Delta T}{N}$ where N is the number of experimental runs).

As expected, the results in Table 1 above show that latency and network load are directly proportional. In other words, the increase in network traffic leads to an increase in latency. In our experiment, it comes to no surprise that latency increased by 34% from scenario 1 to scenario 2.

7.3 Usefulness

In addition to the dreadful latency described by the smart home user in the previous subsection, she indicated that it was too hard to use the camera when she was out and about. The camera deemed to be unuseful when the user was outside and had more need for it. Our smart home participants faced disconnectivity issues with the wireless range extender. When that happens, the garage and backyard cameras became nonoperational. As a workaround, the participants used the available smart plug switch as a means to reboot the wireless range extender remotely when necessary. Studies have shown that the growth in homeowner adoption of smart homes is declining due to the users' lack of confidence in the reliability of connected smart devices. Because of reliability issues, users tend to abandon the idea of transforming their homes into smart ones.

Table 1: Latency measurement of Foscam FI8910W.

Scenario	Run	T_1	T_2	ΔT (ms)	Latency Average (ms)
Baseline	1	00:00.000	00:00.252	252	324.5
	2	00:00.000	00:00.241	241	
	3	00:00.000	00:00.514	514	
	4	00:00.000	00:00.291	291	
Video Stream Upload	1	00:00.000	00:00.338	338	435.0
	2	00:00.000	00:00.498	498	
	3	00:00.000	00:00.399	339	
	4	00:00.000	00:00.565	565	

There are many reasons why such issues arise. One of the main factors is bandwidth. Usually, bandwidth is not a critical factor when controlling smart home devices. Most of smart home devices use minimal amount of data that is sent back and forth to the device. It is sent in the form of commands and received back in the form of status information. If that's the case, why do smart home users (our participants included) complain about latency? Cameras, being the exception, are one of the devices that consume a large chunk of bandwidth. The higher the video quality, the more portion of bandwidth will be utilized. The participants in our smart home experiment used the cloud as a means for storage. That required compressed video to be continuously uploaded to the cloud. The video upload will occupy a large portion of bandwidth depending on the video quality. Therefore, it comes to no surprise that the participants noticed significant latency in the limited home network bandwidth. There are several workarounds to the bandwidth bottleneck. For example, one is reducing the video quality or recording video in black and white rather than in colors if possible. Another is ensuring that the wireless router speed does not directly affect the bandwidth speed. The network speed a smart home user experiences is determined by the slower speed between the bandwidth and the router. To promote better smart home user experience and overcome many of the issues discussed in this subsection, we will motivate discussion about edge computing in the next subsection.

7.4 Edge Computing Needed

Thanks to the burgeoning of IoT, more and more devices and applications are coming out for it, especially low-cost, small but powerful sensors and chips that can be deployed easily in the domestic environment [11]. Considering the pending issues that generally exist

in a smart home as we mentioned above, shifting the computing from PC, mobile device, and cloud to the things at the edge of the network is a potential solution [15]. As we discussed in the previous subsection, some IoT devices use more bandwidth than others. Our participants in the smart home experiment experienced network slow down especially when they selected the cloud to store video stream. Even though the data-processing speeds have improved greatly, network bandwidth that transfers data to and from the cloud has not increased at the same rate. Therefore, with IoT devices generating more data, network bandwidth is becoming the cloud computing's bottleneck [5].

In our smart home experiment, although the surveillance cameras capture and send a huge amount of video data to the cloud without the need to do real time processing, other scenarios might be different requiring data to be processed in the cloud. For example, assume that our participants will use the video data stored in the cloud to set the smart thermostat temperature. In this case, the data is sent to the cloud for processing resulting in increased latency. One solution is to process data at the network edge yielding more efficient computing, less bandwidth utilization, and shorter response times. In addition to the bandwidth issue, there is a significant cost associated with cloud storage. One can argue that instead of the network edge approach, one can configure and install a Network-Attached Storage (NAS). This is a valid argument except that configuring and installing such a system requires a considerable amount of knowledge and expertise. That is not the only drawback of a NAS system. Cost is another factor. It should be obvious that cost, bandwidth, and storage play an important role in the popularity of smart homes. If cost is high, bandwidth is congested, and storage is expensive and not properly secured, a typical home owner will probably not explore the smart home path. Thus, storing data at the edge of the network could be a decent way to protect user privacy and reduce cost. Hence, edge computing could be a potential solution to the smart home environment allowing computation and storage to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of IoT devices [5].

8 CONCLUSION AND SUGGESTIONS

In this paper, we discussed the experience of a typical homeowner taking on a DIY smart home project. The project consisted of six wireless surveillance cameras and few other devices. We discussed many facets of setting up a wireless camera system in a smart home: installation, configuration, troubleshooting, data management and storage, and maintenance. A DIY like this one will help the user to learn more about smart home devices and be self-reliant when it comes to enhancing smart home features. The learning experience will also reduce cost and prove to be vital when troubleshooting is required. Smart home technology is still in its infancy. Multiple smart home devices require multiple applications and programs. They also require some technical expertise to install, configure, backup and maintain. This all affects the experience of an average user in a negative way. Smart home devices receive lot of negative feedback that is sometimes due to the complexity of device configuration, maintenance, and usefulness. If some or all of these issues are resolved, a homeowner is more likely to convert his/her home to a smart one. For example, complexity is reduced if one application is required for multiple devices ranging from a smart thermostat to a smart door lock; therefore, a one-to-many mapping between application and devices is necessary to make the DIY experience easier and more pleasant to an average user. Also, the shift from data processing in the cloud to the edge of the network can dramatically improve bandwidth bottlenecks. As we move forward in time, smart homes will move from being a hobby to a ubiquitous home product.

REFERENCES

[1] 2017. F-Secure. (July 2017). Retrieved 07-27-2017 from https://business.f-secure.com/

[2] 2017. Foscam C1 Lite HD Wireless Camera: Good hardware, poor control. (July 2017). Retrieved 07-27-2017 from http://www.zdnet.com/product/foscam-c1-lite-hd-wireless-camera/

[3] 2017. Smart Homes, Buildings (Energy Efficient, Automated) Market by Application (Energy management, Lighting control, HVAC, Safety and Security, Home healthcare and child safety) and Technology (Bluetooth, Zigbee, RFID, Wi-Fi) - Global Opportunity Analysis and Industry Forecast, 2013 - 2020. (Aug. 2017). Retrieved 08-07-2017 from https://www.alliedmarketresearch.com/smart-home-automated-building-market

[4] 2017. ZDNet. (July 2017). Retrieved 07-27-2017 from http://www.zdnet.com/

[5] Jie Cao, Lanyu Xu, Raef Abdallah, and Weisong Shi. 2017. EdgeOS_H: A Home Operating System for Internet of Everything. In *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 1756–1764.

[6] Prafulla Nath Dawadi, Diane Joyce Cook, and Maureen Schmitter-Edgecombe. 2016. Automated cognitive health assessment from smart home-based behavior data. *IEEE journal of biomedical and health informatics* 20, 4 (2016), 1188–1194.

[7] Biyi Fang, Qiumin Xu, Taiwoo Park, and Mi Zhang. 2016. AirSense: an intelligent home-based sensing system for indoor air quality analytics. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 109–119.

[8] Rhys Hill, Christopher Madden, Anton van den Hengel, Henry Detmold, and Anthony Dick. 2009. Measuring latency for video surveillance systems. In *Digital Image Computing: Techniques and Applications, 2009. DICTA'09*. IEEE, 89–95.

[9] Peng Huang, Tianyin Xu, Xinxin Jin, and Yuanyuan Zhou. 2016. Defdroid: Towards a more defensive mobile os against disruptive app behavior. In *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 221–234.

[10] Andreas Jacobsson, Martin Boldt, and Bengt Carlsson. 2016. A risk analysis of a smart home automation system. *Future Generation Computer Systems* 56 (2016), 719–733.

[11] Nanyan Jiang, Cristina Schmidt, Vincent Matossian, and Manish Parashar. 2004. Enabling applications in sensor-based pervasive environments. In *Proceedings of the 1st Workshop on Broadband Advanced Sensor Networks (BaseNets 2004)*. 48.

[12] Robert B Miller. 1968. Response time in man-computer conversational transactions. In *Proceedings of the December 9-11, 1968, fall joint computer conference, part I*. ACM, 267–277.

[13] Pooshkar Rajiv, Rohit Raj, and Mahesh Chandra. 2016. Email based remote access and surveillance system for smart home infrastructure. *Perspectives in Science* 8 (2016), 459–461.

[14] Nazir Saleheen, Supriyo Chakraborty, Nasir Ali, Md Mahbubur Rahman, Syed Monowar Hossain, Rummana Bari, Eugene Buder, Mani Srivastava, and Santosh Kumar. 2016. mSieve: differential behavioral privacy in time series of mobile sensor data. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 706–717.

[15] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. 2016. Edge computing: Vision and challenges. *IEEE Internet of Things Journal* 3, 5 (2016), 637–646.

[16] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers. 2016. Twenty security considerations for cloud-supported Internet of Things. *IEEE Internet of Things Journal* 3, 3 (2016), 269–284.

[17] Biljana L Risteska Stojkoska and Kire V Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production* 140 (2017), 1454–1464.

[18] Frank Wang, Catherine Yun, Shafi Goldwasser, Vinod Vaikuntanathan, and Matei Zaharia. 2017. Splinter: Practical Private Queries on Public Data.. In *NSDI*. 299–313.

[19] Jong-bum Woo and Youn-kyung Lim. 2015. User experience in do-it-yourself-style smart homes. In *Proceedings of the 2015 ACM international joint conference on pervasive and ubiquitous computing*. ACM, 779–790.