University of Regina

PROJECT PROGRESS REPORT

A Survey on IoT- Based Smart Home Applications

Course; Topic on Communications

Course code; CS890DH

Submitted to: Dr. Maher Elshakankiri

Oluwatobi Adegbola

200397493

2019-02-22

Table of contents

1.0 Introduction

The internet of thing is fast changing how we interact with our environment especially how we interact with our homes and the appliances in it. IoT describes a technological concept where all the things around us from animals(Liu et al. 2015) to home appliances have digital identities(Yie et al. 2013) and are connected to the internet in such a way that they can share data about their current state and perform actions when possible based on instructions sent to them via the internet. This has revolutionized the way a lot of things are being done, from parks using IoT to monitor animals and trees to industries using IoT to monitor machines and heavy equipment.

Homes also have not been left out of this revolution. Traditional smart home systems in time past usually come with basic time controlled or remote controlled automations but with IoT, homes now respond in real time to changes around them and provide the occupants with the opportunity of monitoring their homes from wherever they are, taking actions with tap of a single buttons to turn on/off appliances. The paper being developed, examines IoT-based smart home applications via a survey of previous works that has been done on the topic, evaluating the underlying components of its architecture including the sensors, communication modes, protocols and security features. The paper also examines the current state of IoT-based smart home applications including the challenges being faced, solutions being adopted and the possible future trends and applications of IoT based smart home systems.

This report provides an update on the work that has been done. So far, a total of 3 chapters has been written including the literature review. For the literature review , about 25 literatures including journal papers, conference papers, and whitepapers related to the topic has been

reviewed to identify the trends, technologies, and use cases that have been covered in previous works around the topic. Extracts from these papers are currently being used to build the survey.

2.0 Literature Review

In order to examine the amount of work that has been done around this topic and critically evaluate their observations, several papers were reviewed. The papers were evaluated along the focus of our survey to identify trends around the key components which make up the IoT-based smart home architecture including; sensors, communication, data processing techniques, protocols, and security.

One of the most notable papers which has been examined is the work of Jiang et al (2018) around Sensing in IoT based smart home systems. They created a survey on the recent applications of Wi-Fi sensing in smart home systems. Wi-Fi Sensing refers to a technology concept in which Wi-Fi signals and radios are being used to sense the environment instead of the traditional sensors. A good example of the application of this sensing technique is the detection of sudden fall which is important when monitoring the health of elderly persons. Jiang et all (2018) referenced the works of Wang et all (2016) which used distortions in CSI (Channel State Information) of Wi-Fi signals to detect sudden falls with about 87% accuracy. The Survey examined other applications of Wi-Fi sensing under categories including; Health Monitoring, Gesture recognition, Contextual information (e.g. Location) Acquisition, and for Authentication related applications like Access control.

As the number of smart home applications grow, one of the, major dilemmas faced is combining them together due to lack of interoperability between devices. From different communication protocols to different message structure, users sometimes have to switch between platforms to access data. This is however changing as platforms (Software and hardware) are being developed to solve this challenge. This was the focus of Patru et all(2016) in their paper “Smart Home IoT

System". They presented a solution that integrates different home automation solutions into just one application making it easy for users to monitor and take action. The solution enables the connection of multiple smart home devices into an entity, accessible on a single application.

Zaidan et al(2018) carried out a survey to the examine the communication concepts in IoT based smart home solutions. They retrieved over 82 papers across diverse databases, examined and categorized them into four groups. The first group discussed articles that discussed frameworks and models for IoT devices, the second group contained articles that focused on the analytical evaluation of case studies, identifying the difference in the variables while the third and fourth category focused on papers that did a worth or merit assessment and papers that conducted reviews of IoT communication components respectively. All of the information from the papers evaluated was then used to provide a clear description of communication systems in IoT stressing the approaches and limitations of existing systems.

The architecture of a typical IoT-based smart home solution feature the transmission a generated data by sensors to a remote cloud via the internet. This can sometimes not be scalable and exhibit certain limitation along the lines of speed, security and the real time nature which is desired. To this, Sun and Ansari (2016) proposed a solution that involved the use of Mobile edge computing for IoT to facilitate data processing at the mobile edge. The paper proposed an implementation of a hierarchical architecture for fog computing in each of the fog nodes such that flexible services are provided with user privacy, protected. Each IoT device is associated with a proxy Virtual Machine, which will collects and analyzes raw data from the device, convert it into metadata, and transmit the metadata to corresponding application virtual machines which then uses the received metadata to service its users.

Security has been one of the major cause of concerns for IoT-based smart home systems and this was one of the topics evaluated by Vashi et al (2017). The paper discusses the Architecture of IoT systems, stating its complexity and vulnerabilities as the number of connected devices increases. It enumerates some of the security challenges this systems can encounter and also recommended possible measures to prevent breaches.

In similar directions as above, Ali et al (2017) Investigates common attacks on IoT based smart home systems and evaluates the level of disruption that occurs in the smart home system as a result this attacks. The paper specifies security requirements and proposed that security goals should be set for smart home systems using this requirements as a solution to security challenges. In conclusion, the paper uses data analysis to predict the types, targets and severity of future attacks on IoT based smart home systems.

These papers and the rest being studied, provided key information for the development of the smart home application survey.

3.0 IoT Based Smart Home Architecture

Traditional smart home systems feature devices which perform more of automation based tasks and shouldn't in the real sense be called smart as those system generally do not make any decision on their own. They usually only respond to preprogrammed decisions e.g. a thermostat which turns off when its preset temperature is attained and turns back on when the temperature drops. This settings makes the system simple and easy to implement. IoT based smart home systems on the other hand, involve a plethora of devices including sensors and actuators and have the ability acquire data, store them, analyze them for patterns and take actions based on those decisions. Using the same thermostat example, this means instead of user preset temperature, the system is able to obtain the temperature of the surroundings and based on that adjust itself to match the health and wellness needs of the user without the need to adjust the preset temperature as the case is with the thermostat. This brings a lot of complexity to the system, from the communication between the devices, to the storage and processing of the data and other things like security in between. This complexity is represented by the architecture of the system.

The architecture implemented for each system determines how the devices communicate, the protocols being used, the storage platform, how data is processed, how trends in the data are extracted and how the system used the extracted information.

Quite a number of IoT architecture for smart home systems have been developed. The architectures include seemingly simple architectures like the one developed by Soliman et al(2013) which involved the use of Zigbee based data hubs which obtains data from sensors using the zigbee communication protocol and uploads to a cloud solution which then processes the data and makes it available to the user via an application interface(webpages) to enable them monitor their homes in real time.

Irrespective of the Architecture adopted, the key components of the system usually include;

1. Sensors/Actuators
2. Communication systems
3. Data Processing and visualization
4. Protocols

3.1 Sensors

Sensor provides systems with a medium of measuring physical properties. They are usually infused with transducing elements which convert physical quantities into quantities recognized by the system which is usually to voltage, resistance in electronics based systems. In IoT based smart home systems, this sensors are usually infused with communication capabilities which allows then send the data obtained to either a data concentrator or to cloud applications based on the architecture on which the system was built. Sensing elements in IoT systems are fast advancing beyond the days of traditional sensing techniques like photovoltaic cells to determine light intensity. The design of sensing elements in recent times has focused on the use of more non-invasive/ passive sensors, a good example of which is the Use of WiFi signals (Wang et al. 2017) by smart home systems to measure health and security related parameters. Many more Sensing advances will be discussed in the paper itself alongside other components of the IoT based smart home architecture.

4.0 Additional Work

About 10 more literatures will be reviewed within the scope of the paper to ensure accuracy after which the other parts of the survey will be developed based on the literatures.

5.0 References

Ali, W., Dustgeer, G., Awais, M. and Shah, M.A., 2017, September. IoT based smart home: Security challenges, security requirements and solutions. In *2017 23rd International Conference on Automation and Computing (ICAC)* (pp. 1-6). IEEE.

Jiang, H., Cai, C., Ma, X., Yang, Y. and Liu, J., 2018. Smart home based on WiFi sensing: A survey. *IEEE Access*, *6*, pp.13317-13325.

Jie, Y., Pei, J.Y., Jun, L., Yun, G. and Wei, X., 2013, June. Smart home system based on iot technologies. In *2013 International Conference on Computational and Information Sciences* (pp. 1789-1791). IEEE.

Liu, X., Yang, T. and Yan, B., 2015, November. Internet of Things for wildlife monitoring. In *2015 IEEE/CIC International Conference on Communications in China-Workshops (CIC/ICCC)* (pp. 62-66). IEEE.

Pătru, I.I., Carabaş, M., Bărbulescu, M. and Gheorghe, L., 2016, September. Smart home IoT system. In *2016 15th RoEduNet Conference: Networking in Education and Research* (pp. 1-6). IEEE.

Soliman, M., Abiodun, T., Hamouda, T., Zhou, J. and Lung, C.H., 2013, December. Smart home: Integrating internet of things with web services and cloud computing. In *2013 IEEE 5th international conference on cloud computing technology and science* (Vol. 2, pp. 317-320). IEEE.

Sun, X. and Ansari, N., 2016. EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Communications Magazine*, *54*(12), pp.22-29.

Vashi, S., Ram, J., Modi, J., Verma, S. and Prakash, C., 2017, February. Internet of Things (IoT): A vision, architectural elements, and security issues. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 492-496). IEEE.

Wang, Y., Wu, K. and Ni, L.M., 2017. Wifall: Device-free fall detection by wireless networks. *IEEE Transactions on Mobile Computing*, *16*(2), pp.581-594.

Zaidan, A.A., Zaidan, B.B., Qahtan, M.Y., Albahri, O.S., Albahri, A.S., Alaa, M., Jumaah, F.M., Talal, M., Tan, K.L., Shir, W.L. and Lim, C.K., 2018. A survey on communication components for IoT-based technologies in smart homes. *Telecommunication Systems*, *69*(1), pp.1-25. https://doi.org/10.1007/s11235-018-0430-8