Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 5 Issue 11, November - 2018

Modular Architecture for IoT Home Automation and Security Surveillance

Kuo-pao Yang, Garth Kiepper, Benjamin Henry, Richard Hunter
Computer Science Department
Southeastern Louisiana University
Hammond, LA 70402 USA

***Abstract*— This paper presents modular architecture for home automation and security using Internet of Things (IoT) devices. This home automation and security system is explored using a customizable and modular approach by connecting a variety of IoT devices to microcontrollers. This approach is compared to purpose-built systems using commercial, off-the-shelf hardware.**

Keywords*— *home automation; home security; prototype; microcontrollers; motion sensors

I. Introduction

Most home automation and security systems involve selecting a pre-packaged setup from a vendor. Such systems are usually composed of the Passive Infrared Sensor (PIR) motion sensors for hallways and living rooms, magnetic reed sensors for exterior doors, and video cameras pointed at the main points of entry for the front and back doors. These vendors typically offer different tiers of protection where customers can increase system capabilities by purchasing additional sensors, such as placing a magnetic reed sensor on each window and adding additional security cameras.

These types of pre-packaged systems delivered by vendors are inferior since the base level of protection comes with only enough sensors for an average home. If consumers need more doors to their home, they must pay for a more advanced tier of security. This monetary barrier discourages consumers from choosing the appropriate level of protection for their home. Therefore, most consumers select the basic level of protection without choosing the required number of sensors. In addition to paying for sensors, all reputable vendors charge a monthly fee that increases for each video surveillance camera added to the system.

Another shortcoming of these pre-packaged systems is that they are mass-manufactured, which leads to the development of software exploitation due to security vulnerabilities and bugs. A homogenous mass-manufactured system is not desired since it can impair the privacy of consumers and allow hackers to eavesdrop video surveillance even without access to the video hardware [1]. For example, consumers that pick ADT as their security vendor are required to use Vivotek brand cameras. This brand is known to have a security vulnerability where attackers can view the video feed remotely. If an attacker knows a consumer uses this vendor, they are aware of common faults. Instead of being forced to take a vendor's only product, consumers can gain security through obscurity by selecting video cameras of their choice. By letting consumers pick their own video camera hardware, attackers will not be able to identify common faults associated with certain vendors. It is important to deliver a customized, heterogeneous system for each consumer.

Our solution for home automation and security is worth considering since it achieves greater affordability by allowing consumers to use existing sensors and video cameras they already have. If users want to add more cameras, they can select the desired brand and model themselves instead of being forced to choose a specific model offered by a vendor. Additionally, this system provides the ability to customize actions in response to certain triggers. For example, when motion is triggered by a user walking by, the lights can be turned on. This is customized by zoning lights into different groups controlled by individual motion sensors. As a result, when the user is moving in the kitchen, the motion sensor would trigger for only that room and the lights in that zone will turn on. If the user moves in the hallway, a different motion sensor will be triggered, causing the lights in the hallway zone to be turned on. The user has ultimate control over the functionality of the home automation and security system and can customize it as they see fit.

This paper reflects on existing implementations in the realm of home automation and security using Internet of Things (IoT) devices. It discusses the solution which utilizes hardware and software components to protect a home's entry points, provides fixed video surveillance, and offers mobile video surveillance via the security land robot. Full implementations are presented in detail. Finally, this paper shows the results of what this home automation and security system has achieved, difficulties it has overcame, and provides ideas for future areas of research.

II. Related Work

Many architectures are available for home automation. The homeBLOX provides process-driven home automation through simple, graph-based interfaces [2]. Although it provides an easy user interface, the homeBLOX lacks modern IoT infrastructure. This architecture for home automation is improved by offering a similarly easy-to-use interface via the web-application, while providing increased compatibility with modern devices such as Google Home and Phillips Hue.

This home automation and security system design focuses on networking sensors with a hard-wired connection wherever possible. Another architecture for home security suggests that it is important to jam unwanted wireless devices because they pose a security threat to the software backbone of the home security network [3] [4]. Instead of using Wi-Fi, Zigbee, or other third-party wireless protocols, this system adopts I2C, serial, and one-wire connectivity to mitigate the security vulnerabilities posed from wireless networks.

This home automation and security system also considers wireless signals being involved as a point of network security. Wireless signals are used as a point of intelligence to gain insight as to the proximity of nearby Wi-Fi devices. This system is able to detect wireless devices inside the home, outside the home, and within the surrounding neighborhood. Furthermore, this home security system can also distinguish between devices that frequently appear in the home and devices that are uncommon. When new devices are identified, their presence is logged. This allows to retroactively pinpoint who was near the home when an incident occurs.

Another architecture for designing a network of IoT devices utilizes the Power-Line Communication (PLC) by transmitting data over pre-existing electrical ground lines instead of creating new wiring dedicated to security systems in homes [5]. This conservative approach is lack of robust communications associated with PLC. For example, the X10 communications protocol relies on power line communication. However, this protocol is lossy and requires sending messages multiple times. Additionally, if any nearby electrical devices create a surge, communication with sensors is lost. For these reasons, this system runs additional wiring for data acquisition sensors. In locations that need both power and network connectivity such as video surveillance cameras on the exterior of the home, this system uses the Power-Over-Ethernet (POE) technology, where networking infrastructure provides data and power over a single ethernet cable.

Other methodologies focus on the use of a single microcontroller such as Raspberry Pi to provide a low-cost hybrid solution for home automation [6]. Rather than choosing Arduino, Raspberry Pi [7] is adopted since it provides significantly more computational resources and supports a wide range of protocols such as fast ethernet, which Arduino cannot provide. To integrate with a wide range of devices such as Phillips Hue lighting, Google Home speakers, and other IoT devices, the advanced ARM CPU is required and provided by the Raspberry Pi. Furthermore, Raspberry Pi can also easily maintain the heterogeneous infrastructure of multiple IoT devices on the network [8].

III. Implementation

A. Magnetic Reed Sensors

The first level of security is supported by the magnetic reed sensors on the doors and windows. They work by showing an alternating current when the door is opened and a constant open current when the door is closed. Coding around this feature is done by simply adding a counter that was directly related to the amount of time between alternating fulgurations. For example, this feature can set the alarm to go off when there is no current for more than 2 second.

B. PIR Motion Sensors

The PIR sensors are used for motion detection. They detect infrared heat signatures, so the Phillips Hue Lights as opposed to normal incandescent bulbs are an excellent fit. The purpose of the motion detectors is bifold, detecting movement inside the house in case the first level of security is broken or down and as an everyday household feature controlling the household lighting for improved efficiency [9] [10].

C. Video Surveillance

There are eight 4-megapixel resolution (2560x1440) IP cameras to cover all the windows and doors. Cameras are positioned outside to cover the break-in zones and cover the package delivery zone to offer an IoT based surveillance solution [11]. This level of detail comes at a cost using 360GB of recorded footage per day. This footage is stored on an external USB hard disk that is connected to Raspberry Pi.

D. Google Home Mini Audio

Google home mini audio has a two-fold purpose. It offers the convenient feature of voice commands to turn on and off the lights, as well as other electronics including the security system itself, providing the sound support for the alarm, and changing the color of the lights inside the house. Python programming language is implemented to integrate with the whole-house Google Home audio system by streaming MP3’s to it. It can send audible alerts when a break-in is detected.

E. Phillips Hue Lighting

There are fifteen Phillips Hue lightbulbs which communicate with the Phillips Hue bridge. This works via a REST (REpresentational State Transfer) web API (Application Program Interface) that the user is able to control via Python to turn individual lights on or off, and change the hue, saturation, and brightness to achieve different colors. This contributes to the home security system because the Hue lights are able to flash red and blue when a break-in is detected. Additionally, when the user moves between rooms in the house, the lights turn on when passing from room to room. Python is able to control the timeouts for each light and turn off the lights after a specified interval such as 10 minutes when no motion or activity is detected in a given room. It not only improves the aesthetics of the home but also helps conserve electricity through human-building interaction [12].

The Phillips Hue lighting uses the Tint Saturation Luminance (TSL) color space. The TSL defines color as tint, saturation, and lightness. This is significantly different than the standard Red Green Blue (RGB) color space that is conventionally used in web programming.

F. Security Robot

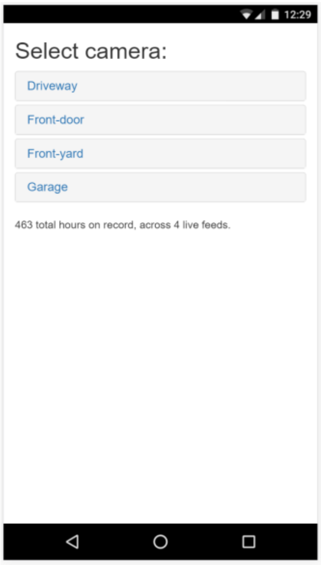
There are four 12V motors used to power the security robot. These motors are selected because they use the same voltage as 12V lead acid battery. These particular motors have a gear reduction box for 6000 RPM to 30 RPM speed. These motors give about 0.5 miles per hour of speed and provide 12 Kg cm force to power the robot.

There are two relays to move each motor forwards and backwards. Thus, these four relays are able to achieve zero-radius turning since each relay has a connection to both positive and ground. It connects the appropriate signal to each motor terminal and can flip flop between clockwise and counterclockwise movement with this circuit.

The MAX471 integrated circuit is used to detect the amount of current used by each motor. This data is integrated by the Python script on the robot so that stalling motors can be powered off before they burn out. This ensures the robot is able to move smoothly without being damaged.

G. Software

A web application is coded in PHP, HTML5, and CSS3 for both viewing security footage as well as arming and disarming the house. Bash scripts are used on the backend since the Raspberry Pi runs Linux. It can process video feeds and save them to the external hard disk drive. Also, a cronjob in Linux is used so that old video recordings are automatically deleted every 30 days. Therefore, the surveillance system will not run out of storage space. This web interface for viewing security footage is shown in Fig. 1.



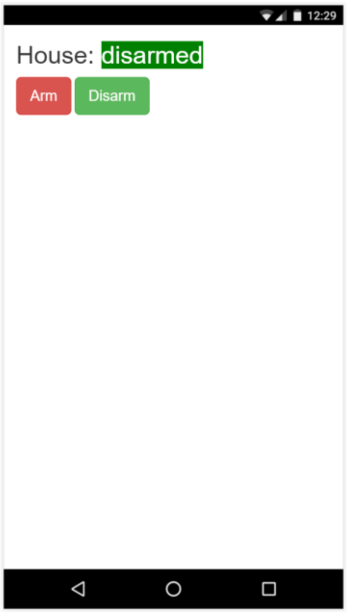
Select camera:

- Driveway
- Front-door
- Front-yard
- Garage

463 total hours on record, across 4 live feeds.

Fig. 1. *Web Interface for Viewing Security Footage*

A Raspberry Pi acts as the server for the system and provides the connection that enables control over the system. A PHP web application is implemented for arming the security system. This web application communicates with the Python script to monitor all sensory inputs. When the user arms, this system stores the state in a file. Python reads the state from this file every 100ms and triggers an alarm if sensors are triggered during an arm state. This web interface for arming and disarming house is shown in Fig. 2.



House: disarmed

Fig. 2. *Web Interface for Arming / Disarming House*

IV. Evauation

This home automation and security solution is tested on Raspberry Pi by constructing a mock house out of wood. This house contains two rooms and has exterior doors on the left and right sides. These exterior doors are wired with the magnetic reed sensors and connect to the Raspberry Pi so that it can detect when doors are opened and closed. Additionally, each room has a PIR motion sensor, which can be seen mounted on the doorway dividing the two mock rooms. This house is shown in the Fig. 3.

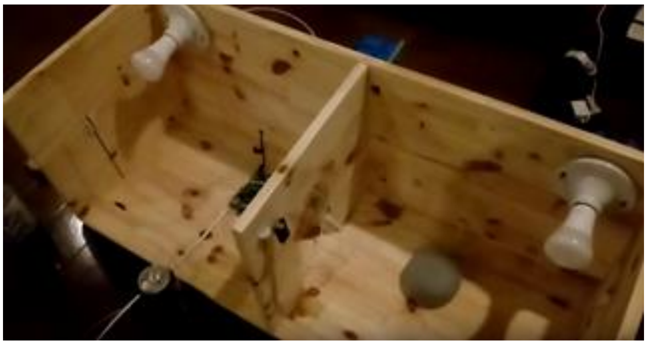


Fig. 3. *Prototype House Wired for Two Rooms*

Inside this mock house, a Google Home device provides audible alerts. Whenever motion is detected, the light in that room is illuminated. To test the light timeouts, the timeout is set to 2 seconds. Raspberry Pi is able to continually observe motion activity in a room and leave the light on while the room is occupied. For all given sensor inputs, spoken feedbacks are provided for debugging purposes. The following messages are spoken using the Google home:

- Left door opened
- Left door closed
- Right door opened
- Right door closed
- Motion in left room
- Motion in right room
- Break-in detected. Alert! Alert!
- System silenced. System disarmed.

A laptop is used for testing the web application to arm and disarm the security system shown in Fig. 4. Testing on a laptop quickly triggers the alarm on this prototype house by opening a door. Then, the alarm can be silenced by clicking disarm.

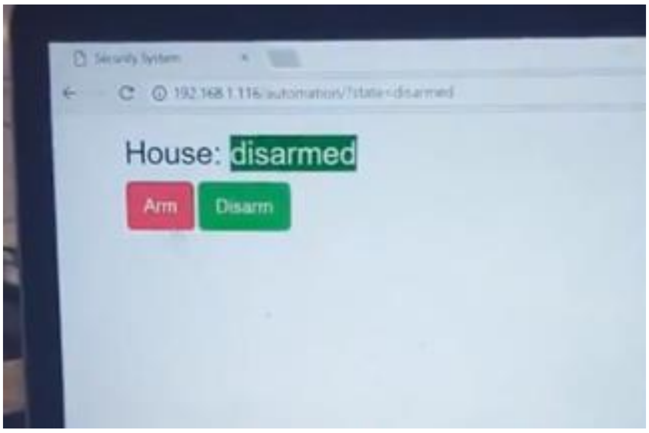


Fig. 4. *Laptop Testing the Security Arm / Disarm Website*

In Fig. 5, the security land robot has full movement capabilities indoors and outdoors.

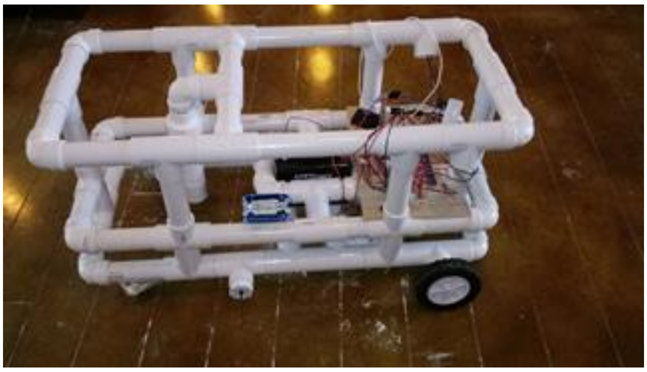


Fig. 5. *Security Land Robot*

A web interface is used to access the security robot's front-mounted camera. This enables to see a live stream of the robot's movement so that users can control it remotely. In Fig. 6, the SSH controls start the Python script to move the robot. The left, right, up, down arrow keys are used to change the direction of the robot and drive it around the house.

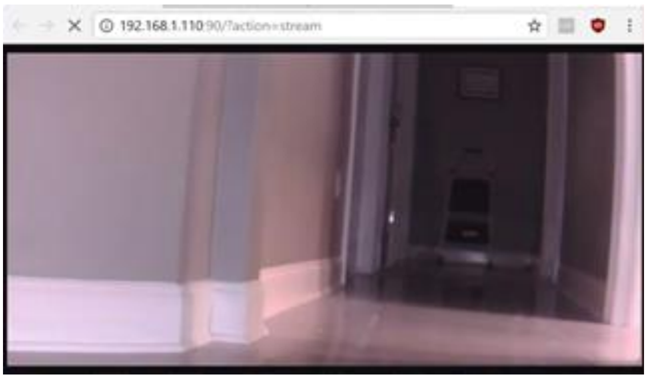


Fig. 6. *Land Robot Video Feed*

Other camera feeds also have a web interface. Their live stream can be viewed on PC or phone remotely. Fig. 7 shows a view of the driveway where a vehicle is parked in front of the house. Eight cameras are strategically positioned around the house to deliver full video coverage.

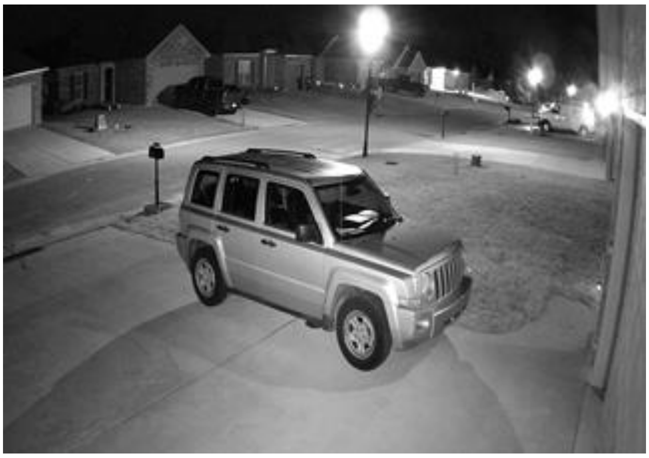


Fig. 7. *Surveillance Camera Video Feed from House Exterior*

In Fig. 8, this system is also able to use automated license plate recognition to track vehicles common to the neighborhood. The cameras work well during the day time, but they do not have the ability to read license plates at night, which is an automation challenge [13] in the future.

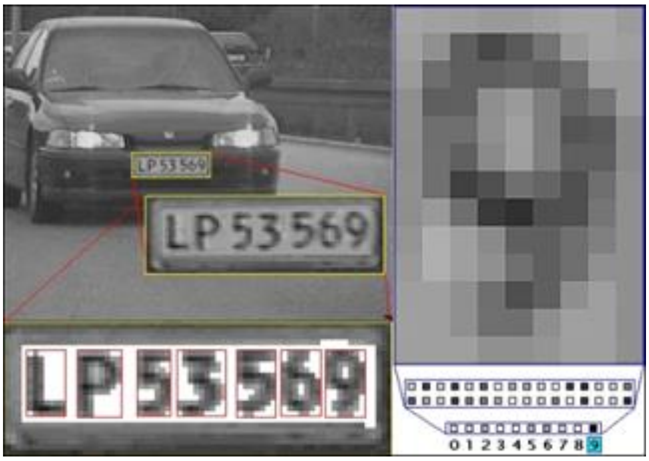


Fig. 8. *Surveillance Camera Video Feed from House Exterior*

V. Conclusion

In conclusion, the heterogenous infrastructure of IoT devices employed in this paper reflect a complete home automation and security system that rivals the capability of a commercial solution available for purchase from a vendor. This system is able to achieve surveillance, integrate with a variety of hardware sensors, and further integrate with modern technologies such as Google Home and Phillips Hue lighting. Future research can be performed in computer vision to achieve additional intelligence of the surroundings of a modern smart home by detecting license plates automatically.

References

[1] J. Obermaier and M. Hutle, "Analyzing the security and privacy of cloud-based video surveillance systems," IoTPTS '16 ACM International Workshop on IoT Privacy, Trust, and Security, pp. 22-28, 2016.

[2] M. Rietzler, F. Schaub, J. Greim, B. Wiedersheim, M. Walch, and M. Weber, "homeBLOX: introducing process-driven home automation," UbiComp '13 Adjunct ACM Conference on Pervasive and Ubiquitous computing, pp. 801-808, 2013.

[3] K. Yang, R. Dejean, C. Clapp, R. Banks, D. Raygadas, I. Bendanas, "Network security practical concepts, importance, and potential implications," Journal of Multidisciplinary Engineering Science and Technology (JMEST), ISSN 2458-9403, 4(10): pp. 8318-8322, October, 2017.

[4] J. Brown, I. Bagci, A. King, and U. Roedig, "Defend your home!: jamming unsolicited messages in the smart home," HotWiSec '13 Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy, pp. 1-6, 2013.

[5] J. Slacik, P. Mlynek, R. Fujdiak, and J. Misurec, "Equipment for power line communication based on single-carrier system for home automation system," Progress In Electromagnetics Research Symposium, pp. 1787-1792, 2017.

[6] C. Nayyar, B. Valarmathi, and K. Santhi, "Home security and energy efficient home automation system using arduino," Communication and Signal Processing (ICCSP), pp. 1217-1221, 2017.

[7] K. Yang, T. Beaubouef, and M. Chiu, "Lesson learnt from smart home automation systems," Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, 6(3): pp. 149-153, March, 2015.

[8] M. Gauger, D. Minder, P. Marr?n, A. Wacker, and A. Lachenmann, "Prototyping sensor-actuator networks for home automation," REALWSN '08 Workshop on Real-world Wireless Sensor Networks, pp. 56-60, 2008.

[9] F. Molers, S. Seitz, A. Hellmann, and C. Sorge, "Extrapolation and prediction of user behaviour from wireless home automation communication," WiSec '14 ACM Conference on Security and Privacy in Wireless & Mobile Networks, pp. 195-200, 2014.

[10] B. Alhafidh and W. Allen, "Comparison and performance analysis of machine learning algorithms for the prediction of human actions in a smart home environment," ICCDA '17 International Conference on Compute and Data Analysis, pp. 54-59, 2017.

[11] S. Quadri and P. Sathish, "IoT based home automation and surveillance system," Intelligent Computing and Control Systems (ICICCS), pp. 861-866, 2017.

[12] H. Alavi, D. Lalanne, J. Nembrini, E. Churchill, D. Kirk, and W. Moncur, "Future of human-building interaction," CHI EA '16 Conference Extended Abstracts on Human Factors in Computing Systems, pp. 3408-3414, 2016.

[13] A. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: challenges and opportunities," CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2115-2124, 2011.