WWJMRD 2017; 3(12): 143-146
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Gamidelli Yedukondalu
Department of Computer Science and Engineering
Asst Professor at Samskruti College of Engineering and Technology, India

Correspondence:
Gamidelli Yedukondalu
Department of Computer Science and Engineering
Asst Professor at Samskruti College of Engineering and Technology, India

A Proposed Model for Smart Secure Home through Iot

Gamidelli Yedukondalu

Abstract
Smart home design has undergone a metamorphosis in recent years. The field has evolved from designing theoretical smart home frameworks and performing scripted tasks in laboratories. Instead, we now find robust smart home technologies that are commonly used by large segments of the population in a variety of settings. Recent smart home applications are focused on activity recognition, health monitoring and automation. In this system, we take a look at another important role for smart homes: security. We first explore the numerous ways smart homes can provide protection for their residents. Next, we provide a comparative analysis of the alternative tools and research that has been developed for this purpose. We investigate not only existing commercial products that have been introduced but also discuss the numerous research that has been focused on detecting and identifying potential threats. Finally, we close with open challenges and ideas for future research that will keep individuals secure and healthy while in their own homes.

Keywords: Detour Evacuation System, Wireless Sensor Network, Internet of Things, Fire Detection, Integrated Control System

Introduction
In many ways, smart homes embody this vision because sensors embedded into everyday environments unobtrusively collect data that monitor the state of the physical environment and its residents while everyday routines are performed. The computational component then reasons about the collected information in order to take an action that optimizes goals such as comfort, safety, or productivity.
While smart homes initially consisted of theoretical designs and smart laboratory experiments, they are rapidly maturing. The results of this evolution include number of actual prototype smart homes, associated public sensor datasets, and commercial products. Smart homes are used for a diverse range of applications including activity recognition, health assessment and assistance, environment quality monitoring, resource efficiency, and home automation.
In smart home system, we take an in-depth look at smart home technologies that can be used for home and resident security. Individuals spend a majority of their time in their home or workplace, and for many, these places are our sanctuaries. As such, smart home technologies need to contribute to maintaining the safety of residents by preventing as many threats as possible, accurately detecting threats that do occur, and responding quickly and effectively to them.
As Figure 1 shows, a smart home collects data from sensors embedded in the environment. Based on the sensed information, the home reasons about the potential threat and takes an action based on the nature and level of threat that is posed. These three steps – sense, assess, and act - serve as the basis for our coverage of current
Research and technologies in secure smart homes. We initially describe different types of security issues that smart homes may face and illustrate ways in which the home technology can assist. Second, we then describe current stand-alone sensor systems that detect specific types of threats and summarize current approaches that are taken to responding to threats. Third, we focus on the area that has received the greatest amount of research attention,

namely assessing and identifying threats based on sensor data. Finally, we close with a discussion of ongoing challenges for secure smart homes and ideas for future research directions.

Here we motivate the survey of secure smart home technologies through a series of scenarios that illustrate the types of threats that can be encountered in smart homes. Each scenario highlights a different type of security challenge and the role that smart homes can play in assisting with sensing, assessing, and acting on the threat.

Scenario 1: Intruder detection

Mary lives with her family who are all away for the day. During the morning, the home detects a person's arrival. The house recognizes that the time of day and the type of car fit those of a delivery person. The home provides access to the garage to drop off the items and notifies Mary. When Mary's husband Bob returns home in the afternoon, the home registers his presence and lets Mary know. Late in the evening, the home senses an unusual entry through the window. The camera is turned on to further identify the individual

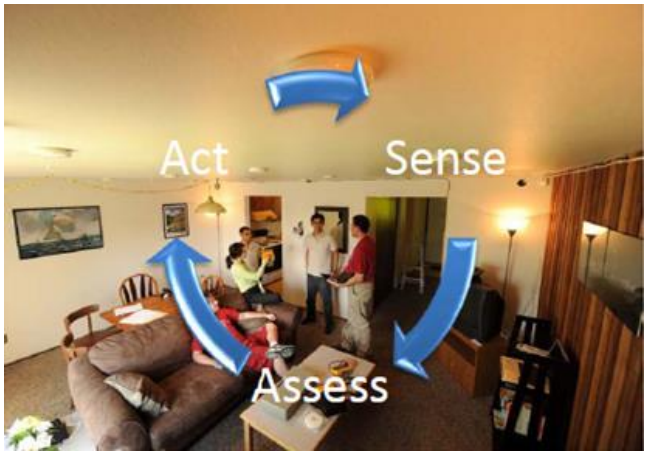

Fig. 1: A secure smart home senses threats, assesses them and tales action to keep the home and residents safe.

And to stream the video to Mary and Bob. They confirm that the individual is their son, who did not have his key and was entering through a window.

Scenario 2: Health event detection

Phil is an 81-year-old man who was diagnosed with Parkinson's disease five years ago. His mobility has been declining and when getting out of bed one evening he stumbles and falls. Phil is unable to get up to call for help but the home detects the sleep interruption and the subsequent lack of movement. The home asks Phil to confirm he is okay, and when it receives no response, the home contacts emergency services.

Scenario 3: Building system failure detection

Security of smart homes extends beyond individual homes to communities of residents. One complex included fifty apartments, each of which is a smart residence and which share some basic information between them such as indoor air quality, temperature, and electricity usage. When the apartments noted that the levels of volatile organic compounds (VOCs) in five of the residences suddenly raised beyond safe levels the compound notified the residents in all of the apartments to leave their homes and not return until the situation had been addressed. One of the apartments noted that its resident had been smoking in an apartment which was being remodelled and suggested that the combination of smoke and open toxic chemicals may have contributed to the problem.

These scenarios highlight the diverse nature of security issues that are faced by residents and thus by smart homes as well. A common theme of home security is detection and prevention of intruders, as shown in Scenario 1. However, smart homes that provide security should also be sensitive to health issues that can jeopardize the well-being of residents, as described in Scenario 2. This includes detection of falls, lack of movement, and significant changes in behavioural patterns. In the same way that the health of a smart home resident can be monitored by a secure smart home system, so the health of the physical home environment can and should be monitored. For example, as described in Scenario 3, the building can be subject to gas leaks, freezing pipes, fires, and,

Fig.2: Technologies found in a secure smart home

Other issues that can threaten the health of residents as well as the building. Many of the sensor, assessment, and action strategies can be used across these scenarios as we will see throughout the paper.

While the scenarios illustrate traditional security threats that can be addressed by a smart home, the smart home technology itself can introduce new threats. This motivates the need for smart home systems to be robust and resilient. In particular, if there is a sensor or system failure, the home must still provide protection and needed assistance. Therefore, the smart home itself needs to detect system anomalies and failures in its hardware, software, or communication components. Smart home technologies and the more general Internet of Things technologies also introduce a whole new type of intrusion, namely hacking into the technology infrastructure. Currently smart homes are fairly vulnerable to hacking and this can lead not only to costly pranks (e.g., run the washing machine multiple times) but also life-threatening manipulations (e.g., instead of turning the oven up to 150 degrees, turn the sauna up to 150 degrees). As shown in Figure 1, the first step of a secure smart home is to sense the current state of the environment and the residents. Smart home sensors are very diverse and often include a subset of sensors for motion, temperature, lighting, humidity, door use, appliance use, and power consumption, as well as cameras and microphones. With the advent of the Internet of Things (IoT), there is a wealth of devices that provide insights and

use the Internet to communicate with each other as well as the resident. In this section, we examine a sampling of technologies that provide sensing capabilities specifically for the purpose of providing a secure environment.

Video cameras are a traditional mechanism for monitoring an environment. They are found in many public venues and provide records of events as well as remote or even automated sensing of threats. Recently, companies including iControl, Nest, Smart Things, Viian, and Ring have enhanced the traditional camera system for the purpose of smart home safety monitoring. Vivint and Nest cameras can send alerts to homeowners when they detect activity, at which point the resident takes over the task of interpreting the data and acting on it. Ring is unique because it provides a smart doorbell system by connecting the doorbell to the camera. iControl is even more integrative, because the camera is combined with motion detection, sound detection, and an intruder siren. Alternatively, Smart Things not only facilitates camera-based monitoring and resident alerts, but other devices can be connected as well such as door locks to help residents take remote action in response to possible threats.

A second source of ambient sensing in the home for security is audio. Zhuang et al. use Gaussian mixture models to analyze data from a single microphone to specifically detect human falls. Moncrieff et al.scale up the role of the audio signal by quantifying a measure of home "anxiety" based on unusual loud noises that are detected by microphones throughout the home. The microphone is accompanied by a wearable accelerometer to detect whether the resident has experienced a fall.

Commercially-available home security sensing technologies often rely on the resident to interpret data and suggest actions. This process can be made more automated through the use of biometrics. Biometrics will automatically recognize individuals based on unique anatomical traits including voice, gait, retina, and face, as well as body shape (anthropometry), footstep shape, body weight, and heart beat pattern. While biometrics are used frequently for large buildings and operations, they are not as frequently incorporated into individual homes due to the amount of machine learning-based model training that is involved as well as privacy issues. In the context of individual homes, researchers often instead require that residents carry devices to identify themselves. Another approach to recognizing individuals in the home is to recognize behavioural patterns, or behaviometrics, rather than just physical properties, or biometrics. Behaviometric-based approaches will be discussed in more detail in Section 4.

An advantage of using the sensor packages described in this section is that they provide a rich source of fine-grained information

ined from video, audio, and specific biometric devices and can ultimately produce a more accurate interpretation of potential threats. This level of information does come at a price, however. Most of the sensors operate with a well-defined field of view, which is the total physical area that is observable by a sensor. Therefore, they need to be placed at locations that would be most likely to encounter the home threats. Employing a large number of such devices would be costly in terms of the initial purchase, the maintenance, the processing of a large amount of data, and the power consumption. On the other hand, utilizing too few devices or placing them in nonoptimal locations will negate their security benefit.

Another challenge posed by these security devices is the potential loss of privacy. Even if the captured information is only stored locally, many individuals feel that the uninterrupted monitoring by the devices is an invasion of their privacy. In fact, many residents turn off these devices when they enter the home, relying on the fact that most crimes happen when the home is empty. However, another frequent time for crimes is when the residents are sleeping, and turning off devices in these situations leaves residents vulnerable to threats.

Acting in Response to Threats

A smart home is typically infused with sensors to monitor the environment. As we described in the last section, these sensors can provide a fairly comprehensive analysis and identification of potential threats. Assuming that the collected information is processed and analyzed for the likelihood and type of threat (discussed in the next section), a smart home will ideally take appropriate steps to act on the threat.

Research and technology development in the area of smart homes has evolved to the point where homes can take autonomous actions in response to detected security or health risks (see Figure 2). As described in Section 2, existing commercial systems automatically provide residents with real-time information when an alert is generated, including notifying them of visitors and providing streaming video identification.

The variety of steps that a smart home can and should take is not limited to alerting and informing the resident, however. In their work, Chitnis et al.surveyed urban, suburban, and rural dwellers from a diversity of backgrounds including homeowners with children who are left unsupervised and individuals with traditional lock-and-key systems. As a result of the survey they proposed an infrastructure that

Granted different types of home access based on biometric matches. As described in Scenario 1 of Section 1, some individuals may only have access to the garage or front porch while repair technicians would also be granted access to areas of the house that need their attention. If an individual manages to enter unauthorized areas of the house, the homeowner is notified.

Homeowners may choose to let ambient sensors run continuously and use the more intensive data-gathering devices such as cameras only when they are out of the home. In such cases, Petersen et al. propose a method to automatically detect these situations and turn on video cameras. In this work, motion and door sensors continuously collect data and a machine learning system is trained to map these sensor readings onto a label indicating whether the residents are at home or away from the home. This approach extracts features including the number of sensor firings during each five- minute interval, an indicator of whether or not the resident is in bed, whether the door sensor was the last reading in the interval, whether the door sensor was the first firing in the interval, and whether the last sensor in the interval emanated from a room connected to an external door. A logistic regressor yielded a sensitivity of 0.939 and a specificity of 0.975 on sample data collected from actual smart homes, which are strong preliminary results supporting this approach.

While intrusion detection is a common application for security systems, much of the technology can also be applied to health monitoring and assistance as well. In the case of work by Dodge et al. by Hodges et al. by Dawadi et al.and by Lotfi et al.unexpected behavioural patterns are viewed as a health risk for individuals who are at risk of cognitive decline. These researchers have found that an increase in the number of activity anomalies and variation in behaviour patterns such as activity times and walking speed are correlated with changes in cognitive health. As in the case with the intrusion detection research, these findings provide insights that can be used by smart homes in order to keep residents safe. For example, residents and their caregivers can use this information to change the level of care that the individual needs.

In research by Ali et al. and of Das et al.threats are detected in the form of abnormalities in how residents perform their daily activities. For many individuals, these variations would not be considered a risk. However, for individuals with memory limitations, performing daily activities independently is critical. Functional impairment has been associated with increased health care use and placement in long-term care facilities days in the hospital falls conversion to dementia and morbidity and mortality. When an abnormality is detected, the individual can be prompted for the next activity step to help them keep on track and successfully complete the activity without caregiver intervention. This in turn increases functional independence and reduces the burden for caregivers.

And Assessing Threats

In this section, we close the loop shown in Figure 1. Both research and commercial efforts have made contributions in the areas of eveloping sensors for secure homes and acting autonomously or in partnership with residents to response to threats. The largest body of research, however, has focused on the middle step, analyzing collected sensor data to detect and assess potential security threats.

We organize our discussion of threat assessment in order of scale. We start with describing approaches to detect specific security-related situations, move toward summarizing approaches that perform general detection of threat-based anomalies, and finish with a discussion of security-based research in other fields that can impact future work on secure smart homes.

Conclusions

A proposed model for smart secure home through IoT is a distributed smart security system,which consists of server and sensors. In this system, the server controls and monitors the various sensors, and can be configured to handle more hardware interface module (sensors). This system not only monitors the sensor data, like temperature, gas motion sensors, but also top to bottom of the screen, which provide a view of the typical location-based circadian activity rhythm and deviations from normal rhythms.

References

1. M. Weiser, “The computer for the Twenty-First Century,” Sci. Am., vol. 165, pp. 94–104, 1991.
2. C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, “Smart homes and their users: A systematic analysis and key challenges,” Pers. Ubiquitous Comput., vol. 19, no. 2, pp. 463–476, 2015.
3. M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, “A review of smart homes - past, present, and future,” IEEE Trans. Syst. Man, Cybern. Part C, vol. 42, no. 6, pp. 1190–1203, 2012.
4. T. Jones, “Artificial intelligence coming to a home near you,” Digital Construction, 2012. [Online]. Available: http://www.constructiondigital.com/innovations/artificial-intelligence-coming-to-a-home-near-you.
5. T. Cohen, “I’m afraid I can’t let you do that, Dave’: Scientists predict ‘smart’ homes controlled by computer will be a reality in 10 years,” Mail Online, 2012. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2122343/Scientists-predict-smart-homes-controlled-reality-10-years.html. Available: http://www.dailymail.co.uk/sciencetech/article-2122343/Scientists-predict-smart-homes-controlled-reality-10-years.html.
6. G. Abowd and E. D. Mynatt, “Designing for the human experience in smart environments,” in Smart Environments: Technologies, Protocols and Applications, 2005, pp. 153–174.
7. H. Hagras, F. Doctor, A. Lopez, and V. Callaghan, “An incremental adaptive lifelong learning approach for type-2 fuzzy embedded agents in ambient intelligent environments,” IEEE Trans. Fuzzy Syst., vol. 15, no. 1, pp. 41–55, 2007.