Smart Computing Review

Smart Home Automation Security: A Literature Review

Arun Cyril Jose[1] and Reza Malekian[2]

[1]PhD Student, Department of Electrical, Electronic and Computer Engineering, University of Pretoria / Private bag X20, Pretoria, South Africa / poonjarian@outlook.com

[2]Senior Lecturer, Department of Electrical, Electronic and Computer Engineering, University of Pretoria / Private bag X20, Pretoria, South Africa / reza.malekian@up.ac.za

*Corresponding Author: Reza Malekian

Received June 4, 2015; Revised June 29, 2015; Accepted July 24, 2015; Published August 31, 2015

***Abstract*:** This paper presents a comprehensive description about different home automation systems and technologies from a security standpoint. The work highlights various security flaws in existing home automation systems. In our work, we address how the concept of security and the meaning of the word "intruder" have evolved over time. We examine the challenges in home automation security from the point of view of both the homeowner and security engineer. The work goes on to explain why home automation systems are such attractive targets for an attacker. We point out the role of user interfaces in security. Various home automation technologies considered in our work include context-aware home automation systems, central controller-based home automation systems, Bluetooth-based home automation systems, Global System for Mobile communication or mobile-based home automation systems, Short Messaging Service-based home automation systems, General Packet Radio Service-based home automation systems, Dual Tone Multi Frequency-based home automation systems, and Internet-based home automation systems. The work concludes by explaining future directions home automation Security Research could take.

Keywords: Smart Home, Access Control, Data Security, Intrusion Detection, User Interfaces

Introduction

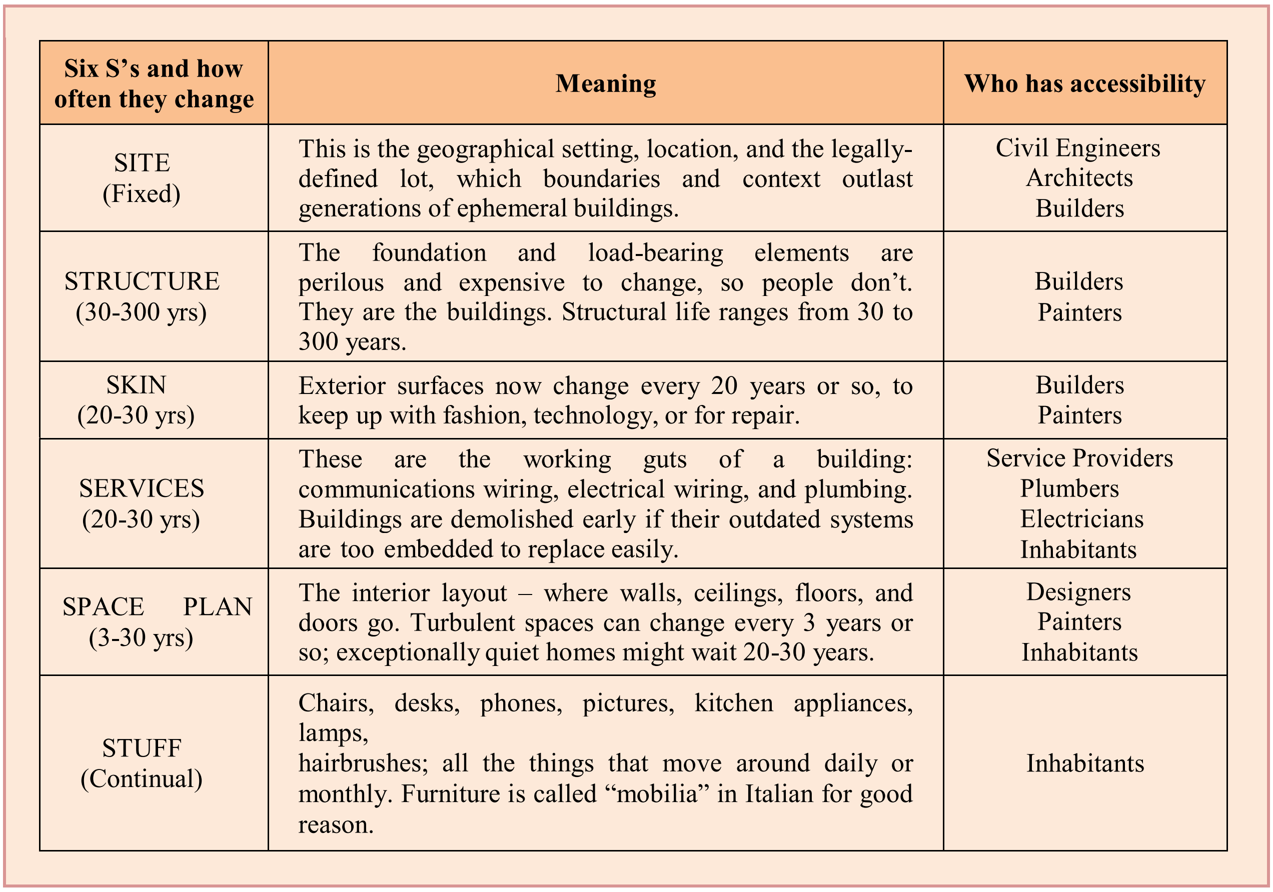
The concept of home automation has been around since the late 1970s. But with the advancement of technology and services, people's expectations of what a home should do or how the services should be provided and accessed at home has changed a lot during the course of time, and so has the idea of home automation systems. If we look

DOI: 10.6029/smartcr.2015.04.004

at different home automation systems over time, they have always tried to provide efficient, convenient, and safe ways for home inhabitants to access their homes. Irrespective of the change in user expectations, advancement of technology, or change of time, the role of a home automation system has remained the same.

From an engineering point of view, a home can be broken down into the “Six S’s” as specified by Brand [1] and given in Figure 1 below, along with who has access to each “S”. Home automation systems mainly deal with the last “S’s,” namely Service, Space Plan, and Stuff. A study [2] showed that in addition to home automation technology and devices, a modern home relies on three to seven services or companies to provide them with infrastructure support like Internet, telephone, electricity, gas, etc. Another study [3] done on different homes showed that people choose the “Site” of the home based on factors like the availability of uninterrupted power, high speed Internet, etc., excluding other factors like property prices and neighbors, which are beyond the scope of this work. The study also showed that a typical home environment handles a plethora of “Services,” so many of these services will have to share the resources of the home. The availability of wireless communication nowadays has helped with the “Space Plan” and improved the aesthetics of the modern home. Moreover, home inhabitants add, remove, and move equipment in their home as they please, so “Stuff” always changes in a home.

The work of John J. Greichen [4] discussed some of the early challenges faced by home automation systems. These include high manufacturing costs, high development costs, high installation costs, additional service and support costs, lack of home automation standards, consumer unfamiliarity with technology, and complex user interfaces. With the advancement of time, we saw a rapid development in technology and processing power which leads to a considerable reduction in device cost and size. All of these factors have contributed to the popularity of electronic devices today, so people are no longer confused or unsure about the use of computer, mobiles, or tablets. Moreover, a lot of home automation protocols, communication and interface standards like X10 [5], ZigBee [6], LonTalk [7], and CEBus [8] were defined overtime. All these factors contributed to addressing the challenges and concerns of early home automation systems, which lead to the popularity and wide acceptance of automated homes. The study done by A.J. Brush *et al.* [9] discusses the main stumbling blocks in modern home automation systems: the high overall cost of the system, inflexibility due to integration of different devices into the home automation system, lack of reliable devices at home, complex user interfaces, and reliance on skilled consultants. All these factors lead to poor manageability and lack of convincing security.



Six S’s and how often they change	Meaning	Who has accessibility
SITE (Fixed)	This is the geographical setting, location, and the legally-defined lot, which boundaries and context outlast generations of ephemeral buildings.	Civil Engineers Architects Builders
STRUCTURE (30-300 yrs)	The foundation and load-bearing elements are perilous and expensive to change, so people don’t. They are the buildings. Structural life ranges from 30 to 300 years.	Builders Painters
SKIN (20-30 yrs)	Exterior surfaces now change every 20 years or so, to keep up with fashion, technology, or for repair.	Builders Painters
SERVICES (20-30 yrs)	These are the working guts of a building: communications wiring, electrical wiring, and plumbing. Buildings are demolished early if their outdated systems are too embedded to replace easily.	Service Providers Plumbers Electricians Inhabitants
SPACE PLAN (3-30 yrs)	The interior layout – where walls, ceilings, floors, and doors go. Turbulent spaces can change every 3 years or so; exceptionally quiet homes might wait 20-30 years.	Designers Painters Inhabitants
STUFF (Continual)	Chairs, desks, phones, pictures, kitchen appliances, lamps, hairbrushes; all the things that move around daily or monthly. Furniture is called “mobilia” in Italian for good reason.	Inhabitants

Figure 1*:* "Six S’s" as specified by Brand [1]

Smart homes of today consist of a plethora of devices like multiple cameras, microphones, different sensors, actuators, device controllers, and home databases, which can be remotely accessed for user convenience. These devices, along with the home database, have a variety of personal information regarding a home’s inhabitants, like healthcare information, financial information, videos, pictures, live video feeds from home, daily habits or routines, favorite music, movies, and sometimes even a personal dairy. In some rare cases, inhabitants may use implanted medical devices, which need to be remotely accessed by hospitals or medical professionals, which can be done through the home network. Different devices used, bring different security vulnerabilities to the smart home, so, if or when these modern homes are compromised, they present a greater threat to the privacy and physical wellbeing of the home's inhabitants than ever before. A lot of research has gone into automating the home [10] [11], making it accessible via the Internet [12] or mobile phones [13] [14], saving energy [15], technology assisted living for senior citizens [16], and security [17]. Existing research only addresses and proposes defenses against normal intrusion attempts at home, and doesn't consider the risk of intrusion from sophisticated or tech-savvy criminals.

Our work mainly focuses on the security aspect of home automation. We first discuss how the concept of security has changed in modern home automation systems, then focus on various challenges in the field from a security point of view. The paper goes on to discuss various home automation systems and their security issues based on methodology used: context-aware home automation, central controller- based home automation, Bluetooth- based home automation, mobile or GSM- based home automation, Internet- based home automation, and a decentralized approach to home automation. Finally, we discuss the role of user interfaces in security and conclude by discussing where the researchers should focus their work in the field of home automation security.

How the Concept of Security has Changed in the Modern Home

"*The tasks of a modern security system include identifying an intruder trying to gain access to the home, alerting the homeowner about the intrusion or intrusion attempt, preventing the intruder from gaining access to the home, and gathering or collecting evidence regarding the intrusion so that the perpetuators can be brought to justice.*" The advancement of technology has contributed to the changing concept of security in modern homes. It has changed from a simple lock and key security concept to implementing sophisticated security systems using cameras, microphones, contact sensors, proximity sensors, alarms, silent alarms, etc. By connecting modern homes to the Internet which is very popular today, users can access and control their homes remotely at any time and from anywhere in the world. An increase in processing power of newly-designed processors and the considerable reduction in power consumption, cost, and size of new electronics devices enables people to know and control every aspect of their home, like which door or window is open, which device or light is switched on, and which rooms are occupied. Inhabitants can keep an eye on their home using live video and audio feeds from different parts of their home. They can also be aware of different environmental factors inside and outside their home, like humidity, temperature, and light intensity. In a Wireless Sensor Actor Network, sensors gather information about the physical world or environment around them. Actors perform the appropriate actions on the environment as directed by the user or any other party. Improvements in Wireless Sensor Actor Networks are certainly a contributing factor in the popularity of smart homes. Combining Ubiquitous Computing, Wireless Sensor Actor Networks and the popularity of the Internet has allowed designers, engineers, and researchers to come up with efficient methods to allow home inhabitants to access and control each and every aspect of their home, including the environment.

Commonly used technologies and networks for home automation have many vulnerabilities, as discussed by C. Karlof and D. Wagner [18]. They consider various routing attacks on wireless sensor networks (WSNs). This includes Sinkhole attacks, Selective Forwarding attacks, Sybil attacks, and Cloned ID attacks. In 2006, Y.C Hu *et al.* [19] detected an important attack on wireless networks called a Wormhole attack in which the attacker records data packets in the network at one location, tunnels them to another location, and retransmits them to the network. This attack can be carried out even if all communications in the network are done with confidentiality and integrity using IP sec in 6LoWPAN.

Data packet integrity, device authenticity, key establishment, and encryption standards are specified in almost all wireless encryption protocols these days. In 2011, J. Wright *et al.* [20] showed how a ZigBee or 802.15.4 wireless networks can be hacked using replay attacks [21]. During reflashing, the new key is sent in plain text over the air. An attacker can take advantage of this and sniff for encryption keys in plain text, inject, decode, and alter data packets to manipulate a device's operations. In 2013, B. Fouladi and S. Ghanoun [22] demonstrated a vulnerability in Z-Wave door locks, which gave the attacker full access without proper authorization.

In 2013, T. Oluwafemi *et al.* [23] showed how a simple device in a home, such as a fluorescent lamp (CFL), which is connected to a home automation network or Internet could be manipulated to cause physical harm (shattered glass, fire outbreak, mercury poisoning) to a home's inhabitants. Moreover, lights fluctuating at certain frequencies could be very dangerous for people with photosensitive epilepsy [24]. When a home automation network is connected to the Internet, there is the possibility that an attacker could gain control of switches and dimmers along with devices plugged into the power outlets. Researchers also discussed the presence of some well-known vulnerabilities in home automation systems, such as Cross Site Scripting (XSS).

They were able to embed persistent Javascript in the log pages of one of the products. The researchers also observed that in some home automation systems, every communication between the homeowner and home automation system, both from within the home network and over the Internet, is done in clear text (over the Internet HTTP is used instead of HTTPS). This allows an attacker to eavesdrop on the communication and gather legitimate login credentials. In some home automation systems, a user is authenticated using an authentication cookie, which is not associated with any session ID or expiration time frame, so if an attacker could steal this authentication cookie from a legitimate user and include it in their browser session, they could bypass the authentication page altogether.

In an attempt to capture the home automation market companies and designers gave little importance to security. They took the stance that “we will worry about security when we have to,” and focused their manpower and resources on system flexibility, user convenience, and improved functionality. It is the approach that most software developers take, except for those security critical operations like defense and air traffic control, before deploying their systems, and try to fix security issues via patches and system upgrades. But for homes it is different. The home is a place where everybody is supposed to feel safe and secure. Even the slightest doubt that a home could be compromised can have a serious psychological impact on its inhabitants.

We have to give a broader explanation or meaning to the term “intruder” in our definition when we combine homes with the Internet and ubiquitous computing, also considering the number of devices used in home automation today and their vulnerabilities. In traditional homes, intruders could only steal or threaten a home if they are in physical proximity to the home. By connecting a home to the Internet, an intruder or attacker can access the home from anywhere in the world at any time with an Internet connection, and with cameras in the home they can keep an eye on a home’s inhabitants. So identifying and defending against such intrusions are extremely difficult, even without the added security flaws of the technologies implemented at home.

In short, when we talk about security at home we think about intruders in the traditional sense, like thieves trying to break in by picking the lock or prying opening a window, and rarely consider sophisticated thieves who are good with technology or criminals who work with hackers. Our concept of intruder has to evolve from the traditional sense in order to account for device vulnerabilities. A lot of research has gone into identifying and preventing such intruders by using alarms, infrared sensors, or contact sensors, but very little work has gone into identifying and preventing technologically-skilled intruders.

Challenges in Home Automation Security

In this section, we discuss why home automation systems are such an attractive target for an attacker, and the challenges faced by a home automation system from the point of view of the homeowner and security engineer.

■ Why Home Automation Systems are Such Attractive Targets for an Attacker

- Data, information, video or audio feeds available from home are almost always personal.
- Almost all smart homes are connected to the Internet 24/7. This allows an attacker to be anywhere in the world and can still be targeting the home. Moreover, an attacker can cherry pick the moment of attack.
- Home automation systems don’t have a dedicated system administrator, unlike a traditional network, which means that attackers can do their “footprinting” efficiently with comparatively less monitoring. When the network is compromised, there is also very little chance of detection.
- A homeowner who is also the system administrator may be reluctant to do the upgrades or patches necessary, like a homeowner’s reluctance to do the plumbing. In addition to this, home automation systems could look very complicated to an ordinary non tech-savvy homeowner.
- Home automation systems usually consist of devices belonging to different manufacturers. Each comes with its own vulnerabilities. Moreover, home inhabitants who are not experts on networking or security do the upgrade or reconfiguration of their own home networks, unlike researchers do in the labs, which brings in its own set of vulnerabilities.
- An attacker always has the choice to scan the Internet for a specific vulnerability belonging to a specific home automation device from a particular manufacturer. An attacker can keep up the scanning process until finding the specific vulnerability they are looking to exploit.

■ From a Homeowner’s Point of View

- In most cases, money is the bottom line or motivation for the common homeowner when choosing different home automation products. They are either unaware, misinformed, or doesn’t care enough about various security risks.
- Homes are used by people of all backgrounds; people with and without technical backgrounds, people of

different age groups both young and old. Moreover, a home is expected to have guests. Homeowners can't expect all of these people to be careful about security.

- Devices connected to home networks are portable like mobile phones, PDAs, etc. These devices stay with the user wherever they go and are connected to various networks. An attacker trying to compromise a home automation system could use these portable devices as a gateway to the home when they are connected back to the home. Users are more careless about their phones, more so than they are about their physical home.
- Most homeowners implement some sort of access control mechanisms to protect personal data from guests and others who have access to the home. Their access control parameters are often complicated and difficult to implement from an engineering perspective. Some of the access control parameters include who all are present while accessing the data, why and where the data is being accessed, and which devices are used to access the data.
- While implementing access control, the homeowner also has to consider the social implication of denying data access to a guest. A guest may feel insulted, so the owner may have to consider the guest's feelings. The owner may have to change access control polices quite often, which, if not properly established, proposes a big security threat. In order to avoid such complicated social situations T.H Kim et al. [25] came up with Clairvoyant Access Right Assignment (CARA), which reduces the burden of allocating each resource to individual guests on the homeowner. CARA grants access to home resources based on the owner's social standing with their guests. The social standing is obtained from social networking sites, Instant Messaging Services, owner call logs, and Short Messaging Service (SMS) logs. This is a dangerous precedent, as we know that social networking sites are vulnerable to hacking, and people can manipulate the owner or pretend to be a friend. Moreover, close friends on social networks could fall out with each other quickly, but CARA is not equipped to successfully handle the situation. Social standing obtained from the social networking sites and chat logs are not always accurate, either. People can chat a lot as part of their job or as part of an argument and still not be friends. Moreover, clever attackers can initiate and keep the owner talking or make him initiate communication. The same applies for phone conversations as well. People don't use SMS messages anymore, they use services like WhatsApp. Assumptions based on emoticons and abbreviated words could be wrong, as well. People have their own style of writing; some people use emoticons and abbreviated words more than others.
- The research done by M.L Mazurek et al. [26] showed that there is a big difference between a user's mental model (what user thinks is implemented) of access control and the access control and security measures that are actually implemented.

■ From a Security Engineer's Point of View

- Complexity of the home environment: Ubiquitous computing is an evolving field of study. It hasn't been around in a home environment for that long, so we never know how this is going to influence the delicate dynamics of the home. It is a nightmare from a security standpoint. We can do all the studies, projections, and approximations possible, but no one can predict how it will impact an inhabitant's life in a home.
- Unlike in companies and software firms, you can't enforce security procedures or policies that affect the convenience of inhabitants at home, or their guests. Even a few suggested security policies may not be followed by the home inhabitants.
- Homes consist of people of all ages who have different behaviors. Some of them, generally senior citizens with limited technical knowledge, are more vulnerable to social engineering.
- Unlike any other cybersecurity breaches, an attacker who compromises a home automation network can cause a wide range of damage, including physical harm to a home's inhabitants, emotional harm, permanent damage to electronic devices, loss of reputation, financial damages, environmental damages, granting unauthorized access to anyone, theft, blackmail, vandalism, or voyeurism, to name a few.
- The mixed ownership of devices at home and guests with varying technical knowledge and different intentions compounds security issues at home.

Various Home Automation Methodologies Analyzed from a Security Standpoint

In this section, we discuss various home automation methodologies and techniques from a security perspective. We discuss each technology, its features, and what security pitfalls they have.

■ Context-aware Home Automation Systems

A modern home can be accessed by its inhabitants from the outside through Internet, Global System for Mobile communication (GSM), and wireless portable devices like mobile phones, tablets, laptops, or through stationary devices like an office workstation (PC). In other words, an average automated home user's computing environment keeps on changing. By computing environment, we mean a user's type of network connectivity, type of network access at different places, cost of accessing the home over the Internet, processing power of the devices, and other hardware available to the user. We can't expect the user to be security conscious every time he or she accesses their home from the outside. This brings in new security vulnerabilities to the home front. Understanding the context of a particular action by the user could go a long way in improving a home's security. The work of A.K. Dey [27] defines context as "*Any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.*" In a context-aware home automation system, the system tries to be aware of the context in which a user makes a decision. Predicting the location of a user inside the home adds to defining the context. The work of B.N. Schilit *et al.* [28] discusses different techniques for identifying the location of a user at home. The work proposes the uses of an infrared grid to accurately predict the position of the user in the home, thus contributing to improved security. But this grid of infrared sensors is difficult to implement in a home environment. The work also discusses the use of badges to identify the location of inhabitants inside the home. This could significantly improve security, but it is inconvenient for the user. Moreover, inhabitants can be careless in their home and misplace these badges, which leads to confusion in the system. Another method mentioned in the work is Static Object Checking. It identifies an inhabitant's location by checking to see if someone is in the proximity of a static object. This method limits the flexibility of the environment, and if someone moves or changes the position of these static objects, it will be very confusing to the system.

The work of V. Bellotti and K. Edwards [29] explain in detail why contextual sensing is difficult. The human aspect or human behavior is very difficult to predict or reason for. People tend to be unpredictable or unreasonable at times. Unlike computers, they improvise, and tend to make impulsive decisions about their context. Context-aware computing raises a serious question of user privacy. With context-aware computing, the system has even more intimate information about the user. In order to implement context-aware computing, the system will have to share this information. This raises issues like who the information is shared with, how the shared information is used, and who all has access to the shared information. In short, the technology raises more privacy concerns than it solves. In his work, S.S. Intille [30] states that the home of the future will not control the environment, but instead will help its inhabitants to learn how to control the environment on their won. In other words, taking the power of decision-making away from home inhabitants, what context-aware computing does, will have a negative impact on their psyche. The author infers that technologies in a smart home should assist the home inhabitants to make energy-saving or security-conscious decisions by informing or reminding them when such an opportunity arises, rather than the system making context-aware decisions on its own.

In order for context-aware systems to be successful when implemented at home, several factors must be considered:

- The system must disclose to the user what it knows, how it knows it, and what it is going to do about it.
- The system must make a user aware when its context-based actions affect others.
- Context-aware computing considerably increases a system's complexity. Accurately interpreting the environment is hard enough without the added overhead of predicting the user's context, intention or reasoning for an action.
- Contextual computing increases a system's manufacturing, implementation, and maintenance costs, which make them unaffordable to the common man.
- In order for the system to be successful it requires constant user interference, which most users find annoying. Moreover, if the system malfunctions, only an expert or skilled person can fix the system.

The concept of context-aware systems look good on paper, but it is difficult to implement correctly and creates some privacy issues.

Central Controller-based Home Automation System

A central controller-based home security system looks to improve the security of the homes in a locality by combining many homes into a security network with a control node dedicated for each locality depending on the number of users. These control nodes are controlled by a few central or chief control nodes with considerably high processing power. The security system described by S. Tsai *et al.* [31], called Home Security System on Intelligent Network (HSSIN), uses such a central controller-based approach. The proposed system lacks modern security parameters.

A central controller based security system has its own unique challenges:

- All or most homes in the neighborhood have to join in for the approach to be cost effective and successful.
- The main question we have to consider here is who controls or has access to the central controller and its data? The central controller will be able to know about a home's intimate and private information from the data at its disposal, like if a home's room heater is on, or if an inhabitant in a home is taking a shower. This raises serious privacy concerns. We already know how people feel about government surveillance on the Internet. Central controller-based security systems provide an opportunity to do even more privacy-violating surveillance on homes.

The work of K. Atukorala *et al.* [32] proposes a home automation Security System called SmartEye using General Packet Radio Service (GPRS). SmartEye also uses a central controller, to which many individual home controllers are connected. The system proposes a real-time home automation and monitoring system. The system alerts the homeowner by mobile phone using GPRS, and the user can view the home using live camera feeds. The system uses a RabbitCore Module to connect an electrical appliance in the home to the home system, usually a PC. Each home system is connected to a central server. RabbitCore has an IP address, so each device connected to it can be identified and operated via mobile phones using GPRS. The user sends device management commands to a central server. The home system reads the command from the central server, called home polling, and makes the changes needed to a device. When a device changes state, the home system, usually a PC, sends the change of state of the device to the central server. The user's mobile will read the change from the central server, called mobile polling. The mobile user is provided with a home plan and places where each piece of equipment is kept in their home. The proposed research gives importance to communication and network setup rather than security. It mentions intrusion detection, but no concrete parameters identifying intrusions are mentioned.

SmartEye uses video cameras for security. Its security issues are discussed below. Moreover, like all centralized home security systems, the proposed system is also not ideal for securing single homes, but suits a group of homes best, and the author's claims of "increase in poll rate leads to increase in security" is debatable and misleading.

In reality, a central controller-based security system is difficult to implement and raises some very serious privacy concerns.

Bluetooth-based Home Automation System

The work of N. Sriskanthan *et al.* [33] shows the implementation of a home automation system using Bluetooth. They use a host controller implemented on a PC, which is connected to a microcontroller-based sensor and device controllers. The researchers even built a new protocol on top of the Bluetooth software stack, called Home Automation Protocol (HAP), to make the communication between devices possible. The device controller is connected to electronic devices through the I^{2}C Bus. The system allows more than one device controller to be connected to the host controller.

The work of H. Kanma *et al.* [34] also proposes a home automation system using Bluetooth that can be accessed remotely through GPRS. The researchers use a cellphone equipped with Bluetooth connectivity as a host controller and a GSM modem that provides Internet connectivity. Home devices are fitted with Bluetooth communication adapters so that they can communicate with the host controller phone via Bluetooth. The paper discusses remotely controlling and updating home devices along with fault diagnostics and detection. The work also talks about providing an electronics user manual on the phone using Bluetooth and Internet.

Issues of using Bluetooth for home automation:

- Bluetooth has a maximum communication range of 100m in ideal conditions. More may be needed in a home environment.
- Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced.
- Bluetooth technology has advanced and improved to Bluetooth Low Energy (BTLE), which provides the same range of communication. However, it has serious security concerns such as eavesdropping and weak encryption as discussed by M. Ryan [35].

- Bluetooth communication should only be used on occasions where there is a need for quick short-lived network communication with little concern for security.

Bluetooth looks like an attractive communication technology for creating smart homes. It is cheap, easy, and quick to set up. People are already familiar with the technology. The hardware required for establishing

Bluetooth communication is readily available. And the technology also provides the necessary bandwidth for the operation in a home. But they also have serious flaws, as discussed above.

■ GSM or Mobile-based Home Automation System

Mobile-based home automation is attractive to researchers because of the popularity of mobile phones and GSM technology. We mainly consider three options for communication in GSM, namely SMS-based home automation, GPRS-based home automation, and Dual Tone Multi Frequency (DTMF)-based home automation. Each of these three technologies is discussed below, along with their shortcomings.

Figure 2 printed below is from the work of A. Alheraish [14]. It shows the logical diagram of how a home's sensors, electrical, and mechanical devices interact with the home network and communicates through the GSM module using a Subscriber Identity Module (SIM). The system converts the machine functions into electrical signals through a transducer, which goes into a microcontroller. A transducer converts physical quantities like sound, temperature, and humidity into some other quantity like voltage; here, a sensor does that function. For electronic devices, their reading goes directly into the microcontroller. The microcontroller analyses these signals and converts them into commands that can be understood by the GSM module. Based on the received commands, the GSM module selects the appropriate communication method (SMS, GPRS or DTMF).

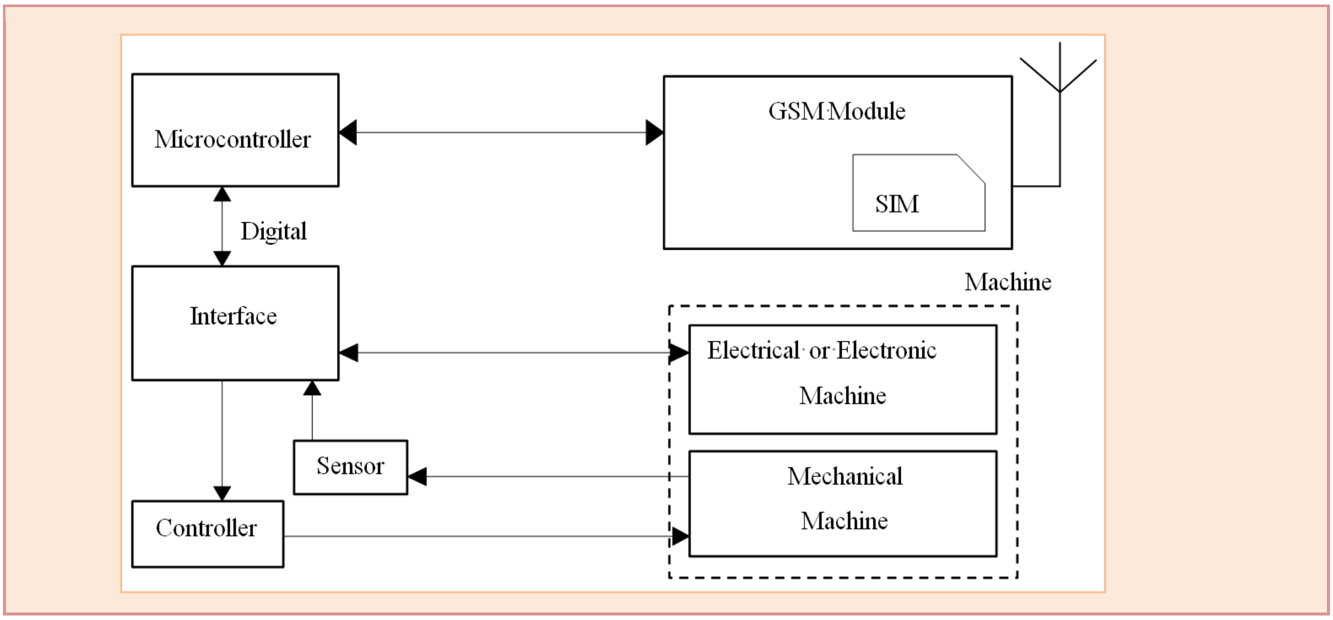


Figure 2. Mobile-based home automation from the work of *A. Alheraish* [14].

■ SMS-based Home Automation System

The work of A. Alheraish [14] proposes a home automation system using SMS. The proposed system detects illegal intrusions at home and allows legitimate users to change the passkey for the door and control lights in the home. The illegal intrusion into the home is identified by monitoring the state of the home door, which is done using Light Emitting Diode (LED) and infrared sensors. The passkey to the door can be any 4 digits, which can be set either by using the keypad or by using SMS from a registered user's mobile number. A user can control the lights in their home remotely using SMS from their registered mobile number; by turning the lights on in different rooms at random intervals of time, one can give the impression that the home is occupied, even when it is not.

The work of M.S.H Khiyal *et al.* [36] proposes an SMS-based home security system called SMS-based Wireless Home Appliance Control System (HACS). In their work, a homeowner can control their home using SMS messages from a preset registered mobile number. If the SMS is not from a legitimate mobile number, the system ignores the message. In the case of an intrusion, the appliance control subsystem and security subsystem in the proposed system informs the owner through SMS.

The work of U. Saeed *et al.* [17] also proposes an SMS-based home automation system. The system has a Java application running on the phone. Legitimate users can log in to the application using their username and password, and can select the building/floor/room/device that they wish to remotely control along with an appropriate action from the list of available user actions. The Java application will compose the appropriate SMS message and send it to the home's GSM modem. The GSM modem will receive the SMS message, decode it, and pass it to the home network to perform the action specified. The researchers use a 4-digit passkey and facial recognition for security.

In the work of A.R Delgado *et al.* [37], GPRS communication is used as a backup for an Internet-based home automation system. This adds to the fault tolerance of the system. The homeowner will be able to get alerts on their mobile phone about the unusual state changes in the sensors. The user could then react either by messaging or using a web interface. In any case, there will be two possible ways to access the home, so if one fails the user can rely on the other.

Security concerns about SMS-based home security systems:

- The 4 digit security passkey (used by A. Alheraish [14] and U. Saeed *et al.* [17]), in itself proposes a security vulnerability. An attacker could wait outside the home and peep through the window to learn the passkey. One can't expect the owner to be careful every time he or she enters the passkey. The user punches in the passkey routinely, so the probability of the user being careless is high.
- The passkey used in the work of U. Saeed *et al.* [17] is different for each individual at home, which improves the odds for hacking the keypad. Moreover, these passkeys are chosen by users who are vulnerable to social engineering and other hacks.
- Most of the proposed systems don't consider sophisticated attackers, or are no match for a sophisticated attacker. The systems don't consider any other entry points into the home apart from the front door. The LED and IR sensors used by A. Alheraish [14] to identify intrusions could easily be spoofed by a sophisticated attacker.
- Informing the homeowner about an intrusion at home through an SMS message is never a good practice. Users may not frequently check their phones for SMS messages, or may not be near enough to the phone to hear a message received tone, so they could easily miss the intrusion alert.
- Simple facial recognition systems could be hacked using a photograph of an authorized person, as the system can't distinguish between a picture and a real human.
- In today's world, attackers are very sophisticated. One should always consider the possibility of an attacker cloning the SIM card of a legitimate device with which the attacker can do all the tasks a legitimate homeowner does. Moreover, one can never rule out the possibility of the homeowner misplacing his or her registered cell phone or the attacker stealing it. If that happens, then breaking into a home can be as easy as stealing a cell phone.
- The researchers A.R Delgado *et al.* [37] point out the increase in security of the home because of remote access. The user can be made aware of an intrusion as soon as it happens, so that he can view the home through various cameras installed at different parts of the home. The paper completely ignores the plethora of security vulnerabilities that exist in the devices used to connect and automate a home. Moreover, the chance of an attacker exploiting these vulnerabilities is increased significantly when the home is connected to the Internet. In addition, the cameras used in this work have security issues, which are discussed below.

■ GPRS-based Home Automation System

There are a lot of home security systems implemented using GPRS. Most systems use the word security in the traditional sense, and only address the threat put forth by old fashioned intruders in home.

Researchers M. Danaher and D. Nguyen [13] propose a home security system using GPRS. The work uses a webcam to stream video and pictures of the home to its owner's mobile through GPRS. The webcam detects movement by comparing frames for differences, including light intensity. Video streaming in the proposed work is done using the home Internet connection, not the GSM modem.

The work of B. Wu *et al.* [38] describes video camera surveillance using the GPRS facility in mobile phones. The camera is triggered when an intrusion is detected or the door bell is rung. The system identifies intrusions with an infrared sensor. In the case of a doorbell, the system calls the homeowner and establishes voice communication with a live video feed between the visitor and the homeowner. When an intrusion is detected, an email is sent to the user along with a picture, most likely of the intruder. Upon receiving this email the user can start monitoring the video feed on his phone.

The work of L. Yang *et al.* [39] allows a user to read and change the status of the devices at home using a preregistered mobile number using GPRS. The proposed system doesn't allow external devices to connect directly to the home devices. When a legitimate device with the correct phone number tries to connect to the home environment, a connection is established between the virtual home which mirrors the current state of the home devices and user, acting like a honeypot. The commands issued by the user are analyzed, and if they don't pose any harm to the home devices then the command is applied to the real devices at the home. When an emergency situation arises, like an intrusion or a fire, the intelligent devices at home initiate a communication between the home and the user via telephone, text message, or email that is called "phone-out-only." The reverse never happens – a user never initiates direct communication with the home devices.

U. Ali *et al.* [40] proposes another home and office automation system using GPRS in mobile phones. The user interacts with the home via a client/server architecture implemented at home using a PC and a micro Java application. Home devices are controlled by a device controller, which is connected to the PC's parallel port. The proposed system allows users to remotely control and inquire the status of the devices that are connected to the device controller.

The researchers J. Jin *et al.* [41] discuss a home automation system based on WSNs and GPRS. It allows it users to control equipment in their home, and collect data about a device's status and weather conditions at home through their mobile devices. The authors' custom-made the application for China, as users receive information about home intrusions and fire through the Chinese Instant Message Mobile Service. Unlike other GPRS-based home automation, the proposed system uses an embedded system-based central controller.

Researchers S.R. Das *et al.* [42] developed an iOS-based home automation security system using GPRS. The proposed system uses the client/server model for communication. The authors develop an iOS application that runs on a user's mobile phone and acts as the client, and the cloud to which the home devices are connected acts as the server. The authors use video cameras, microphones, and motion sensors for providing security at home. When a motion sensor is triggered, the video cameras in the vicinity start to record. A user can view these live feeds on a mobile device through GPRS. The proposed system can also be accessed using a web browser.

Security concerns in GPRS-based home security systems:

- The works of M. Danaher and D. Nguyen [13], B. Wu *et al.* [38], L. Yang *et al.* [39], and S.R. Das *et al.* [42] all implement cameras at home. Streaming live video feeds over the Internet is never a good idea, especially when it is from inside the home. If these implemented cameras are compromised, then the attacker will have an eye inside the home. A recent BBC report by L. Kelion [43] highlights the vulnerabilities in wireless cameras. Moreover, people do not like to be watched; it affects their normal behavior and makes them uncomfortable.
- Video feeds could be looped by skilled attackers if the cameras and the system are not installed and maintained properly.
- In a GPRS-based intrusion detection system, the user will have to monitor his or her phone constantly to successfully defend against intrusion.
- The infrared sensor-based intrusion detection system specified by B. Wu *et al.* [38] can be spoofed by a skilled intruder, so its ability to identify intruders can be questioned.
- The work of L. Yang *et al.* [39] uses terms like "safe" and "do not harm," which have a broad meaning that the paper does not clearly specify. Moreover, in their proposed system, a legitimate mobile number could be spoofed by skilled attackers, so such attackers could manipulate home devices or at least know the status of the home devices. From the status of different home devices, one can infer whether a home is occupied, and which rooms are occupied.
- Alerting a user about an intrusion attempt by email is never a good practice. Users may not check their phones for email messages frequently, or may not be near enough to the phone to hear a message received tone, so they could easily miss the intrusion alert.
- Researchers S.R. Das *et al.* [42] provide users access to the home using a web browser, which opens the home to a different set of browsing-related security issues like session hijacking, cookie stealing, and cross-site scripting.
- The work of M. Danaher and D. Nguyen [13] provides limited security, as they only use cameras and no other security mechanisms.
- Almost all the GPRS-based home security systems use one or more video cameras, motion sensors, or infrared sensors to identify intruders in a home environment. They rarely use any complicated techniques or algorithms to identify a more technically-skilled attacker.

■ DTMF-based Home Automation System

The work of L. Muhury and A.H.M.A Habib [44] describes the design and implementation of a DTMF-based home automation system. The user calls a SIM number assigned to the home and presses the digits on their phone's keypad to control the home's devices by generating a DTMF tone. The tone is received and decoded by the GSM module at home using a DTMF decoder. The decoded instructions are passed to the microcontroller so that user commands can be implemented at home.

Home automation systems using DTMF are not very commonly implemented, maybe because there are other better options for communication available. Like all other systems, DTMF-based home security systems also have their security flaws. They are vulnerable to "fuzzing attacks," as described by R. Sasi [45]. In a fuzzing attack, a user exploits a vulnerability in DTMF processing algorithms by giving unusual input data, which results in triggering an exception. This could cause the entire home network to crash.

■ Internet-based Home Automation System

Internet or IP protocol-based communication in home automation systems is always a popular choice among researchers. The Internet is easily scalable, flexible when it comes to access and use, and very popular as a communication method in today's world, so the hardware and the network required for access is readily available, offers high bandwidth and very low communication cost, and devices can connect to and disconnect from the network easily. These are some of the features that make the Internet such an attractive choice for researchers. Utilizing the Internet as a means to access and control the home seems to be the next logical step forward for home automation systems.

From an end user's point of view, using Internet to access their home is easy, convenient, cheap, flexible, and offers no complication of an added technology to learn. User interface devices like laptops, smartphones, PCs, and tablets are easily available in the market, and these devices are already a part of people's daily lives. So, incorporating home automation into these already-popular user devices seems to be the natural progression.

Figure 3 printed below shows the components of a typical home automation system using the Internet.

The User Interface (UI): UIs are usually web pages or any Android/iOS/Windows applications developed by the researcher. A user can use these applications or a web browser to access their home from their portable devices using the Internet. Most home automation systems use a username and password as the way of identifying legitimate users before granting access to the home.

In most Internet-based home automation systems a username and password seems to be the only authentication method used.

This raises some security concerns:

- People are generally careless in nature. They tend to write complicated passwords and usernames on paper near their workstations or underneath their keyboards, thinking "who bothers to look there?"
- People often repeat the same passwords and usernames on different websites and forums. This behavior makes them vulnerable to phishing attacks.
- During the course of time, a homeowner will have to log in to the home from different networks like from the office, from their friend's house, from public Wi-Fi networks such as coffee shops, even parks, sometimes using untrusted devices. The network chosen by the user to access the home may be vulnerable. This could result in the user being exposed to variety of attacks like man-in-the-middle attacks. Moreover, when accessing the home from a compromised device, legitimate user credentials could be stolen by the use of simple software tools such as a keylogger.
- Researchers should also be aware of the human factor when depending only on passwords for security. The human factor means normal people tend to choose passwords that have some sort of significance to them like their pet's names, name of their favorite movie, music artist, sports team, etc. Moreover, we should never underestimate the most powerful hack of all, social engineering, which could prove to be very effective when trying to obtain a person's password and username.
- Accessing a home through a web browser opens the home up to a variety of browser-related security issues mentioned earlier. Researchers have to assume that when accessing their home over the Internet, people will choose convenience over security if given the choice.

Web Server, Database and the Microcontroller: The user interface is connected to the database via a web server. The database consists of details of all the home devices and their current status. A user remotely accessing their home can query the device's status information from the database via the web server. A microcontroller manages all the operations and communications in the home network, as shown in Figure 3. In reality, a PC can do all these tasks, so researchers replace these three components (web server, database, and microcontroller) with a PC for convenience.

Network Interface Module: It manages the communication between the PC and the home device controllers. When a user issues commands to change the status of the devices at his home, these commands are transmitted through this interface to the device controllers. Upon completion of these commands, the status of a device is relayed to the database through the interface.

Device Controller: A Device Controller consists of an interface module, a wireless communication module, and a microcontroller to control its operations. A Device Controller is connected to multiple home devices and sensors. User commands and status enquiries to a home device are relayed through the device controller.

Communication Module: There are a few choices in technology when selecting the mode of communication between the devices within the home. Depending on the inhabitant's preference, wired or wireless connections can be used. For wired communication, X10 is the most commonly-used communication protocol, as it can be implemented using existing wiring without a lot of drastic changes. For wireless communication, the choices include infrared, Bluetooth, Wi-Fi, and Radio Frequency (RF). Each of these communication technologies has their own pros and cons. We discussed Bluetooth-based home automation in the previous section. We also discuss a few works based on infrared, Wi-Fi and RF communication below.

The work of A.Z. Alkar and U. Buhur [46] implements a home automation system using Internet for enabling remote home access and infrared technology for device communication within the home. The researchers use a PC to perform the task of a web server, database, and interface. They use an RS232 module as a communication interface. The user interface is also developed by researchers and made accessible through the Internet. The work proposes the use of SSL certificates to ensure the authenticity of the web server.

The SSL certificate proposed by the authors is relatively secure, but there are still issues like SSL certificate stealing, certificate authority hacking, and fake certificate authorities. User authenticity is ensured using a username and a password, which is an area of security concern, as discussed before.

Wi-Fi communication technology has a lot of advantages: low installation cost, easy to deploy and install, decent communication range, scalable technology, high bandwidth, and low power consumption. AES encryption offers good security. Moreover, repeaters can be used to extend communication range. Wi -Fi is an ideal choice of communication for automating an already-existing home without altering the existing architecture. Besides, the communication is wireless so it improves the aesthetics of the home. All these factors make Wi-Fi an ideal choice for wireless communication among researchers. The work of A. ElShafee and K.A. Hamed [12] proposes an Internet-based home automation system. Their work uses Wi-Fi to enable communication between different devices and the server at home. A user can login using a username and password and control the devices at home. In their work, the researchers use a PC as a web server. The PC also has built-in Wi-Fi communication capabilities and a communication module that enables communication between the home devices and the server (PC). The home devices are connected to the server via Wi-Fi by a hardware interface module. Security is improved in the proposed system by blocking access to a login page for some time after successive failed login attempts. This protects the system from brute-force attacks and dictionary-based attacks. The system is still vulnerable to browser vulnerabilities and social engineering.

The work of J. Shah *et al.* [47] proposes a home automation system using RF and SMS. The RF module discussed here is used for communication between the homeowner and the devices. The homeowner uses an RF remote to control their home devices. The RF remote used has a range of 20 to 30 m. When a device changes state, an SMS is sent to the homeowner alerting him about the change in state.

The proposed system doesn't allow homeowners to access their home remotely from their mobile device. They can only control home devices through the RF remote. RF remote used here has very limited range to be successful in a home environment. Furthermore, the proposed system only allows 15 devices to be connected to the home network.

Home Router: A home automation system is connected to the Internet using a home's router. This allows the home's inhabitants to access their home from anywhere with the right credentials. Some issues with the home router are:

- When choosing a wireless router for the home, an average homeowner considers factors like the speed of the connection, range offered for communication, and cost. Usually, security is not the main concern. Moreover, most homeowners lack the technical expertise to configure their routers properly.
- A research firm named Security Evaluators (ISE) of Baltimore [48] did a security study on 13 off-the- shelf small office and home routers. Eleven of the 13 routers analyzed can be taken over from a Wide Area Network. Two of these attacks didn't even require an active management session. The most common successful attack was Cross Site Request Forgery (CSRF). If CSRF doesn't work, they used shell command injection. The results of their study showed that all the observed routers could be exploited by a moderately-skilled attacker.
- A compromised router could be used to launch a number of attacks like a man-in-the-middle attack, impersonating servers, or a denial of service attack against its users. In most home and small office networks, routers also act as firewalls, so this makes the whole home vulnerable. Evaluated routers are from leading router manufacturers like Linksys, Belkin, Netgear, TP-Link, D-Link, ASUS, and TRENDnet.
- Most routers don't provide software updates. Finding and fixing the security issues in the router causes the manufacturing cost to go up, so manufacturers lose their competitive edge in the market. Security is not a manufacturer's primary concern.
- The average homeowner is happy with an old router with security issues as long as it is doing the job. He is either unaware of the security issue or doesn't care about the security flaws, thinking "who is going to hack me?"

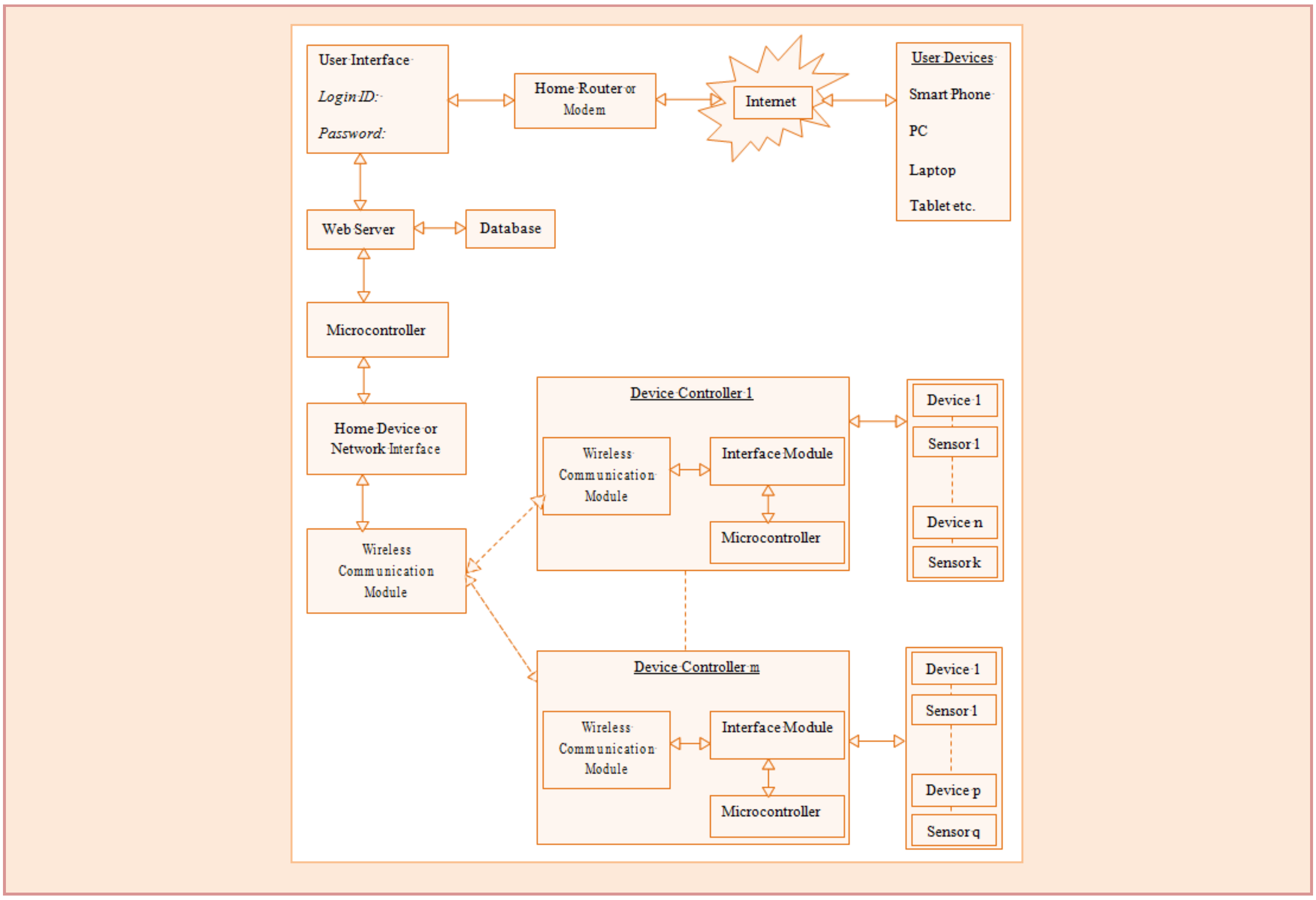


Figure 3. An Internet-based home automation system

From the study we can infer that routers implemented in homes are vulnerable to hacks because of carelessness from the user when choosing the product, poor router configuration, and poor device security from router manufacturers. Even though the home automation system and its access methods are completely secure, vulnerabilities in the home router can compromise a home. An attacker can scan for a particular type of vulnerability belonging to a router from a specific manufacturer.

Internet: A home inhabitant can access and control his or her home from anywhere in the world if the home automation system is connected to the Internet. It has advantages, as we discussed earlier, but connecting the home to the Internet opens it up to the world, i.e. anyone with an Internet connection can try to access the home. An attacker can search for known vulnerabilities and zero-day exploits belonging to a particular device from a specific manufacturer from anywhere in the world. If the home was not connected to the Internet, attackers have to be in the proximity of the home to exploit the vulnerabilities. In other words, the probability of an attack decreases considerably, but it defeats the whole purpose of automating the home.

End User and their Portable Devices: Advancements in electronics, processing power, and a considerable reduction in size and cost allows people to own and frequently use mobile portable devices for accessing the Internet. So people use smartphones, laptops, and tablets to access their homes via the Internet. This allows a flexible and convenient way for home inhabitants to access their home on the go. They use the same device to access other applications and do their daily tasks like browsing, playing games, installing apps, and watching movies with the Internet. This increases the probability of having a security risk in the mobile device, as we can't expect an average Internet user to be security conscious all the time. When a user accesses their home from a compromised mobile device, an attacker could easily steal legitimate user credentials to access the home. This, coupled with known and unknown vulnerabilities in the installed applications and services, raises serious questions about the portable device's security. Furthermore, a user's mobile devices can be stolen by an attacker, so if the user is already logged in to his home via a smartphone app., the attacker can then easily access the home. Also, the end user is vulnerable to social engineering, and their choice of user credentials can be questioned, as discussed before.

In short, connecting a home automation system to the Internet has its advantages and disadvantages. Home automation system users have to be aware of these security issues and operate their home automation system accordingly.

■ Decentralized Approach to Home Automation Systems

Home automation systems discussed so far use a central controller or centralized approach, which has a single point of failure. In this section, we discuss another approach.

The work of M. Gauger *et al.* [49] proposes a decentralized approach to home automation control. They implement the decentralized approach by integrating actuators into the WSN of the home. The authors propose a distributed control or process architecture. The information from the sensors are received and processed by one or more control nodes, which in turn initiates the appropriate actuators to change or control the environment as previously specified by the user. The system thus eliminates the need for a central controller.

Issues in the decentralized approach for home automation systems:

- A sophisticated attacker with prior knowledge of the network and actuator positions can simply disconnect them from the network. No alert mechanisms are implemented for such a case.
- The communications proposed here are done in clear text, so an attacker with the right hardware can eavesdrop on the communication.
- A home automation system consists of complicated tasks which require analyzing and processing various values and inputs from different parts of the home during different points of time. It requires some processing power and storage, which the actuator nodes can't provide at present.

The decentralized approach to home automation is an interesting concept, but it requires a lot of work from the research community to be efficiently and securely implemented in a home environment. In addition to this, the actuators discussed here require a significant increase in processing power and storage for it to be effective in a decentralized architecture.

■ Role of User Interface in Security

According to a recent study done on mobile phone usage, by the end of 2017, 5.13 billion people will be using mobile phones, and out of them, 2.50 billion will be using smartphones. It is only a natural evolution for people to expect more functionality on their phones, like controlling their homes from it. User interfaces provide a way for a user to interact with an application, in this case their home automation system. So, understanding a user's preferences and how a user interacts with a device is crucial in ensuring home security.

The work of T. Koskela and K. Vaananen-Vainio-Mattila [50] demonstrate that, out of the choices of PC, media terminal, or mobile phone for control devices at home, people prefer PCs to set their pre-planned activities or pattern control, while mobile phones are preferred by people as an instant control mechanism for home devices like a remote, as they always carry it with them. Inhabitants rarely choose media terminals to control their home devices.

A study done by M. Ahmed *et al.* [51] showed that almost 65% of economic damage in information security breaches are caused due to human mistakes. Home automation systems are designed to be operated by humans. So user interfaces for popular home automation control devices like smartphones, tablets, computers, and laptops should be designed efficiently in a way that is easy to understand. Interface designers should also consider the fact that these control devices will be operated by people of all ages and varying technical knowledge.

People tend to follow habitual actions, like if they constantly click yes buttons, they have a tendency to click yes buttons even if they want to click no. Interface designers should take this into account when they are developing security control interfaces for home automation systems. In their work, T. Klockar *et al.* [52] implore user interface designers to consider a user's mental model while designing security-critical user interfaces. The mental model signifies what a user understands or assumes when seeing a menu or an option.

Conclusion

Our work focuses on the security aspect of the existing home automation system and points out its flaws. It shows how the concept of security and meaning of the word "intruder" has changed in modern homes. The paper points out the shortcomings of existing home automation systems in identifying and preventing sophisticated intruders in a home environment.

For future work in the field of home automation security, we encourage the researchers to consider a home automation system as a whole and develop behavior prediction and advanced sensing parameters that can help to identify and prevent skilled and sophisticated intruders.

Security is vital for the proper implementation and development of the home automation systems. Moreover, it provides a sense of security to a home's inhabitants and puts their minds at ease.

References

[1] Brand, S, How Buildings Learn, New York, Viking, 1994.

[2] R.E. Grinter, N. Ducheneaut, W.K. Edwards, M. Newman, "The work to make a home network work," in *Proc. of Ninth European Conference on Computer-Supported Cooperative Work (ECSCW 05)*, pp. 469-488, 2005. Article (CrossRef Link)

[3] M. Chetty, J.-Y. Sung, R. E. Grinter, "How Smart Homes Learn: The Evolution of the Networked Home and Household," *Lecture Notes in Computer Science,* vol. 4717, pp. 127-144, 2007. Article (CrossRef Link)

[4] Greichen, J.J., "Value based home automation or today's market," *IEEE Transactions on Consumer Electronics*, vol. 38, no. 3, pp.34-38, Aug. 1992. Article (CrossRef Link)

[5] "The X10 Specification," *X-10 (USA) Inc*., 1990.

[6] "ZigBee Specifications," *ZigBee Alliance*, version 1.0 r13, Dec. 2006.

[7] "LonTalk Protocol Specification Version 3.0," *Echelon Co*, 1994.

[8] "EIA-600 CEBus Standard Specification," *EIA*, 1992.

[9] A.J. Bernheim Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, C. Dixon, "Home automation in the Wild: Challenges and Opportunities," in *CHI '11 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2115-2124, 2011. Article (CrossRef Link)

[10] K. Madhuri, B. L. Sai, B. S. Sirisha, "A Home Automation System Design Using Hardware Descriptive Tools," *International Journal of Engineering Research & Technology*, vol. 2, no. 7, Jul. 2013. Article (CrossRef Link)

[11] E.M.C Wong, "A Phone-Based Remote Controller for Home and Office Automation," *IEEE Transactions on Consumer Electronics*, vol. 40, no. 1, pp.28-34, Feb. 1994.

[12] A. ElShafee, K. A. Hamed, "Design and Implementation of a WiFi Based home automation System," *World Academy of Science, Engineering and Technology*, vol. 6, 2012.

[13] M. Danaher, D. Nguyen, "Mobile Home Security with GPRS," in p*roceedings of the 8th International Symposium for Information Science,* Oct. 2002.

[14] A. Alheraish, "Design and Implementation of Home Automation System," *IEEE Transactions on Consumer Electronics*, vol. 50 , no. 4, pp.1087-1092, Nov. 2004. Article (CrossRef Link)

[15] V. Singhvi, A. Krause, C. Guestrin, James H. Garrett Jr., H. Scott Matthews, "Intelligent Light Control using Sensor Networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, SenSys '05, pp. 218-229, 2005. Article (CrossRef Link)

[16] A. Gaddam, "Development of a Bed Sensor for an Integrated Digital Home Monitoring System," *IEEE International Workshop on Medical Measurements and Applications*, pp. 33-38, May 2008. Article (CrossRef Link)

[17] U. Saeed, S. Syed, S.Z. Qazi, N.Khan, A.Khan, M.Babar, "Multi-advantage and security based home automation system," *2010 Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS)*, pp.7-11, Nov. 2010. Article (CrossRef Link)

[18] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks*, vol. 1, pp. 293–315, 2003. Article (CrossRef Link)

[19] Y. Hu, A. Perrig, D. Johnson, "Wormhole attacks in wireless networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–380, Feb. 2006. Article (CrossRef Link)

[20] J. Wright, "Practical ZigBee Exploitation Framework", *Toorcon*, Oct. 2011.

[21] Z. Feng, J. Ning, I. Broustis, K. Pelechrinis, S.V. Krishnamurthy, M. Faloutsos, "Coping with Packet Replay Attacks in Wireless Networks," *8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 368-376, Jun. 2011. Article (CrossRef Link)

[22] B. Fouladi, S. Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol," *Black hat USA*, Aug. 2013.

[23] T. Oluwafemi, S. Gupta, S. Patel, T. Kohno, "Experimental Security Analyses of Non-Networked Compact Fluorescent Lamps: A Case Study of home automation Security," *Workshop on Learning from Authoritative Security Experiment Results*, pp. 13 – 34, Oct. 2013.

[24] A. Verrotti, D. Trotta, C. Salladini, G. Corcia, G. Latini, R. Cutarella, F. Chiarelli, "Photosensitivity and epilepsy: a follow-up study," Developmental Medicine & Child Neurology, vol. 46, no. 5, pp. 347-351, May 2004. Article (CrossRef Link)

[25] T. Hyun-Jin Kim, L. Bauer, J. Newsome, A. Perrig, J. Walker, "Access Right Assignment Mechanisms for Secure Home Networks," *Journal of Communications and Networks*, vol. 13, no. 2, pp. 175-186, 2011. Article (CrossRef Link)

[26] Michelle L. Mazurek, "Access Control for Home Data Sharing: Attitudes, Needs and Practices," in *CHI'10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 645-654, 2010. Article (CrossRef Link)

[27] Anind K. Dey, "Understanding and Using Context," *Personal and Ubiquitous Computing*, vol. 5, no. 1, pp. 4-7, Feb. 2001. Article (CrossRef Link)

[28] B. Schilit, N. Adams, R. Want, "Context-Aware Computing Applications," in *WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications*, pp. 85-90, 1994. Article (CrossRef Link)

[29] V. Bellotti, K. Edwards, "Intelligibility and Accountability: Human Considerations in Context Aware Systems," *Human-Computer Interaction*, vol. 16, issue 2, pp. 193-212, Dec. 2001. Article (CrossRef Link)

[30] Stephen S. Intille, "Designing a Home of the Future," *IEEE Pervasive Computing*, vol. 1, no. 2, pp. 76-82, Apr. 2002. Article (CrossRef Link)

[31] S.-M. Tsai, P.-C. Yang , S.-S. Wu , S.-S. Sun, "A Service of Home Security System on Intelligent Network," *IEEE Transactions on Consumer Electronics*, vol. 44, no. 4, pp. 1360-1366, Nov. 1998. Article (CrossRef Link)

[32] K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva, "SmartEye - Integrated solution to home automation, security and monitoring through mobile phones," *Third International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '09*, pp. 64-69, Sep. 2009. Article (CrossRef Link)

[33] N. Sriskanthan, F. Tan, A. Karande, "Bluetooth based home automation system," *Microprocessors and Microsystems, Elsevier*, vol. 26, pp. 281-289, 2002. Article (CrossRef Link)

[34] H. Kanma, N. Wakabayashi, R. Kanazawa, H. Ito, "Home Appliance Control System over Bluetooth with a Cellular Phone," *IEEE Transactions on Consumer Electronics*, vol. 49 , no. 4, pp.1049-1053, Nov. 2003. Article (CrossRef Link)

[35] M. Ryan, "Bluetooth: With Low Energy comes Low Security," *WOOT'13 Proceedings of the 7th USENIX conference on Offensive Technologies*, pp. 4-4, 2013.

[36] M. Sikandar, H. Khiyal, A. Khan, E. Shehzadi, "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security," *Issues in Informing Science & Information Technology*, vol. 6, Jan. 2009.

[37] A. R. Delgado, R. Picking, V. Grout, "Remote-Controlled home automation systems with Different Network Technologies," *Centre for Applied Internet Research (CAIR)*, University of Wales, 2009.

[38] Bing-Fei Wu, Hsin-Yuan Peng, Chao-Jung Chen, "A Practical Home Security System via Mobile Phones," *TELE-INFO'06 Proceedings of the 5th WSEAS international conference on Telecommunications and informatics*, pp. 299-304, 2006.

[39] Lili Yang, Shuang-Hua Yang, Fang Yao, "Safety and Security of Remote Monitoring and Control of intelligent Home Environments," *IEEE International Conference on Systems, Man and Cybernetics*, 2006. SMC '06, vol.2, pp. 1149-1153, Oct. 2006. Article (CrossRef Link)

[40] U. Ali, S.J. Nawaz, N. Jawad, "A Real-time Control System for Home/Office appliances automation, from mobile device through GPRS network," *13th IEEE International Conference on Electronics, Circuits and Systems, ICECS '06*, pp. 854-857, 2006. Article (CrossRef Link)

[41] Jian-she Jin, Jing Jin, Yong-hui Wang, Ke Zhao, Jia-jun Hu, "Development of Remote-Controlled home automation system with Wireless Sensor Network," *Fifth IEEE International Symposium on Embedded Computing, SEC '08*, pp. 169-173, Oct. 2008. Article (CrossRef Link)

[42] S.R. Das, S. Chita, N. Peterson, B. Shirazi, "home automation and Security for Mobile Devices," *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*, pp. 141-146, 2011. Article (CrossRef Link)

[43] Leo Kelion, "Breached webcam and baby monitor site flagged by watchdogs," http://www.bbc.com/news/technology-30121159, BBC News, 2014.

[44] L. Muhury, A.H.M.A. Habib, "Device Control by Using GSM Network," *15th International Conference on Computer and Information Technology (ICCIT)*, pp. 271-274, Dec. 2012. Article (CrossRef Link)

[45] R. Sasi, "How I DOS'ed My Bank," *Hack in the Box Security Conference (HITBSecConf2013)*, Oct. 2013.

[46] A. Z. Alkar, U. Buhur, "An Internet Based Wireless Home Automation System for Multifunctional Devices," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 4, pp.1169-1174, Nov. 2005. Article (CrossRef Link)

[47] J. Shah, B. Modi, R. Singh, “Wireless Home Appliances Controlling System,” *International Conference on Electronics and Communication Systems (ICECS)*, pp. 1-6, Feb. 2014. Article (CrossRef Link)

[48] Security Evaluators, “Exploiting SOHO Routers,” *Router Case Studies*, 2013.

[49] M. Gauger, D. Minder, P. J. Marrón, A. Wacker, A. Lachenmann, “Prototyping Sensor-Actuator Networks for home automation,” in *Proc. of the 3rd Workshop on Real- World Wireless Sensor Networks (REALWSN 2008)*, 2008. Article (CrossRef Link)

[50] Tiiu Koskela, Kaisa Väänänen-Vainio-Mattila, “Evolution towards smart home environments: empirical evaluation of three user interfaces,” *Personal and Ubiquitous Computing*, vol. 8, no 3-4, pp. 234-240, Jul. 2004. Article (CrossRef Link)

[51] Ahmed, M., Sharif, L. Kabir, M. Al-Maimani, M, “Human Errors in Information Security,” *International Journal*, 1(3), 2012.

[52] T. Klockar, David A. Carr, A. Hedman, T. Johansson, F. Bengtsson, “Usability of Mobile Phones,” *Department of Computer Science and Electrical Engineering, Luleå University of Technology*, 2005.

Arun Cyril Jose received a degree in Engineering in Computer Science from Mahatma Gandhi University, India in 2009 and his Master’s in Forensic Computing from Coventry University, United Kingdom in 2011. He is currently a PhD student in the Department of Electrical Electronic and Computer Engineering at the University of Pretoria, South Africa. His research interests include home automation security, distributed denial of service attacks, different online surveillance techniques, security-based social engineering, other implementations of P2P protocols, network vulnerability detection and intrusion prevention, network traffic analysis, and completely anonymous communication over the Internet.

Dr Reza Malekian (PhD, PostDoc, CEng) is a Senior Lecturer in the Department of Electrical, Electronic and Computer Engineering at the University of Pretoria, South Africa. He is also a professional member of the British Computer Society and a member of the management committee of Cost Action 1304 (ACROSS). His research interests lie in the area of advanced sensor networks, the Internet of Things, and mobile communications