Problem statement : Home automation systems face four main challenges, these are high cost of ownership, inflexibility, poor manageability, and difficulty achieving security. The main objectives of the project is to design and to implement a cheap and open source home automation system that is capable of controlling and automating most of the house appliance through an easy manageable web interface to run and maintain the home automation system

Features:

automatic lighting (wrt to door and outside lighting. Also syncing with tv)

Temperature control

Motion sensors

Trash collection detection

Screen time control (wrt tv)

Appointment reminders

Energy and water management

 Smart locks- security

Room decor with the help of application

Integration and interoperability

Smoke detector

Smart refrigerator

Various Home Automation Methodologies Analysed:

■ 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 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. 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 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 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. 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. 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. 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 t h e I 2C Bus. The system allows more than one device controller to be connected to the host controller. The work of H. Kanma et al. 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 Smart Computing Review, vol. 5, no. 4, August 2015 276 • 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. 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).

■ SMS-based Home Automation System :The work of A. Alheraish 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. 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. Saeed et al. 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., 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 and U. Saeed et al. ), 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. 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 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. 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

. ■ 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 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. 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. 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 Smart Computing Review, vol. 5, no. 4, August 2015 278 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. 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. 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. developed an iOS-based home automation security system using GPRS. The proposed system uses t h e 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 , B. Wu et al. , L. Yang et al. , and S.R. Das et al. 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 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. can be spoofed by a skilled intruder, so its ability to identify intruders can be questioned. • The work of L. Yang et al. 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. 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 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 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. 279 Jose et al.: Smart Home Automation Security: A Literature Review 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 t h e 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 b e l o w 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. 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. Smart Computing Review, vol. 5, no. 4, August 2015 280 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, a n d 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, WiFi and RF communication below. The work of A.Z. Alkar and U. Buhur 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, a n d 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 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?” 281 Jose et al.: Smart Home Automation Security: A Literature Review 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.

