International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Survey on Efficient Home Automation Systems using IoT

Ms. Anagha Laxmi Hegde[1], Ms. Chetana Anand[2], Ms. Swathi S[3], Ms. Kavana L. S[4], Ms. Jyothi B[5]

[1,2,3,4] UG Student, Department of Information Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India
[5]Assistant Professor, Department of Information Science and Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India

---

Abstract -*An Interactivity with domestic devices can be achieved with the help of Internet of Things. An effective home automation system uses mobile devices to automate home functions and features through the internet. It uses the concept of Internet of Things to combine the benefits of wireless communication and automation technology to provide home owners with remote control of appliances as well as access to sensor data. However, it is susceptible to a few shortcomings. The different varieties of existing home automation systems and their general working mechanisms are discussed. A few disadvantages pertaining to energy efficiency, security and environmental consciousness are explored and some solutions are offered.*

Key Words: **Home Automation, Internet of Things, Lightweight Encryption, Security, Sensor System Integration, Smart Home, Solar Energy**

1. INTRODUCTION

Internet of Things is a field of technology that leverages the connection between ordinary objects and the internet with the assistance of information sensors such as radio frequency identification, temperature sensor, GPS and QR scanner to exchange information and communicate for positioning, monitoring and tracking purposes. It is the concept of interaction of machines or things with the environment. This interaction is achieved by the communication and exchange of data collected by sensors. Sensors gather information from the surrounding environment and provide input to the processing and decision-making aspects of the system. Internet of Things involves advanced connectivity with devices, systems and services that is beyond automation and machine-to-machine communication. Internet of Things has been employed in various systems performing as Traffic Monitoring, Waste Management, Agricultural activities, Environment Monitoring etc.

By bringing the technologies of Internet of Things to the concept of home automation, there have been numerous interactive home systems designed in the past few years. Home automation systems embody the vision of ubiquitous computing as proposed by Mark Weiser. A successful interactive residence is one where the complex technologies used to build the system disappear underneath a clear abstraction so that users need not bother about the mundane tasks or the techniques used to automate them. There is no doubt that advances made in this field promote not only convenience but also security, productivity and scope for further research.

It has been established that using Internet of Things to automate your house enriches your lifestyle. However, smart grid infrastructures are also designed to improve the energy management in the house. Conceptually, a smart grid integrates information technologies and electronics into the house so as to strengthen reliability and efficiency of the electrical workings. Specifically, implementation of Interactive Residence minimizes the electricity usage by coordinating the load balance in the systems. This is taken a step further by utilizing solar power to supply electricity for all devices and appliances.

In home automation, collaboration with portable and wearable or embedded devices with more memory, processing power and diverse sensing technology is needed. This increased interactivity of IoT devices also increases the amount of data being handled and manipulated to provide the intended services. Even though IoT is capable of supporting new home automation models, increasing the efficiency of many applications, and enriching the life of users, the risks are significantly higher. Merging the cyber and physical world gives way to a higher amount of safety and privacy issues than the cyber-only Internet.

2. EXISTING SYSTEMS

With massive advances constantly being made in technology, a large variety of home automation systems have been designed and marketed. Using a number of techniques, there have been systems such as Context-aware Home Automation Systems, Central Controller based Home Automation System, Bluetooth based Home Automation System, GSM or Mobile based home Automation Systems etc.

2.1 Bluetooth based Home Automation System

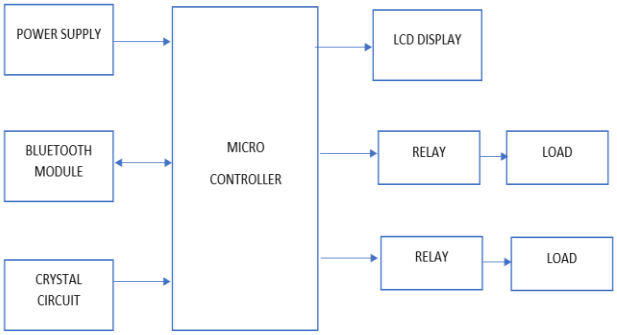

Fig-1: Bluetooth based Home Automation System

Fig-1 represents the existing Bluetooth based system for Home Automation. In this system, the 8051 microcontroller is interfaced with the Bluetooth module. An Android application uses wireless communication to send messages to the Bluetooth. The 8051 microcontroller is coded to receive commands from the Bluetooth in serial manner. The microcontroller automatically switches the loads in the home based on the command received from the Bluetooth. This system consists of a microcontroller, a Bluetooth module, two 5V relays, a lamp, LCD display and DC motor. The reset circuit and crystal circuit must be connected to the circuit to ensure proper working. LCD displays the status of the electrical loads. It also displays the data received from the Bluetooth.

2.2 Central Controller based Home Automation System

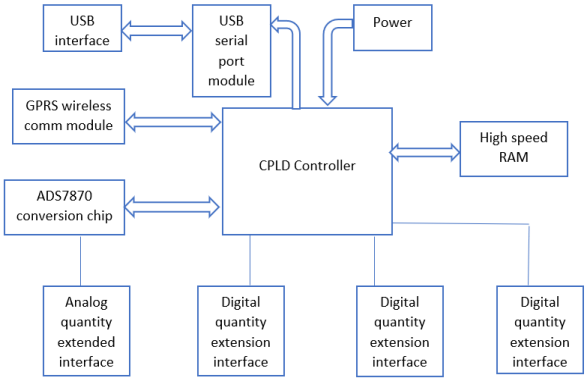

Fig-2: Central Controller based Home Automation System

This type of home automation and control system uses CPLD (Complex Programmable Logic Device). It is quite similar to a microcontroller but it uses Field Programmable Gate Array (FPGA) which provides a different type of hardware control. The main advantage of CPLD is that it can acquire sensor data parallelly and improve the real time efficiency of the system. This system employs a central controller to set up actuator network and radio frequency wireless sensor. The various modules of the system are designed to control the house appliances directly. The central controller system's functionalities are device remote control, appliance monitoring, energy statistics, security etc.

2.3 GSM Based Home Automation System

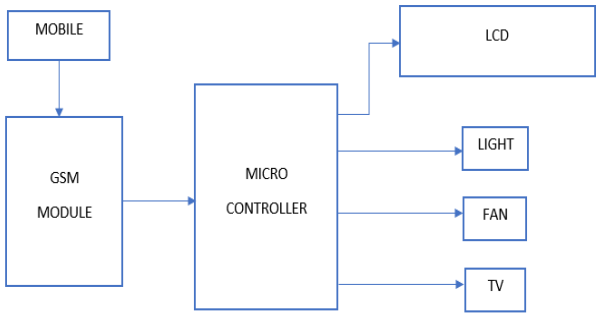

Fig-3: GSM Based Home Automation System

The GSM based Home Automation system comprises of a hardware architecture with s stand-alone embedded system. The hardware is based on 8-bit microcontroller-ATMega2560, GSM handset with GSM Modem-SIM900, sensors and relay. The software is in the form of Arduino programs and an Android application running on the user's handset. The GSM modem is in charge of the communication between owners and the home system via SMS. The SMS includes commands to be performed. The format of the SMS is predefined by the developer. The command is sent to the GSM modem through the GSM public network using text messages. When the modem receives the messages, the microcontroller extracts and executes the commands. ON/OFF functions and alarms can be controlled in this manner.

3. DISADVANTAGES OF EXISTING SYSTEMS

3.1 Energy Source

The basic design and working of various existing home automation systems have been discussed in the previous section. There are numerous liabilities that can be observed in them. The most important disadvantage is the use of only conventional energy sources to power the systems. A system that is unequivocally dependent on commercial power supply is not truly grasping at the immense flexibility granted by home automation systems using Internet of Things. Commercial energy sources are depleting; they are non-renewable and hence, non-sustainable.

Given the current condition of the environment, there is a sizable demand for energy saving and better efficiency in

energy consumption with the help of smart technology. The role of home automation systems to this end is becoming increasingly important. With the variety of functions available in such a system, the users are provided with the flexibility of monitoring the energy consumption of the house and making lifestyle changes to save electricity.

3.2 Security Issues

A liability of the existing systems is the use of networking functionalities of Bluetooth, GSM etc. These technologies are susceptible to network hijacking and various security risks. It is quite difficult to ensure a standard, strong security measure to counteract any malicious attempts. Software in Bluetooth devices will not be perfect. It is quite easy for attackers to discover previously unknown vulnerabilities. Bluetooth is designed to be a "personal area network" and hence devices outside the range should not be accessible by Bluetooth. However, hackers have used directional, high gain antennae to communicate over greater distances.

When it comes to GSM technology, there are two major issues. The first problem with GSM devices are their unilateral authentication schemes as well as vulnerability to man-in-the-middle attacks. GSM networks authenticate users but they do not authenticate the network itself. Malicious attempts can be made by using a false BTS to impersonate the legitimate user's network code and ensue a man-in-the-middle attack. Several scenarios can be performed to change or fabricate the data. Another issue can be termed as "over the air cracking". This method is used to leverage the vulnerability of COMP128 in order to extract the Ki of the user who operates the home automation system without any physical access to the SIM. To do this, the attacker sends multiple challenges to the SIM and analyzes the responses. The IMSI can also be discovered with another approach. Once the attackers know both Ki and IMSI, he can clone the user's SIM to operate phone services and intercept the SMS sent by the system's controller.

Regardless of the method, there are a general set of threats posed by attackers to the security of the house. These threats and the corresponding security goal that they violate are provided in Table 1.

Table-1: Security Threats

Threats	Security goals
Message Alteration Eavesdropping	Authentication Integrity Confidentiality
Malicious Software Tampering Modification Updating	Authentication Integrity
Denial of Service Reply Attacks	Non-Repudiation Integrity Authentication

4. MEASURES TO OVERCOME DISADVANTAGES

4.1 Using Solar Energy

With smart technology and traditional ideas, the use of solar energy is highly beneficial to these systems. As a result, a system that is primarily integrated with solar inverter to reduce the direct dependency on commercial energy must be preferred. According to studies, Residential Energy Consumption accounts for 1/4th of the total electricity consumption in India and this number expected to significantly increase in the future owing to rapid electrification and technology development leading to more appliances at affordable prices. This trend can be visualized with the help of Fig-4.

Grid connected renewable energy (RE) capacity in India has increased about seven times to 35 GW in the last decade. Solar Energy is weather dependent which makes load management a useful tool available in automated houses. Load management includes either reducing the usage of electricity through conservation or reallocating it to time periods when solar generation is high. In addition, home automation systems can generate the required amount of electricity through rooftop solar panels. This introduces a bi-directional network of decentralized sources of energy generation to replace the traditional unidirectional nature of the grid (from large-scale power plants to consumers).

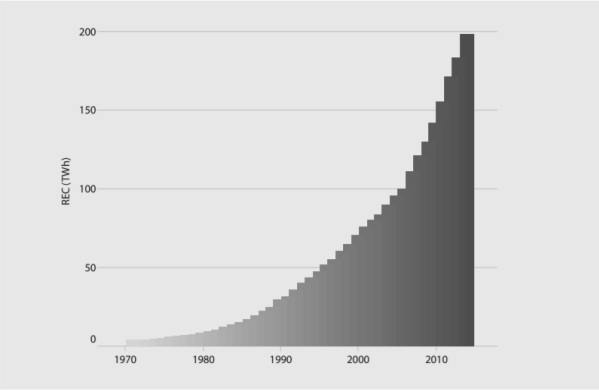

Chart-1: Trend in India's residential energy consumption

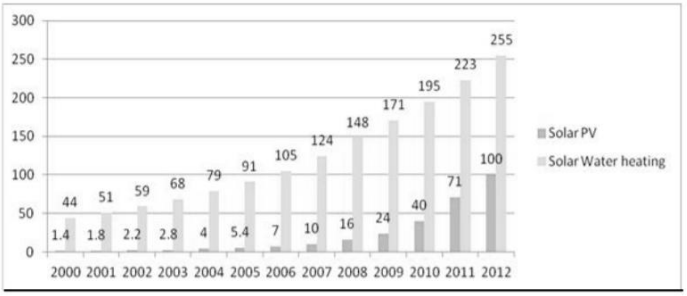

Chart-2: Global capacity of solar PV and solar water heating

4.2 Private Wi-Fi Networks and Lightweight Encryption

A possible option to counteract the ill effects of the previously mentioned technologies is to use Wi-Fi. Wi-Fi security is at the forefront of every wireless communication discussion and it is not fail-safe by any means. But with the rising number of laptops and handheld devices enabled with Bluetooth, security experts are of the opinion that "personal area network" type of wireless technology poses a greater risk than the average Wi-Fi network. Wi-Fi uses wireless access devices to connect clients whereas each Bluetooth device acts as an access point itself. Thierry Zoller, a security consultant with n. runs AG has observed that "the potential for abuse is a lot greater for Bluetooth than for Wi-Fi, as every Bluetooth device is a potential entry point to the local network".

GSM communication for mobiles is more secure compared to Bluetooth and by using hotspot, users can access the same functionality with their laptops. To combat the issues mentioned earlier, a private Wi-Fi connection can be used in the place of GSM. Private Wi-Fi connections are the networks that are set up to be strictly used by the homeowners or office employees. When set up in a proper fashion, they allow password protected access and encryption to the data being transmitted and received. This method, layered with anti-malware protection, VPNs, firewalls etc. proves to be safest approach.

Among the vulnerabilities mentioned in Table-1 is the breach of confidentiality that occurs when authentication and integrity of the system are violated. Confidentiality needs to be addressed urgently to give a basic sense of security to the home owners. Crucial information is present in the data exchanged between home devices and the automation related to the user's privacy and safety. However, there are some challenges present in providing the system with confidentiality services. The efficiency of processing and communication along with the flexibility of key management are a few. Many small, resource-constrained devices are involved in home automation systems. In order to solve this issue, a lightweight encryption scheme might be used. This scheme will provide users and appliances with confidentiality service without incurring the heavy overhead cost associated with computation and communication. This scheme must support flexible public key management through identity-based encryption without complex certificate requirements. The scheme should also deliver a reasonable level of efficiency with respect to the overhead cost associated with computation and communication.

5. CONCLUSION

The emergence on Internet of Things has given vast scope to constantly improve upon trivial tasks in everyday life for which technology can replace human interaction. An effective home automation system is an application of Internet of Things that provides convenience and simplified control of domestic appliances to home owners. With a user-friendly UI and straightforward operations, increased usability is provided by this system. It can store a variety of sensor parameters for users to access and respond to accordingly. The disadvantages of existing systems have been explored. To improve upon them, solar power utilization has been suggested to add sustainability and a smart outlook on the relationship between technology and the environment.

REFERENCES

[1] Xiaobo Mao, Keqiang Li, Zhiqiang Zhang, Jing Liang "Design and Implementation of a New Smart Home Control System Based on Internet of Things" Zhengzhou University, China, 978-1-5386-2524-8/17/ ©2017 IEEE

[2] Kaibalya Prasad Panda, Nirakar Behera, Shubhrajit Parida "Wireless Power Transfer Application in Solar Power Inverter Integrated Internet of Things based Home Automation" C.V. Raman College of Engineering, Orissa, 2017 International Conference on Power and Embedded Drive Control (ICPEDC)

[3] Yujun Han, Baobin Liu "Interactive Smart Home Design Based on Internet of Things" School of Information Technology, Nanjing, China, The 12th International Conference on Computer Science & Education (ICCSE 2017) August 22-25, 2017. University of Houston, USA

[4] "Home Computing Unplugged: Why, Where and When People Use Different Connected Devices at Home" Fahim Kawsar A. J. Bernheim Brush

[5] "Location Aware Resource Management in Smart Homes" - Abhishek Roy, Soumya K. Das Bhaumik, Amiya Bhattacharya

[6] "Conceptual framework for IOT, virtualization via openFlow in context aware networks"-Rahim Rahmani, Arif Mahmud

[7] Z. Yu, X. Zhou, Z. Yu, J. H. Park and J. Ma, "iMuseum: A scalable context-aware intelligent museum system," Computer Communications, vol. 31, No. 18, pp. 4376-4382, 2008.

[8] N. S. Liang, L. C. Fu, C. L. Wu, "An integrated, flexible, and Internet-based control architecture for home automation system in the internet era", in Proceedings ICRA '02. IEEE International Conference on Robotics and Automation, Vol. 2, pp.1101-1106, May 2002.

[9] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms," in Proceedings of the 6th International Conference on the Internet of Things.