



An Intelligent and Effective Cyber-Secured Smart-Home Automation System with Embedded AI



Mohd Kamran Ikram , Karama M. K. Senan, Mohd Mustaqeem, and Mohammad Sarfraz 

Abstract With technological advancement, the concept of controlling household equipment remotely via the internet from anywhere in the world at any time is now a reality. This paper presents intelligent smartphone-based home automation and cyber-secured system by using an Arduino microcontroller. The system has two modes of operation, the manual mode, and automatic mode, i.e., the system can operate on its own without any interference of humans or in a dehumanized way. The hardware of the proposed method is successfully developed and its various subsystems are successfully tested. With the help of the ESP866 Wi-Fi module, the whole system can be taken to the cloud (online) mode and the system can be accessed from anywhere in the world. When the appliances start exchanging information with smartphones, and this makes the system vulnerable to security threats and hence threatens the privacy and security of the end-user. The security requirement will be displayed in second place. Our proposed method can provide additional protection in network security, which is easily integrated with heterogeneous IoT devices and protocols.

Keywords Home automation · Cyber security · Vulnerability · Threat · Arduino · Microcontroller · Sensor

1 Introduction

Automation is an integral part of human life and it brings ease to the users by giving them the freedom to control and monitor their home appliances by just using a smartphone. It also gives tons of advantages to the old aged and handicapped

M. K. Ikram (✉) · K. M. K. Senan · M. Sarfraz
Department of Electrical Engineering, Aligarh Muslim University, Aligarh, UP 202002, India
e-mail: mki.kamran@gmail.com

M. Sarfraz
e-mail: msarfraz@zhcet.ac.in

M. Mustaqeem
Department of Computer Science, Aligarh Muslim University, Aligarh, UP 202002, India

people. A smart home is the integration of twenty-first century people. It is basically deploying technology into the home to improve quality of life [1]. Moreover, it also provides home security [2]. The improved lifestyle is one of the benefits of home automation. Household automation allows customers to manage and monitor many home appliances through a single system, providing more convenience, improved security, and increased energy. Consumers will regulate their home systems and conserve energy more effectively when home automation technologies are integrated into future smart grids [3]. Also, with the advancement of IoT, The Internet of Things is widely regarded as one of the most crucial areas of future technology and the IoT-connected devices are exponentially increasing [4, 5]. Smart homes have been recognized as one of the industrial areas with the greatest potential for IoT adoption, such as home automation and energy management [6].

Plenty of systems of home automation is documented in the literature. ZigBee-based home automation systems are proposed in [7, 8]. Although the ZigBee technology is inexpensive, the integration of different devices of different manufacturers is the main disadvantage associated with this technology [9].

Several methods based on Bluetooth technology and android are reported [10, 11]. Most of the methods require an Arduino board and a cell phone to form the system's hardware architecture, and the Arduino board and cell phone communicate wirelessly using Bluetooth technology. The major issue with these Bluetooth-based smart-home systems is that they can only operate household appliances within Bluetooth range [12].

The voice recognition-based home automation system is also studied and documented [13, 14]. A smartphone-based application is developed to control home appliances by recognizing the voice commands of the user. The android application communicates with microcontroller boards via Bluetooth or Wi-Fi technology. The voice recognition-based system is user-friendly. The major limitation of this method is that it requires a noise-free environment to operate. Moreover, it also demands the correct pronunciation; otherwise, the system will fail to execute the commands.

The global system of mobile communication (GSM) based home automation systems are also presented [15]. The GSM modem is equipped with a microcontroller to decode the SMS sent from the user's mobile device. It has been established that using GSM in a home automation system provides the highest level of security [16]. Moreover, the GSM technology is vulnerable to power failure [9].

In wireless technology, Wi-Fi-based systems are also studied [17, 18]. The Wi-Fi technology enables the user to control home appliances from anywhere in the world. Wi-Fi technology makes home automation systems easier to adopt than ZigBee technology since Wi-Fi has lower connection latency than ZigBee [9].

It is known that IoT-based smart-home automation systems also suffer from the problem of security threats which is a very big challenge to protect the system from cyber-attacks and risk. According to [19], smart-home automation with the learning of human behavior can be secure by reducing the computation overheads, but they have used traditional and conventional methods. In the study [20] author has used the network security approach to protect the system from cyber-attack. They have used the central router concept, but if the attack on the main router becomes successful, all

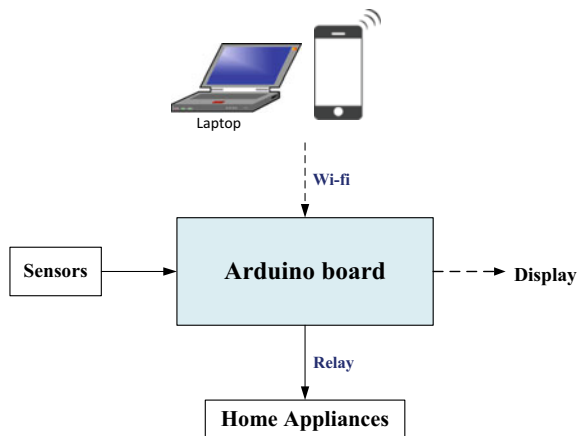
the connected devices will be easily manipulated. In the manuscript [21] author has told about the reference architecture of the smart home that facilitates the security analysis, along with the security attacked surfaces by providing the three viewpoints. Still, they have used old approaches to demonstrate the scenario. In comparison to others, our proposed system will contain multi-level security points that can provide the next level of security to the IoT devices. We will give multi-layered network security so that if the cracker can get the primary level, it cannot break the other layer easily.

In this work, an Arduino microcontroller-based dual-mode home automation system is being designed. The system is controlled via the smartphone/laptop through a Wi-Fi module. In addition to this, the user has control over the system to use it either in manual mode or in automatic mode. Four subsystems are designed, temperature control monitor, lighting control, door security, and fire-fighting systems. This research work is based on machine learning algorithms with the internet of things. IoT devices constitute a large number of devices and sensors that can monitor/control different physical quantities. With the dawn of Big Data, there is a need for proper automated data storage solutions and cloud-based applications to analyze and extract the required information from the data.

2 System Overview

The system is designed so that four subsystems are coupled with an Arduino microcontroller via sensors and the home appliances are connected to the Arduino microcontroller via a relay system for their respective operation. The system is controlled via smartphone/laptop with the help of a Wi-Fi module. The basic system design is shown in Fig. 1.

Fig. 1 System architecture



The proposed methodology has two modes; one is manual mode, in which the user has a choice to operate appliances on his own. The other is an automatic mode in which the home appliances will automatically operate without any interference of humans or can be called a dehumanized mode.

The ESP8266 takes the whole system to the Wi-Fi system mode, where all the developed algorithms and methods are being utilized. The information exchanged among the heterogeneous devices will be taking place in the network-secured manner to fulfill the CIA triad of security.

3 Subsystems

The components of the system are connected with a microcontroller. A 16×2 Liquid Crystal Display (LCD) is used to display the data like room temperature, object distance, and the information about the number of devices connected, etc. The hardware of the system is successfully implemented and its various subsystems are verified. An android application Blynk is used to monitor the connected home appliances.

3.1 Temperature Control Monitoring System

In a temperature control system, an LM35 temperature sensor is used along with the infrared (IR) sensor, the LM35 is used for the purpose of measuring the ambient temperature of the room. The IR sensor is used to improve the accuracy. The temperature is adjusted to be less than $30\text{ }^{\circ}\text{C}$; if the temperature exceeds $30\text{ }^{\circ}\text{C}$, the microcontroller will turn on the fan or Air Conditioner to reduce the temperature.

3.2 Lighting Control System

A LED will turn on according to the place's luminosity. It is performed through a light-dependent resistor (LDR). As the light impinging on the photoresistor gets stronger, the resistance decreases, and the voltage output of the divider increases. The reverse happens when the impinging light gets weaker.

3.3 Door Automatic Opening System

The HC-SR04 is a complete ultrasonic distance measurement device. The HC-SR04 works simply by sending a pulse to the trigger input and waiting for a pulse from

the echo output. The length of this pulse allows the calculation of the distance to the detected object.

3.4 Fire-Fighting System

In the fire-fighting system, an MQ-2 gas sensor is to operate when the amount of smoke or gas exceeds 400%, when this condition occurs, the Arduino will operate the buzzer first and then the fire-fighting system will operate.

3.5 System of Other Appliances

The other appliances like refrigerators, microwave ovens, and geysers can be connected with the home automation system in such a way, they operate in accordance with the user.

4 Cyber-Attack on Home Automation System

The problem with the Wi-Fi-connected home automation devices is that it is remotely controlled when we are away from home. To communicate with them, they need to be connected to the internet (cloud database) from outside the home network. They are controlled by smartphones or laptops that detect the devices and are connected. This availability of the device on the internet through Wi-Fi makes it vulnerable to hackers and attackers to manipulate. It can be done in the following manners, as shown in Fig. 2.

4.1 Man-In-The Middle

In this attack, the attacker can breach, interrupts or spoofs communications between two systems. The attacker can send the fake temperature data generated by the device to be spoofed and sent to the cloud; similarly, the attacker can disable vulnerable devices during heat waves, creating a disastrous situation for the system users.



Fig. 2 Process leading to security happenings

4.2 Data and Identity Stealing

When unprotected wearable and smart devices generate data, they can provide important personal information to the hackers that can be exploited for fraud, transactions, and identity hacks.

4.3 Device Hijacking

In this type of attack, the attacker can hijack the device and control the device effectively. These attacks are quite difficult to detect because the attacker does not change the device's basic functionality. It simply controls a single major device and can get access to others as well.

4.4 Distributed Denial-of-Service

It is the advanced version of the Denial-of-service (DoS) attack. The attacker can flood the incoming traffic coming from multiple sources to a targeted network. It can block the simple source to get access to the data. This attack is now common in IoT devices nowadays due to the lack of security of the devices. Another version called Permanent Denial-of-service (PDoS) attack is a lethal attack. It can damage the device badly the device cannot recover, it can replace, or reinstallation takes place.

5 Protection from Cyber-Attacks of Home Automation System

The IoT devices can be protected by comprehensive IoT security solutions that do not disrupt home or service providers' smart devices. It can include the following things to get a more secure system.

5.1 Multi-level Authentication

As the smart device is ready to connect with the network, it should be authenticated before information exchange with the cloud. This can ensure the data generated from the device is not fraud and corrupt. Hashing algorithms SHA-256 can be used

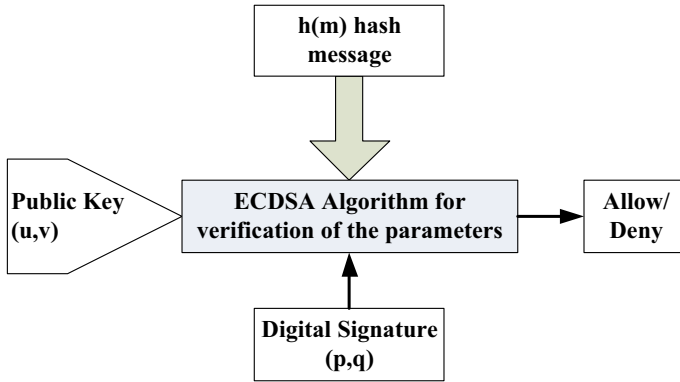


Fig. 3 ECDSA algorithm

for symmetric keys and Elliptic Curve Digital Signature Algorithm (ECDSA) for asymmetric keys cryptography (Fig. 3).

5.2 Network Data Communication Security

Data transmission between the device and cloud can be done in encryption key authentication mode. It can be protected by ensuring or allowing those with the secret decryption key to communicate with the cloud data. The information sent to the cloud by the smart device must be protected from digital eavesdropping (Fig. 4).

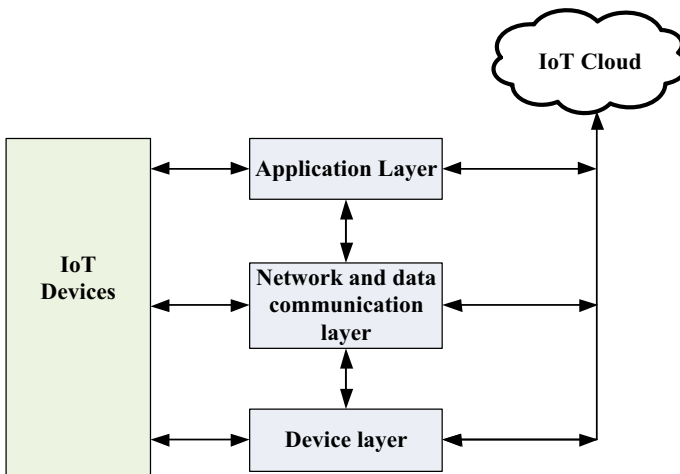


Fig. 4 Security layered model of IoT

5.3 Analysis of Security Monitoring

The cloud system or smartphone will capture the data from the various smart devices, including endpoint devices and network traffic data. Our system can analyze whether any threat or vulnerability occurs or not if necessary actions can be formulated for the system security policy like isolation of vulnerable devices. This analyzing cycle can be run in real-time or later to detect the attack pattern and scenarios.

5.4 Machine Learning Approach

Detecting the anomalies and vulnerability of attacks in the smart-home systems through a traditional approach like traffic pattern recognition, it is better to use dynamic machine learning methods to classify the data flows. It is because the unknown attack detection possibility can also be enhanced by using this approach.

Our proposed model can be secured in the techniques mentioned above. The overall demonstration of the cyber security portion of the proposed model can be seen in Fig. 5. The device present at the device layer and the most important layer, i.e.,

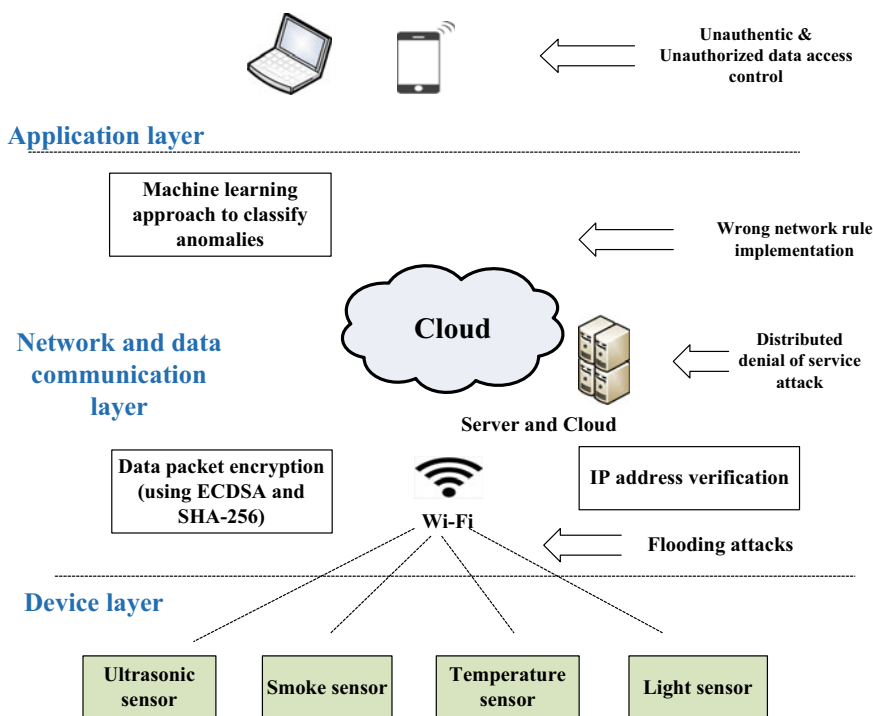


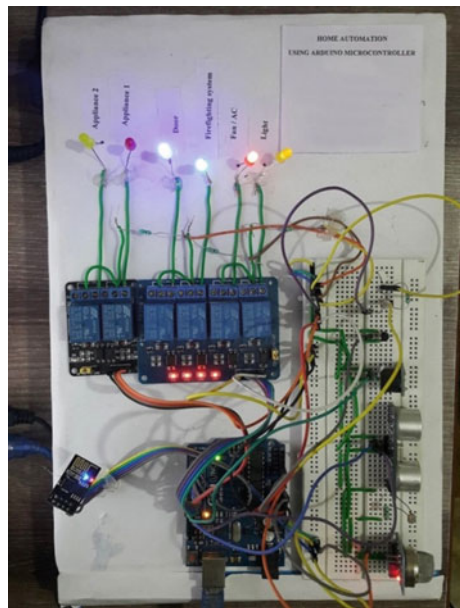
Fig. 5 Overall cyber security demonstration of home automation devices

network, has the vulnerability from multi-level attacks. We have to apply security in data transmission on the second layer by using ECDSA and SHA-256 algorithms for encrypted data transfer and IP-address verification through verification code generation technique along with the anomaly detection using machine learning approach in which we can apply Support Vector Machine (SVM) technique to classify the anomalies in the unknown data. It can classify defective and non-defective datasets, which can save our time to manual and traditional classification and more accuracy so that the information exchange can occur securely.

6 Experimental Evaluation

The Arduino is powered via the USB cable through a laptop or PC. The relays are connected to the output ports of the Arduino. The appliances are connected to the relays; the relays are behaving just like a switch. The system has three main components, the Arduino board, sensors, and a Wi-Fi module. Figure 6 shows an experimental evaluation of the Hardware model of the proposed home automation system. The hardware model is successfully tested on various smartphones and laptops.

Fig. 6 Experimental setup of proposed home automation system



7 Conclusion and Future Research Challenges

This paper proposes a fundamental design of a cyber-secured and smart-home automation system based on Arduino microcontroller and the hardware model is successfully implemented. The key features of this design are low cost, effective, scalable, fast responsive, straightforward implementation, and online compatibility. Moreover, the user can use the system with the help of a smartphone by just downloading an application named Blynk. The system is capable of performing tasks on its own. In security aspects, the proposed system is smart and cyber-secured with multi-level security that can produce a tangible innovation roadmap with real impact, and the system can maintain the security triad, i.e., Confidentiality, Integrity, and Availability (CIA). If anyone wants to get unauthorized access or manipulate the exchanged information, it cannot be done easily; it has to crack the multi-layered security of the system.

In the future, there will be the use of some AI-based techniques to automate the system's security that can detect and correct if any vulnerabilities occur in the system. Because the Arduino MEGA has more pins than the Arduino Uno, the same work may be expanded. Controlling only a few items can be addressed by expanding automation to all other home appliances. Security cameras may be operated, allowing the user to watch what is going on around their home or company. Motion sensors may be used in security systems to detect any illegal movement and alert the user. Through Wi-Fi and sensor signals, the scope of this work may be expanded to numerous locations, rather than being limited to only the home.

References

1. Bromley K, Perry M, Webb G (2003) Trends in smart home systems. Connectivity and services, www.nextwave.org.uk.
2. Das SR, Chita S, Peterson N, Shirazi BA, Bhadkamkar M (2011) Home automation and security for mobile devices. In: 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). IEEE, Seattle, WA, USA, pp 141–146. <https://doi.org/10.1109/PERCOMW.2011.5766856>
3. Ahmim A, Le T, Ososanya E, Haghani S (2016) Design and implementation of a home automation system for smart grid applications. In: 2016 IEEE International Conference on Consumer Electronics (ICCE). IEEE, Las Vegas, NV, USA, pp 538–539. <https://doi.org/10.1109/ICCE.2016.7430721>
4. Ding J, Nemati M, Ranaweera C, Choi J (2020) IoT connectivity technologies and applications: a survey. IEEE Access. 8:67646–67673. <https://doi.org/10.1109/ACCESS.2020.2985932>
5. Lee I, Lee K (2015) The internet of things (IoT): applications, investments, and challenges for enterprises. Bus Horiz 58:431–440. <https://doi.org/10.1016/j.bushor.2015.03.008>
6. Santoso FK, Vun NCH (2015) Securing IoT for smart home system. In: 2015 International Symposium on Consumer Electronics (ISCE). IEEE, Madrid, Spain, pp 1–2. <https://doi.org/10.1109/ISCE.2015.7177843>.
7. Gill K, Yang S-H, Yao F, Lu X (2009) A zigbee-based home automation system. IEEE Trans. Consumer Electron 55:422–430. <https://doi.org/10.1109/TCE.2009.5174403>

8. Byun J, Jeon B, Noh J, Kim Y, Park S (2012) An intelligent self-adjusting sensor for smart home services based on ZigBee communications. *IEEE Trans. Consumer Electron* 58:794–802. <https://doi.org/10.1109/TCE.2012.6311320>
9. Danbatta SJ, Varol A (2019) Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In: 2019 7th International Symposium on Digital Forensics and Security (ISDFS). IEEE, Barcelos, Portugal, pp 1–5. <https://doi.org/10.1109/ISDFS.2019.8757472>
10. Asadullah M, Ullah K (2017) Smart home automation system using Bluetooth technology. In: 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT). IEEE, Karachi, Pakistan, pp 1–6 <https://doi.org/10.1109/ICIEECT.2017.7916544>
11. Husain MdI, Alam M, Rashed MdG, Haque MdE, Rashidul Hasan MAFM, Das D (2019) Bluetooth network based remote controlled home automation system. In: 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT). IEEE, Dhaka, Bangladesh, pp 1–6. <https://doi.org/10.1109/ICASERT.2019.8934500>
12. Al-Ali AR, AL-Rousan M (2004) Java-based home automation system. *IEEE Trans Consumer Electron* 50:498–504. <https://doi.org/10.1109/TCE.2004.1309414>
13. Eric T, Ivanovic S, Milivojsa S, Matic M, Smiljkovic N (2017) Voice control for smart home automation: evaluation of approaches and possible architectures. In: 2017 IEEE 7th International Conference on Consumer Electronics-Berlin (ICCE-Berlin). IEEE, Berlin, pp 140–142. <https://doi.org/10.1109/ICCE-Berlin.2017.8210613>
14. Mittal Y, Toshniwal P, Sharma S, Singhal D, Gupta R, Mittal VK (2015) A voice-controlled multi-functional Smart Home Automation System. In: 2015 Annual IEEE India Conference (INDICON). IEEE, New Delhi, India, pp 1–6. <https://doi.org/10.1109/INDICON.2015.7443538>
15. Yuksekkaya B, Kayalar AA, Tosun MB, Ozcan MK, Alkar AZ (2006) A GSM, internet and speech controlled wireless interactive home automation system. *IEEE Trans Consumer Electron* 52:837–843. <https://doi.org/10.1109/TCE.2006.1706478>
16. Alheraish A (2004) Design and implementation of home automation system. *IEEE Trans Consumer Electron* 50:1087–1092. <https://doi.org/10.1109/TCE.2004.1362503>
17. Jakovljevic S, Subotic M, Papp I (2017) Realisation of a smart plug device based on Wi-Fi technology for use in home automation systems. In: 2017 IEEE International Conference on Consumer Electronics (ICCE), IEEE, Las Vegas, NV, USA, pp 327–328. <https://doi.org/10.1109/ICCE.2017.7889340>
18. A JC, Nagarajan R, Satheshkumar K, Ajithkumar N, Gopinath PA, Ranjithkumar S (2017) Intelligent smart home automation and security system using arduino and Wi-Fi. *IJECS*. Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Namakkal India. <https://doi.org/10.18535/ijeecs/v6i3.53>
19. Chaurasia T, Jain PK (2019) Enhanced smart home automation system based on internet of things. In: 2019 Third international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp 709–713. <https://doi.org/10.1109/I-SMAC47947.2019.9032685>
20. Saha R, Bera JN, Sarkar G (2018) An alternate approach for power quality computation using sample shifting technique towards load characterisation. *Measurement* 129:642–652. <https://doi.org/10.1016/j.measurement.2018.07.037>
21. Ghirardello K, Maple C, Ng D, Kearney P (2018) Cyber security of smart homes: development of a reference architecture for attack surface analysis. In: *Living in the internet of things: cybersecurity of the IoT—2018*. Institution of Engineering and Technology, London, UK, p 45 (10 pp)—45 (10pp). <https://doi.org/10.1049/cp.2018.0045>