Received: May '22
Revised:
Accepted: Jun '22



# A REAL-WORLD SCENARIO STUDY ON SOFTWARE MECHANISM TO IMPROVE THE SECURITY OF IOT AND ANDROID SOFTWARE FOR SMART HOME

**Vijay Kumar Meena**
Research Scholar, University of Technology, Jaipur

***ABSTRACT***

*Any device (so long as it has an on/off switch) might potentially become part of the Internet of Things. Entryway lock systems, which have replaced many traditional locks due to increased customer comfort and lower prices, are an essential part of any home security system. Security in the Internet of Things (IoT) refers to the protection of both individual devices and the networks that connect them; it influences the iterative improvements and preventative measures that must be taken to guarantee the safety of IoT infrastructure; and it was proposed that the application would learn from user actions to further tighten protections. User information, including the time and date of each lock access, will be stored on the server, where it may be analysed to predict when the user is likely to enter the home and adjust security measures accordingly. The control module in the house was utilised. As one of the most rapidly expanding sectors of the economy, home automation necessitates the development of a simple yet effective system that, with enough training, can predict the client's next move and carry it out on their own.*

**Keywords:** Innovative, Wireless, Communication, Technique, IOT.

## 1. INTRODUCTION

Any device (so long as it has an on/off switch) might potentially become part of the Internet of Things. A vast network of interconnected devices and people, the IoT collects and disseminates information about usage and the surrounding environment. Our suggested advanced smart house is a compound of the traditional smart home, the Internet of Things, cloud computing, and rule-based event management. Each component enhances and emphasises other aspects of the suggested framework with its own unique set of central characteristics. Internet of Things (IoT) supports internet association and remote administration of multipurpose equipment embedded with a wide range of sensors. Home appliances, such as air conditioners, lighting, and other environmental gadgets, might all benefit from having sensors installed. As a result, it integrates computer intelligence into domestic appliances to facilitate monitoring of environmental parameters and appliance performance. The most common type of home security system is a set of locks on the door. Many wireless network configurations, such as Bluetooth, ultra wide band (UWB), remote Ethernet, and many more, have a place with the realm of home networking, as they provide convenience and cost-effectiveness to consumers and allow for the replacement of traditional locks. Bluetooth, which allows for the creation of numerous types of remote frameworks via handsets or smartphones and also leads research by employing handset and actuator via remote operation of various electrical equipment in the home, has emerged as the most appealing method among these. Given Bluetooth's pervasiveness in mobile devices, it was thought to be a simple, inexpensive, and secure solution for connecting a mobile device to a fixed-location network at home.

### IoT security

Both the physical security of devices and the virtual security of networks are impacted by IoT security, which in turn affects the development cycles, technological advances, and precautions needed to guarantee the safety of IoT devices and networks. It includes things that aren't always designed with network security in mind, including as industrial machinery, smart energy grids, building automation systems, entertainment gadgets, and more. IoT device security should protect against a variety of IoT security threats, including those that aim to compromise the following four types of vulnerabilities: Communication attacks on the data transmitted between IoT devices and workers. Lifecycle attacks on the IoT gadget as it changes hands from client to maintenance. Attacks on the gadget software. IoT's primary difficulty is in resolving challenges that arise from connecting the

real world and the virtual one, such as how to deal with information gleaned from electronic hardware via an interface between users and devices. Essential needs for ensuring the functioning of the emerging IoT arrangement have emerged. The proliferation of security concerns has become an obstacle for the IoT infrastructure to overcome.

Since the initial proposal of the IoT concept in the late 1990s, security experts have voiced concerns about the risks posed by a large number of unreliable devices interacting with the Internet. Coding, perceptual, network, middleware, application, and business layers make up the SixLayer IoT Architecture. The Smart Home can use all of these levels, too.

### 1.1 Smart home development for home security based on android

Today, we refer to a city or village where Android-based apps are used in a rapidly expanding network as a "smart city" or "smart village," and to the tiniest extension of this concept as a "smart house." According to author Nicola King, a "smart house" is a residence equipped with a communications network that links together numerous departments and electronic devices and enables remote monitoring, access, and management. Along with the ever-increasing complexity of the network, the ever-increasing portability of technology, the ever-increasing frequency of extreme wrongdoing that exploits the situation and environmental conditions, the most common offence being wrongdoing of robbery and brutality in the home environment, the role of information technology, and smart home in particular, is expected to help provide security and comfort to the homeowner by way of a custom-built application that can monitor the state. By implementing the smarthome, homeowners want to monitor the property's condition from afar, giving residents advance notice of any impending dangers.

## 2. LITERATURE REVIEW

**Islam, Akib (2018)** This study's objective is to design and implement an affordable, malleable, and fantastic Internet of Things-based smart home automation framework through the use of applications.

Intruders, rising levels of toxic gases, smoke, and fire may all be detected using our framework, as can suspicious behaviour, which can be brought to the client's attention with an alert through pop-up message or instant messaging. We've designed our framework to be flexible enough to adapt to meet the evolving needs of our customers. Unlike the previous framework, ours does not have the problems of high ownership costs, stubbornness, ineffective management, difficulty obtaining security, or the inability to integrate other conventions, new methods, or improved tactics to provide better results. Using a variety of sensors placed at strategic locations around the home and subject to the simple to use android app's rules, the homeowner may monitor the temperature and humidity of the whole dwelling. Without modifying the existing home framework or architecture, our framework and application support the dynamic addition or removal of devices.

**Alaa, Musaab and Zaidan, A. and Bahaa, Bilal et. al (2017)** The new and troublesome invention of Internet of Things (IoT)-based smart home apps (hence referred to as apps) is generally limited and dispersed. Understanding the available options and limitations in this branch of research is important for providing useful insights about technical circumstances and bolstering researchers. So, a survey is conducted in this study to map the research environment and provide a reliable taxonomy. We actively searched Web of Science, ScienceDirect, and IEEE Explore to find every paper we could find on smart homes, applications, and the Internet of Things. Articles focusing on IoT-based smart-home applications may be found in these archives. The final dataset produced by the classification conspiracy has 229 items divided into four categories. The best content focuses on audit and overview papers for IoT applications for the smart home. The incompetent recalls IoT application papers and their use in smart home technology. Framework suggestions for making and running apps fall under the second category.

**P. Gupta and J. Chhabra (2016)** the In this paper, we present the design and implementation of an Ethernet-based Smart Home astute framework for monitoring electrical energy consumption based on real-time tracking of devices in the home using an INTEL GALILEO 2ND generation improvement board, which can be deployed in households and communities. The suggested framework reduces the need for real-time monitoring and voice control in favour of remote control and monitoring of electrical appliances and switches, with or without the use of an android-based app. It uses a number of sensors to keep your house safe and track your devices in real time. It is remotely monitored and managed using an Android app connected to either

the Internet or an internal network. The project's proposed outcome seeks to achieve multiple benefits, including lowering homeowners' electric bills, improving home security, allowing users to switch on and off connected devices with the sound of their voice or the touch of a button on their smartphones, and monitoring the consumption of precious natural resources in order to moderate it.

**Lin, Huichen and Bergmann, Neil (2016)** There is a tendency to see the Internet of Things (IoT) as a monolithic problem space, with the expectation that any solutions developed within may be used in any number of contexts. However, the privacy and security requirements of an indigenous Smart Home environment are quite different from those of vital designing infrastructure or sensitive business processes. The availability of resources (both financial and human) to implement security and privacy also varies widely among application areas. Human factors may be just as essential as technical ones under local situations. After examining current methods for bettering IoT security, the study identifies essential future conditions for trustworthy Smart Home systems. For low-resource devices and high-availability infrastructure, a gateway design is favoured. Two significant advances in aiding auto-management of frameworks are highlighted. Support for automatically configuring frameworks improves security immediately. As an added measure, it is intended that automated updates of framework software and firmware would ensure the framework's continued, secure functioning.

## 3. OBJECTIVES

- To study about Iot security and home security based on android.
- To study modules present in the system communicate for security.

## 4. RESEARCH METHODOLOGY

No spare keys will be needed for the suggested system, as with RFID tags, for instance. Fingerprint scanners, facial recognition software, personal identification numbers, and passwords are just a few of the many security techniques available today. The programme will monitor user actions to better tighten security. User information, including the time and date of each lock access, will be stored on the server, where it may be analysed to predict when the user is likely to enter the home and adjust security measures accordingly. Turning the key in the lock will immediately turn off any lights that were left on. When the door is opened, the lights automatically switch on. The customer may schedule time off, and the system will remain in a highly protected state until their return.

For domestic help or guests, the user can establish temporary keys (will be active for a given period).

### A. Control Module:

- **Android application:** The application gives and interfaces between the client and the lock and it is utilized to control the lock and the other segments of the system.
- **Server, DB:** The server is utilized to store the client activities and all the clients that are allowed to access the lock and store the authorized client's credentials, for example, login id or password.
- **Raspberry pi:** Raspberry pi is the central controlling unit and is utilized to communicate with and control all the segments utilized in the system.

### B. Door/Window Module:

- **Camera:** The camera is utilized to capture anyone accessing the lock and in case of a unidentified client the client is alerted about the same, the camera turns on just when there is somebody near the door or the windows.
- **Motor:** The motor is the gadget that controls the latch.
- **Fingerprint sensor:** Fingerprint sensor is utilized to authenticate the client and give a faster, secure and more productive way to open the door.
- **Motion sensor:** The motion sensors screen the activity before the door and near the windows the places that can be utilized to gain entrance in the house in case of development near these places the camera is activated to record the individual going into the house.

### C. House Module:

i. **Relay:** The relay module is a separate hardware gadget utilized for remote gadget switching. With it you can remotely control devices over a network or the Internet. Devices can be remotely fueled on or off with commands.

ii. **Smoke/gas sensor:** This sensor is utilized to check if there is a fire or a gas leakage in the house and alert the client and trigger the alarm if there is any.

iii. **Light sensor:** Light sensors check if the room needs artificial lighting when the client goes into the house if the room is dark and the client

goes into the house the lights turn on automatically.

**D. Alert Module:**

- **Alarm:** The alarm is utilized to alert the encompassing in case of a crisis, for example, fire, gas leakage or constrained section in the house.
- **GSM module:** The gsm module is a gadget that will have the option to send sms to the client it helps in alerting the client even without an internet association.

## 5. RESULT AND DISCUSSION

Each component of the system is interconnected with every other component to provide a seamless operation. Doors and windows are equipped with motion sensors that may detect movement in front of them, alerting the user if someone is approaching them. Likewise, if a break-in occurs and the motion sensors detect movement within the house, even if the lock was not entered, an alarm would ring. The authorised user has the option of using a fingerprint reader to unlock the door, or having the door automatically open when the user approaches with the authorised device, or even using facial recognition software. Other methods, such as entering a pin or password into a phone, are also possible, and can be prearranged by the user.

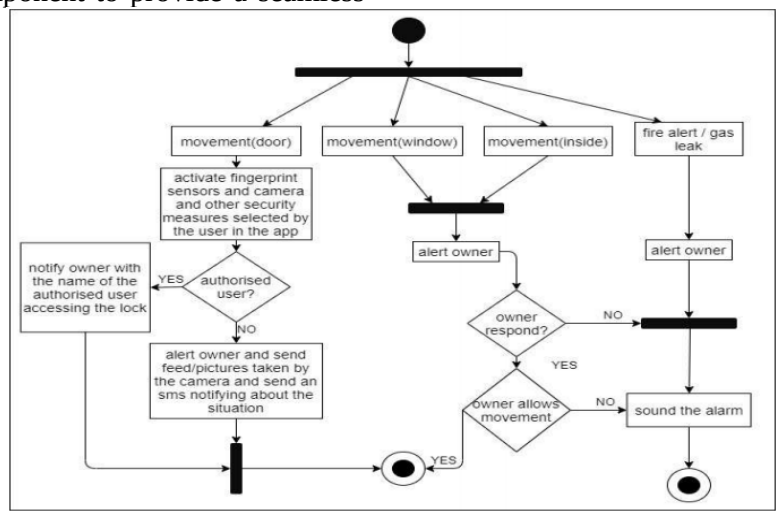


**Figure 1: Activity plan**

An alternative is for the owner to make a temporary key for the guest and add the guest's fingerprints to it; this key would be transitory since the owner would be able to determine how long the guest would be considered an approved client. After determining that it is sufficiently dark, the relay board will activate the lights through the raspberry pi. The mobile app monitors user activity, and if it detects any deviation from the norm (such as when a user fails to unlock their device), it ramps up security and notifies any other approved users. If a client is unable to get an app notice due to a lack of internet connection, the gsm module will send an SMS warning of the gas leak or fire to the client.

### 5.1 Software

The software in the proposed system comprises of a real time database which is firebase the lock is controlled by an android application along these lines the android operating system is needed by the client the improvement of the application requires JAVA, Python, XML and the operating system utilized in the Raspberry pi is Raspbian OS.

### 5.2 Hardware

The hardware necessity for the proposed system are as per the following: Servo motor to operate the lock , piCam to record and stream the happenings around the house, a fingerprint sensor that will help in client authentication a relay board to control the lights and fans ,Raspberry pi light sensor to recognize the degree of darkness a MQ2 smoke sensor to distinguish fire, Raspberry pi 3 acts as the control controlling unit and a GSM module to alert the client in case the client isn't associated with the internet.

## 6. CONCLUSION

A vast network of interconnected devices and people, the IoT collects and disseminates information about usage and the surrounding environment. As one of the most rapidly expanding sectors of the economy, home automation

necessitates the development of a simple yet effective system that, with enough training, can predict the client's next move and carry it out on their own. This study introduces a flexible and straightforward method of putting this into practise by using the integration of relays to Raspberry pi for remote control of household appliances. The suggested system has applications outside the confines of a single dwelling, such as the storage of automobiles, spare parts, and the like. The authors offer a generic framework for the Internet of Things (loT) that makes use of the cloud to manage connections to and data from remote devices and to store collected sensor information.

## REFERENCES


1. Alaa, Musaab & Zaidan, A. & Bahaa, Bilal & Talal, Mohammed & Mat Kiah, Miss Laiha. (2017). A Review of Smart Home Applications based on Internet of Things. Journal of Network and Computer Applications. 97. 10.1016/j.jnca.2017.08.017.
2. P. Gupta and J. Chhabra, "IoT based Smart Home design using power and security management," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 6-10, doi: 10.1109/ICICCS.2016.7542317.
3. Lin, Huichen & Bergmann, Neil. (2016). IoT Privacy and Security Challenges for Smart Home Environments. Information. 7. 44. 10.3390/info7030044.
4. Stergioua C, Psannis KE, Kimb B-G, Gupta B. Secure Integration of IoT and Cloud Computing. Elsevier, Future Generation Computer Systems, Vol. 78. Part 3. January 2018. pp. 964-975
5. Al-Kuwari M, Ramadan A, Ismael Y, Al-Sughair L, Gastli A, Benammar M. Smart-Home Automation Using IoT-Based Sensing and Monitoring Platform, IEEE. 2018.
6. Datta T, Apthorpe N, Feamster N. Developer-friendly library for smart home IoT privacy-preserving traffic obfuscation, IoT S&P 18. In: Proceedings of the 2018 Workshop on IoT Security and Privacy. ACM; 2018. pp. 43-48
7. Mao J, Lin Q, Bian J. Application of Learning Algorithms in Smart Home IoT System Security. American Institute of Mathematical Sciences; 2018.
8. Saeed F, Paul A, Rehman A, Hong WH, Seo H. IoT-based intelligent modeling of smart home environment for fire prevention and safety. Journal of Sensor and Actuator Networks. 2018;7(1):11.
9. Botta A, de Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: A survey. Future Generation Computer Systems. 2016;56:684-700
10. Soliman M, Abiodun T, Hamouda T, Zhou J, Lung C-H. Smart home: Integrating internet of things with web services and cloud computing. In: International Conference on Cloud Computing Technology and Science; IEEE. 2013
11. Islam, Akib. (2018). Android Application Based Smart Home Automation System Using Internet of Things. 10.1109/I2CT.2018.8529752.