Journal of Advances and Scholarly Researches in Allied Education
Vol. 18, Issue No. 2, March–2021, (Special Issue), ISSN 2230-7540

A Study on Software Mechanism to Enhance the Security of IOT and Android Software for Smart Home in Real World Scenario

Pankaj Khairnar*

Research Scholar, Mansarovar Global University, Sehore (MP)

Abstract – The Internet of Things is the idea of associating any gadget (inasmuch as it has an on/off change) to the Internet and to other associated devices. A safe home framework comprises of an entryway lock framework which has been perhaps the most popular purchaser devices replacing many of the conventional locks because of sheer client comfort and affordable costs. IoT security covers both physical gadget security and network security, and impacts the cycles, advancements, and measures necessary to ensure IoT devices and networks we proposed the application will learn from the client behavior and increase security accordingly. The details of the client accessing the lock will be put away in the server along with date and time which can be additionally used to foresee the occasions when the client will go into the house and handle security accordingly. We used House Module, control module. Home automation, being quite possibly the most integral parts of the sprouting realty industry paves forward the need to establish a basic yet productive system that through training anticipates the client's actions and executes it for them.

Keywords: Software, Enhance, Security, IoT, Android, Smart Home, etc.

----------X----------

1. INTRODUCTION

The Internet of Things is the idea of associating any gadget (inasmuch as it has an on/off change) to the Internet and to other associated devices. The IoT is a giant network of associated things and individuals all of which gather and share data about the way they are utilized and about the climate around them. Classic smart home, internet of things, cloud computing and rule-based occasion handling, are the building squares of our proposed advanced smart home integrated compound. Each segment contributes its center attributes and advancements to the proposed structure. IoT contributes the internet association and far off management of versatile appliances, incorporated with a variety of sensors. Sensors may be attached to home related appliances, for example, air-conditioning, lights and other environmental devices. And thus, it inserts computer insight into home devices to give ways to measure home conditions and screen home appliances' functionality. A safe home framework comprises of an entryway lock framework which has been perhaps the most popular Purchaser devices replacing many of the conventional locks because of sheer client comfort and affordable costs many remote network arrangements, for example, Bluetooth, ultra wide band (UWB), remote Ethernet and many more have a place with the area of home networking. From among these, Bluetooth has become the most attractive procedure in the research and commercial domain as Bluetooth enables to create various sort of remote frameworks via handsets or smartphones and also lead research by utilizing handset and actuator by distant operation of various electrical devices at home. Since Bluetooth is so prevalent in cell phones, it was viewed as a basic, economical and secure answer for remote network for associating a cell phone to home network framework.

√ **IoT security:** IoT security covers both physical gadget security and network security, and impacts the cycles, advancements, and measures necessary to ensure IoT devices and networks. It spans industrial machines, smart energy grids, building automation systems, entertainment devices, and more, including devices that often aren't intended for network security. IoT gadget security should ensure systems, networks, and data from a broad range of IoT security attacks, which target four sorts 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.

The main challenge in IoT is to overcome any issues between the physical world and the world of information, for example, how to handle data obtained from electronic hardware through an interface among clients and gear. The creating IoT arrange has approached with essential requirements for affecting it to make sure about. A ton of security issues has transformed into a challenge for the IoT organize. Security specialists have warned of the potential danger of large quantities of unstable devices interfacing with the Internet since the IoT idea was first to propose in the late 1990s. There are SixLayer IoT Architecture that is a coding layer, perception layer, network layer, a middleware layer, application layer, and business layer. These all layers also can apply in the Smart Home.

1.1 Smart home development for home security based on android

Improvement of Android-based applications that applied in the fast-developing network began a broad level today we know as a smart city or smart village and the smallest extension we realize the term called a smart-home. Nicola King characterizes smart-home as an asylum outfitted with a communications network that associates various administrations and electronic gear and allows it to be observed, accessed and controlled remotely. Along with the increasingly perplexing existence of the network, increased portability, increasingly more extreme wrongdoing popping up by abusing the situation and environmental conditions, the most regular offense is wrongdoing of robbery and brutality in the home climate the part of the information innovation especially smart home is relied upon to help give security and solace to the homeowner built up a smart-home application that can screen the state of the house when the house is in its proprietor's home. Expected by the application of the smarthome the homeowners can screen the state of the house remotely and allowing occupants to get a warning.

2. LITERATURE REVIEW

Islam, Akib (2018) the aim of this research paper is to plan and actualize a financially savvy and yet adaptable and incredible application based smart home automation framework utilizing the Internet of Things. Our framework is intended to recognize burglary, increase in the concentration of harmful gasses, smoke and fire flames, discovery of dubious activities and illuminating the client through instant message or pop-up message. Our framework is planned so that it can arrange itself dynamically based on the change in necessities of the client. Our framework eliminates the greater part of the drawbacks in the past framework, for example, significant expense of proprietorship, resoluteness, helpless manageability, and trouble in achieving security, lack of integration of various conventions utilizing new techniques or improving the current strategies to achieve better outcomes. The whole home climate can be observed by various sensors sent all over the home and constrained by the easy to understand android application. Our framework and application uphold dynamic addition or removal of devices without changing the home framework or architecture.

Alaa, Musaab and Zaidan, A. and Bahaa, Bilal et. al (2017) the new and problematic innovation of smart home applications (hereafter alluded to as apps) based on Internet of Things (IoT) is largely restricted and scattered. To give valuable experiences into technological conditions and backing researchers, we should understand the available alternatives and gaps in this line of research. Hence, in this examination, a survey is led to map the research landscape into a sound taxonomy. We lead an engaged search for each article related to (1) smart homes, (2) apps, and (3) IoT in three major databases, namely, Web of Science, ScienceDirect, and IEEE Explore. These databases contain literature zeroing in on smart home apps utilizing IoT. The final dataset coming about because of the classification conspire incorporates 229 articles separated into four classes. The top notch involves audit and overview articles related to smart home IoT applications. The inferior remembers papers for IoT applications and their utilization in smart home innovation. The second rate class contains proposals of frameworks to create and operate applications.

P. Gupta and J. Chhabra (2016) the paper presents the plan and implementation of an Ethernet-based Smart Home astute framework for checking the electrical energy utilization based upon the real time tracking of the devices at home an INTEL GALILEO 2ND generation improvement board, which can be utilized in homes and social orders. The proposed framework chips away at real time observing and voice control, so the electrical devices and switches can be distantly controlled and checked with or without an android based app. It utilizes various sensors to screen the real time gadget tracking as well as maintaining the security of your home. It is observed and controlled distantly from an android app utilizing the Internet or the Intranet network. The proposed result of the venture aims as different advantages of saving on power bills of the home as well as keep the clients updated about their home security with an alternative of controlling the exchanging of the devices by utilizing their voice or straightforward switch address their smartphone, and last however most importantly, screen the usage to moderate the valuable natural assets by decreasing electrical energy utilization.

Lin, Huichen and Bergmann, Neil (2016) Often the Internet of Things (IoT) is considered as a solitary issue domain, with proposed arrangements planned to be applied across a wide range of applications. Notwithstanding, the privacy and security needs of critical designing infrastructure or touchy commercial operations are totally different to the requirements of a homegrown Smart Home climate. Additionally, the financial and human assets available to execute security and privacy vary greatly between application domains. In homegrown conditions, human issues may be as important as technical issues. After reviewing existing answers for enhancing IoT security, the paper recognizes key future prerequisites for confided in Smart Home systems. Gateway architecture is chosen as the most appropriate for asset constrained devices, and for high framework availability. Two key innovations to assist framework auto-management are distinguished. Right off the bat, uphold for framework auto-configuration will enhance framework security. Also, the automatic update of framework software and firmware is expected to maintain continuous secure framework operation.

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

The proposed system is keyless that is we won't have an extra key, for example, the RFID tags. There are various mechanisms of security, for example, fingerprint scan, facial recognition, pin, and password. The application will learn from the client behavior and increase security accordingly. The details of the client accessing the lock will be put away in the server along with date and time which can be additionally used to foresee the occasions when the client will go into the house and handle security accordingly. On locking the door, the lights that are on will automatically kill. On opening the door the lights turn on accordingly. Client can set vacation days and the system will be on maximum security till the client returns User can also set temporary keys (will be active for a set time) for homegrown assistance or for visitors.

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

All the modules present in the system communicate with each other to give smooth working of the system. The doors and the windows have motion sensors that can detect development before them in case somebody approaches the doors or the windows the client is alerted and in the event that somebody breaks in and the motion sensors recognize development inside the house despite the fact that the lock was not accessed the alarm is sounded. The client can open the door utilizing the fingerprint sensor or if the client wants the door will open itself when the client draws close to the door with the authorized gadget or can utilize the face open there are different strategies for opening the door, for example, utilizing a pin or a password that can be entered in the telephone, can be arrangement by the authorized client and could keep more than one way to authenticate an individual going into the house.

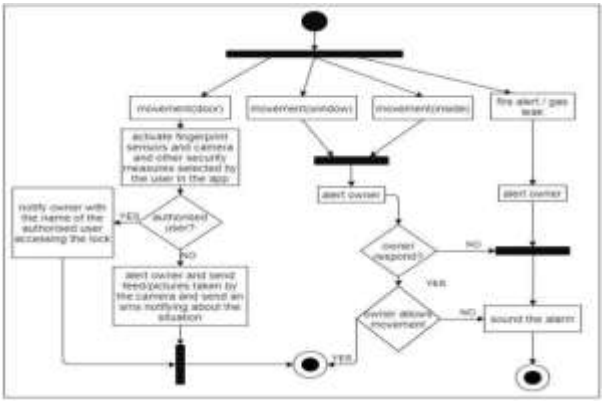

Figure 1: Activity plan

The owner can also create temporary keys for the visitor and add their fingerprints too this key is temporary as the proprietor can set the time till which the visitor will be an authorized client. The light sensors check the light power in the room and in the event that it is dark the raspberry pi will turn on the lights utilizing the relay board. The portable application tracks the client behavior and in case of an alternate behavior then the client usually shows the lock increases the security measures and also alerts the other authorized clients. In case of a gas leakage or fire the alarm is sounded in order to alert the environmental factors the gsm module alerts the client via a SMS in case the client fails to get any app notification because of lack of internet association.

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

The IoT is a giant network of associated things and individuals all of which gather and share data about the way they are utilized and about the climate around them. Home automation, being quite possibly the most integral parts of the sprouting realty industry paves forward the need to establish a basic yet productive system that through training anticipates the client's actions and executes it for them. This paper presents an adaptable and easy to understand technique to actualize the same by integrating relays to Raspberry pi for controlling home appliances from a remote location in a real scenario. The proposed system can be utilized in different scenarios like parking parts, cars, and so forth, apart from one's home. As an expansion, authors propose a non-exclusive IoT framework and use cloud computing infrastructure for interfacing and managing remote devices and also store sensor data.

REFERENCES

1. Islam, Akib. (2018). Android Application Based Smart Home Automation System Using Internet of Things. 10.1109/I2CT.2018.8529752.

2. 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.

3. P. Gupta and J. Chhabra (2016). “IoT based Smart Home design using power and security management,” 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, pp. 6-10, doi: 10.1109/ICICCS.2016.7542317.

4. Lin, Huichen & Bergmann, Neil. (2016). IoT Privacy and Security Challenges for Smart

Home Environments. Information. 7. 44. 10.3390/info7030044.

5. Stergioua C, Psannis KE, Kimb B-G, Gupta B. (2018). Secure Integration of IoT and Cloud Computing. Elsevier, Future Generation Computer Systems, Vol. 78. Part 3, pp. 964-975

6. Al-Kuwari M, Ramadan A, Ismael Y, Al-Sughair L, Gastli A, Benammar M. (2018). Smart-Home Automation Using IoT-Based Sensing and Monitoring Platform, IEEE.

7. Datta T, Apthorpe N, Feamster N. (2018). 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; pp. 43-48

8. Mao J, Lin Q, Bian J. (2018). Application of Learning Algorithms in Smart Home IoT System Security. American Institute of Mathematical Sciences.

9. Saeed F, Paul A, Rehman A, Hong WH, Seo H. (2018). IoT-based intelligent modeling of smart home environment for fire prevention and safety. Journal of Sensor and Actuator Networks; 7(1):11.

10. Botta A, de Donato W, Persico V, Pescapé A. (2016). Integration of cloud computing and internet of things: A survey. Future Generation Computer Systems; 56: pp. 684-700

11. Soliman M, Abiodun T, Hamouda T, Zhou J, Lung C-H. (2013). Smart home: Integrating internet of things with web services and cloud computing. In: International Conference on Cloud Computing Technology and Science; IEEE.

Corresponding Author

Pankaj Khairnar*

Research Scholar, Mansarovar Global University, Sehore (MP)