

Smart Home Security Augmentation

Naman Phadnis, S.S. Sanjay Krishnan, Sourabh Kumar Mishra, R. Sujeetha

Abstract: *In this project based on Smart Home Security, we make the home homelier by connecting members of a residence to it by creating a network between the residents and the home. Using the concept of internet of things and networking, we make sure that the people not only lead a more comfortable life, but a more secure one as well. In this paper we take the concept of smart home systems and add additional security features to the concept to make living safe and secure along with comfortable and cozy. Using Arduino and Raspberry Pi, our system alerts the user when an unknown person is detected within the household so that they can take the required steps needed in case it is an unwanted intruder. In the modern, fast paced world we live in, where security threats grow in large numbers each day, the need for home security increases with the same intensity. A smarter, more efficient and a more convenient approach towards home security ensures an increase in the number of people having access to such systems as well as makes sure of a decrease in the number of people having difficulty with confusing and complex security interfaces. This project turns your mundane everyday object into defenders of your home, eliminating the need to bring in any other expensive security devices. Additionally, it also lets you keep a track of your entire household objects in one place.*

Index Terms: Smart Home, IOT, Security, Arduino

I. INTRODUCTION

Home automation can be defined as using modern technology to computerize day to day household objects. The variety of home automation can vary from a simple light turning on and off to advanced smart locking systems. It is adopted in order to save energy, minimize human effort and make living in a house more convenient. Our paper talks about how we can make the best of this growing technology by the addition of security features, as well as a convenient and easy to use smart home system. People are certainly aware of the need to conserve energy but do very little on their end in order to save it.

It gives you access to control gadgets in your home from a cell phone anywhere on the planet. The term might be utilized for disconnected programmable gadgets, similar to indoor regulators and sprinkler frameworks, yet home mechanization all the more precisely portrays homes in which about everything — lights, apparatuses, electrical outlets, warming and cooling frameworks — are snared to a

remotely controllable system. From a home security point of view, this additionally incorporates your alert framework, and the majority of the entryways, windows, locks, smoke indicators, CCTV and whatever other sensors that are connected to it. Home automation stretches out that planned programmability to lighting, so you can suit your power consumption to your typical day by day plan. With progressively adaptable home mechanization frameworks, electrical outlets or even individual gadgets can likewise be naturally shut down amid hours of the day when they're not required. Similarly as with secluded gadgets like indoor regulators and sprinkles, the planning can be additionally separated to recognize ends of the week and even periods of the year, now and again.

II. LITERATURE SURVEY

“Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids”, This paper focuses on the implementation of metering system in smart grids to make smart home systems more efficient and secure. Smart meters are capable of recording energy at least every hour, and can send reports based on that every two days. They can establish a communication between meter and central system with works both ways. This is known as AMI or Advanced Metering Infrastructure and is quite different from AMR or Automatic Meter Reading, establishes a two way communication between meter and supplier. Communication between meter and network may either be wired or wireless. Wireless communication options in common use include cellular communications (which can be expensive), Wi-Fi (readily available), wireless ad hoc networks over Wi-Fi, wireless mesh networks, low power long range wireless, ZigBee and Wi-SUN Smart meters will enable you to monitor your consumption more precisely so you can make more informed energy choices, however during emergency, network congestion or performance are big challenges in smart grid system.

“Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures”, This paper's prime focus is to discuss about a smart system which indicates threats to the electrical smart grid through which smart home systems are implemented and tries to fix them. If any unwanted or unrecognized change occurs in the smart grid, this system can be used to inform the user or even be designed to deal with the security issue on its own. Not only it facilitates real-time troubleshooting, and also equips the grid to meet increasing demand. The only disadvantage it faces is that some smart meters can be hacked by advanced hackers which can be used to increase or decrease the demand for power and facilitate wrong information without the system being aware of it.

Manuscript published on 30 April 2019.

* Correspondence Author (s)

Naman Phadnis, CSE, SRM Institute of Science and Technology, Chennai, India.

S.S. Sanjay Krishnan, CSE, SRM Institute of Science and Technology, Chennai, India.

Sourabh Kumar Mishra, CSE, SRM Institute of Science and Technology, Chennai, India.

R. Sujeetha, CSE, SRM Institute of Science and Technology, Chennai, India.

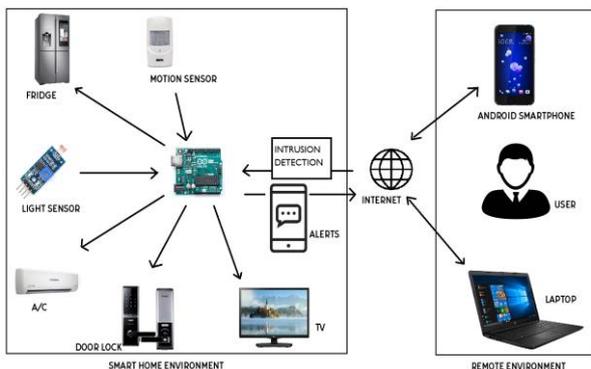
© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

“Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments”, This paper uses the concepts of sessions and keys to deny unwanted intruders any access to a smart home environment. A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers. The concept of session keys is used in this paper, which are also known as symmetric keys as for both encryption and decryption, same key is used. In each session, each message along with encryption contains its own unique key along with the recipient’s unique key. Such approach shows too much dependency on session keys, and therefore, they are changed frequently.

“Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home”, Implementing fingerprint security in smart home devices to make the system more secure. Biometrics security like the fingerprint authentication is not only more convenient but more secure as well. As a result, the market value for fingerprint sensors is constantly on the rise. Fingerprint sensors come in different variations depending on the devices they are being used on. The only drawback to fingerprint sensing is it needs to be built with caution, as security issues will arise in a fingerprint sensor which does not work perfectly.

“Internet of Things Based Energy Aware Smart Home Control System”, Smart System built to implement energy consumption by factoring sunlight, usage time and connected using ZigBee networking. Smart homes offer enhanced energy-efficiency. This system provides automation to the light and thermostat system of the house, turning them on and off and varying the temperature depending on the current amount of present lighting and the current temperature. Implementations of automation of sensors can help in saving various resources such as light, water, energy etc.

III. ARCHITECTURE DIAGRAM



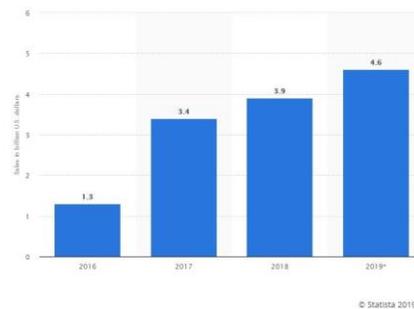
Our proposed system analyzes all aspects and solutions provided by each of the papers we studied in literature survey and uses that information in the development of a self secure, smart home security system which not only provides all the essential features of a smart home, but is secure in itself and provides additional security to your home as well. This eliminates the need of having any extra, separate security systems, boosting your finances.

As the architecture diagram above shows, an Arduino chip provides the primary functions for the whole system. Both the light sensor and the motion sensor send data to the Arduino about the current amount of light and movement

within the house. The household items are also connected to the network and data is sent to them through the chip. The Arduino processes all this data, determines the appropriate action through the algorithm. It then turns on or turns off light depending on the presence of a person and the amount of light present in a room. It automatically turns off lights when lights are on and there is no presence in a room. It can also turn other devices connected to it on and off. Moreover, it sends security alerts to the user if movement is noticed inside the house but it is not of the members of the house.

All this information is shared with the user by the Arduino through the internet and into the end devices of the user. Similarly, the user can access other devices through Arduino via the internet and the interface. The end devices can either be a person’s phone or laptop or both, depending on the final configuration of the system proposed.

Smart home devices sales in the United States from 2016 to 2019 (in billion U.S. dollars)



The above graph represents the Smart home devices sales in USA from 2016 to 2019, acquired from the data collected by Statista. As seen from the statistics, the demand for Smart home devices is ever increasing. With this increasing demand, we shall see a huge number of smart home devices of all kinds in the future, and with a large amount of systems in the market, an enhanced and optimal smart home device which provides security to the house as well tends to beat other devices out there.

The proposed system consists of four basic modules, namely Notification Module, Smart Home module, Sensor Module and Security Module.

The Notification Module looks over the complete alert system and the interaction of devices with the user. It sends alerts to the user in case of a security breach, gives user status about the devices connected to the smart home system, and lets the user know the information provided by the sensors.

The Smart Home Module lets the user access all the devices and the lighting of the house connected to the smart home system.

The Sensor Module is the primary module of the system. It lets the sensors present the information collected to the Arduino module, which processes it and takes appropriate automatic action, when its in the passive state, else it notifies the user through the notification module, and then the appropriate action can be taken by the user. The Security Module is semi-related to the sensor module, but its primary function is security, both in system as well as through the system.

An intrusion system prevents non authorized people from attacking the system, and another intrusion system lets the user protect the house from unwanted intruders.

IV. ALGORITHM

```

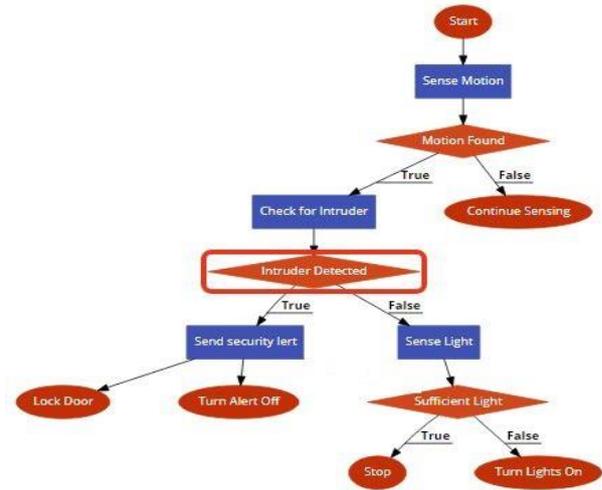
Sense Motion;
if(Motion Found) {
  Check for Intruder;
  if (Intruder Detected)
  {
    Send security lert;
    If (intruder_confirmed)
    {
      Lock Door;
    }
    Else if (false_alarm)
    {
      Turn Alert Off;
    }
  }
  else
  Sense Light;
  if (Sufficient Light)
  {
    Stop;
  }
  else
  {
    Turn Lights On;
  }
}
else
  Continue Sensing;

```

The primary algorithm of the system describes the activities that the system performs when it is in its Passive State, i.e. not being accessed by the user. It is constantly sensing both motion and light throughout the house.

If no motion is detected, the motion sensor continues to sense motion. If motion is detected by the motion sensor, it sends the signals to Arduino, confirming the motion. This information is then sent to the security system, which detects whether the motion present is of an intruder or not. If not, which means there is motion but of a household member, the system senses light in the room where motion is detected. If light in that room is already sufficient without the lights being on, then it does nothing and continues to sense. However, if a person is in that room but the amount of light is insufficient, lights are turned on.

If the motion detected is of an intruder, the user may choose either to lock the door if the door has smart locking system, take necessary action, or turn the security alert off in case the unknown movement is acknowledged and confirmed as a non-threat by the user.



V. CONCLUSION AND FUTURE ENHANCEMENT

Putting everything together, the Smart Home Security Augmentation provided by the proposed system lets the user take control of everyday household objects in their hands by connecting everything to a common network in a secure manner, saves energy by turning lights off without presence and turning them on in a dark room automatically, as well as provides additional security to the house which is integrated inside the smart home system itself.

As of now, the security system of the house is a proposed concept. In the future, we plan on developing the security system of this smart home system further by adding a check-in feature, which will make it easier to detect intruders. Any member of the house may check in the house when the family is inside, indicating to the smart home system that the people are inside the house. When locking the house and leaving with no one left in the house, the family may check out of the house, making the security system turn on the intrusion detection feature. Any movement detected after that inside the house will be counted as intrusion detection and a security alert will be sent to the user.

REFERENCES

1. Vinod Nambodiri, Visvakumar Aravinthan, Surya Narayan Mohapatra, Babak Karimi . Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids. IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2, JUNE 2014.
2. Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014.
3. Pardeep Kumar, Andrei Gurtov, Jari Iinatti, Mika Ylianttila, and Mangal Sain. Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments. IEEE SENSORS JOURNAL, VOL. 16, NO. 1, JANUARY 1, 2016.
4. Arun Cyril Jose , Reza Malekian, and Ning Ye. Improving Home Automation Security; Integrating Device Fingerprinting Into Smart Home. Received August 5, 2016, accepted August 29, 2016, date of publication September 8, 2016, date of current version October 6, 2016.
5. Murad Khan, Bhagya Nathali Silva, and Kijun Han. Internet of Things Based Energy Aware Smart Home Control System. Received October 5, 2016, accepted October 19, 2016, date of publication October 31, 2016, date of current version November 18, 2016.