IOT Based Theft Detection

*Mr. Vikrant A. Agaskar
ME Computer Student, Mumbai University
ALAMURI RATNAMALA INSTITUTE OF ENGINEERING AND TECHNOLOGY A.S.
RAO NAGAR, VILL-SAPGAON, TAL-SHAHAPUR DIST-THANE, PIN: 421601

Abstract—In this proposed system, theft can be prevented using Raspberry pi and PIR sensors. In this system PIR sensors, camera, buzzer, relay, GSM module are connected to Raspberry pi. PIR sensors are able to detect the presence of human being. After detecting any person, relays are triggered to switch on the lights. As soon as lights are on, buzzer will start ringing for specified time. After lights are turned on an image will be captured using cameras. This captured image will immediately upload on the web-page, which can be used as evidence. In addition, victim receives a notification in the form of text message with help of GSM module. Power supply to this system is given by an adapter. In absence of electricity battery backup is also provided. As the lights turn on and the buzzer rings, neighborhood becomes aware about a theft. This will make the thief scared and thief would try to escape the location. Thief is not able to execute his/her plan, belongings will be safe. This system can be implemented in jewelry shops, home etc.

I. INTRODUCTION

Today security and safety is just a click of the appropriate technology away, and with such advancements happening, the security of ones home must also not be left behind. Modern advances in electronics and communications technologies have led to the miniaturization and improvement of the performance of computers, sensors and networking. These changes have given rise to the development of several home automation technologies and systems. Automated home is the combination of home security and surveillance system. Surveillance can be defined as monitoring of the behavior, other changing information, activities, observing or analyzing particular area for the purpose of influencing, directing, managing or protecting. A home security system should provide security and safety features for a home by alarming the residents from natural, accidental and/or human dangers such as: fire, flooding, theft, animals invading, etc. Many of the home automation systems that are commercially available can be classified into two categories: locally controlled systems and remotely controlled systems. Locally controlled systems use an in-home controller to achieve home automation. This allows users complete use of their automation system from within their home via a stationary or wireless interface. Home automation systems using Bluetooth and Zigbee also come under this category. These have limitation of limited access range. Remotely controlled systems use an Internet connection or integration with an existing home security system to allow the user complete control of their system from their mobile device, personal computer, or via telephone from their home security provider. Associating mobile devices such as PDAs and Smart phones with the automation system gets easier in wireless networks. There are a number of issues involved when designing a home automation system. Cloud networking and data infrastructure allow individuals to monitor, manage, and control their personal data points through the Internet. This paper presents the implementation details of the home security system using a public cloud server to detect an intruder at home when nobody is present. This system uses an ARM7 microcontroller and is divided in two sections: viz. Inhome system and Remote user access. As soon as the intruder is in, Infrared (IR) and Pyroelectric Infrared (PIR) sensors detect the intrusion, and report intrusion events to the user by using GSM modem. The installed android mobile IP webcam helps the user to monitor the intrusion from anywhere, on an Internet enabled device by using the IP address of IP webcam and can also use login id and password for authentication.

II. LITERATURE REVIEW

With embedded systems fast expanding its reach, subject matter related to this field is available in abundance. While working on this project we have studied matter from various sources such as books, online articles, and reference manuals. The knowledge gained from this activity has been of great help to us in understanding the basic concepts related to our project and has ignited further interest in this topic. Linux for Embedded and Real Time Applications, by Doug Abbott has been of great help in providing an introduction to the process of building embedded systems in Linux. It has helped us understand the process of configuring and building the Linux kernel and installing tool chains. We understood the preponderance of the ARM processors in the field of embedded systems and the features of ARM processors from the document The ARM Architecture by Leonid Ryzhyk. The ARM architecture is a confluence of many useful features that make it better than other peer processors. Being small in size and requiring less power, they prove useful in providing an efficient performance in embedded applications

III. RELATED STUDIES

Modern security system should be able to identify a housebreaker attempting to enter the home. After this notifying the victim about the invasion or any illegal activity. Also system should be able to prevent the housebreaker from entering the home as well as capturing/collecting proofs about invasion. Technology is changing day by day making the

home security systems more powerful. It has changed from a simple lock and key security concept to implementing sophisticated security systems using cameras, microphones, contact sensors, proximity sensors, alarms, silent alarms, etc. The best feature about todays modern security systems is that, one can control their home devices just by using Internet. In some security systems, IR sensors are used to sense the presence of a human (housebreaker). Then it notifies the homeowner about the illegal activity or theft and buzzer starts ringing. The notification to user is send by Bluetooth or SMS. The user becomes aware of intrusion by receiving notification. Also people in the neighborhood will become alert of the theft because of alarm. The homeowner can take appropriate action after this. An infrared sensor is an electronic instrument which is used to sense certain characteristics of its surroundings by emitting and/or detecting infrared radiation. Infrared sensors are also capable of measuring the heat being emitted by an object and detecting motion. IR sensors need to have direct line of sight between transmitter and receiver because it does not work through walls or doors. They must be almost directly aligned (i.e. able to see each other) to communicate. They are blocked by common materials such as people, walls, plants, etc. Due to short range performance drops off with longer distance. They are affected by environmental conditions like direct sunlight, rain, fog, dust and pollution. Data transmission rate is lower than wired transmission. Bluetooth is wireless LAN technology which is designed to connect devices with different functionality for example telephone, notebook, computer (desktop, laptop), camera, printer when these devices are at short distance from each other. It is a ad-hoc network that is formed spontaneously. Maximum communication range of Bluetooth is 100m in any ideal conditions. But that is not sufficient for home environment. Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced. Bluetooth technology has advanced and improved to Bluetooth Low Energy (BTLE), which provides the same range of communication. However, it has serious security concerns such as eavesdropping and weak encryption. Hence Bluetooth becomes unreliable for sending notification to homeowner. The security systems which use Bluetooth and IR sensor have some limitations. IR sensors can sense anything passing through it which may a living or nonliving thing. After sensing any object it notifies homeowner as well as rings the alarm. This creates problem for the user as well as the people in the neighborhood. This becomes problematic and tedious because whenever alarm rings the nearby people will reach that location for checking if there is something wrong. Also the user who is far away from that location will return back because he has received notification about invasion. This will happen every time even if any object is detected. It will be better approach if PIR sensors are used. The PIR Sensors can detect the Infrared Rays released by human body. The light or any other electrical appliance can be activated automatically by the active presence of a human body within the detection range or coverage area when there

is no presence the light will be deactivated automatically. Even if any object comes in its range it will not detect because it is only programmed to detect those bodies that radiates the heat. So the advantage of PIR sensor is that it will detects only living things. This feature is very beneficial in the security systems. Consider a scenario where the homeowner is out of station for 4-5 days, and if any intruder tries to invade the home. In that case proposed system uses PIR sensors for detecting human presence. If any human presence is detected it will turn the lights ON with the help of relay and the buzzers stats ringing. Camera is used to capture the image of intruder immediately after the lights are turn ON. Homeowner will be notified about the intrusion through SMS. The captured image will be uploaded on a web page as evidence or proof about the intrusion. This system is more efficient and feasible because the user as well as the neighborhood will get aware about this illegal activity. The homeowner will have image as evidence of intruder to take appropriate action. The theft is prevented because after the lights are turned on and the ringing of alarm will make the intruder unsuccessful in executing his plan. The intruder would escape the location and the theft is prevented. This system focuses on the security aspect of the existing home automation system and points out its flaws. It shows how the concept of security and meaning of the word intruder has changed in modern homes. The paper points out the shortcomings of existing home automation systems in identifying and preventing sophisticated intruders in a home environment. For future work in the field of home automation security, effort is to encourage the researchers to consider a home automation system as a whole and develop behavior prediction and advanced sensing parameters that can help to identify and prevent skilled and sophisticated intruders. Security is vital for the proper implementation and development of the home automation systems. Moreover, it provides a sense of security to a homes inhabitants and puts their minds at ease.

IV. COMPONENTS OF PROPOSED SYSTEM

A. Raspberry Pi:

The Raspberry Pi is a series of small single-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote the teaching of basic computer science in schools and in developing countries. The original model became far more popular than anticipated, selling outside its target market for uses such as robotics. It does not include peripherals (such as keyboards, mice and cases). However, some accessories have been included in several official and unofficial bundles.

According to the Raspberry Pi Foundation, over 5 million Raspberry Pis were sold by February 2015, making it the best-selling British computer. By November 2016 they had sold 11 million units, and 12.5m by March 2017, making it the third best-selling "general purpose computer". In July 2017, sales reached nearly 15 million. In March 2018, sales reached 19 million.

B. PIR Sensor:

A passive infrared sensor (PIR sensor) is an electronic sensor that measures infrared (IR) radiation being emitted from objects in its field of view. They are most often used in PIR-based motion detectors. All objects with a temperature above absolute zero emit heat energy in the form of radiation. Usually this radiation isn't visible to the human eye because it radiates at infrared wavelengths, but it can be detected by electronic devices designed for such a purpose.

The term passive in this instance refers to the fact that PIR devices do not generate or radiate energy for detection purposes. They work entirely by detecting infrared radiation emitted by or reflected from objects. They do not detect or measure "heat".

C. Relay:

A relay is an electrically operated switch. Many relays use an electromagnet to mechanically operate a switch, but other operating principles are also used, such as solid-state relays. Relays are used where it is necessary to control a circuit by a separate low-power signal, or where several circuits must be controlled by one signal. The first relays were used in long distance telegraph circuits as amplifiers: they repeated the signal coming in from one circuit and re-transmitted it on another circuit. Relays were used extensively in telephone exchanges and early computers to perform logical operations.

A type of relay that can handle the high power required to directly control an electric motor or other loads is called a contactor. Solid-state relays control power circuits with no moving parts, instead using a semiconductor device to perform switching. Relays with calibrated operating characteristics and sometimes multiple operating coils are used to protect electrical circuits from overload or faults; in modern electric power systems these functions are performed by digital instruments still called "protective relays".

D. GSM SIM:

GSM (Global System for Mobile Communications, originally Groupe Spcial Mobile) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation digital cellular networks used by mobile devices such as tablets, first deployed in Finland in December 1991.

2G networks developed as a replacement for first generation (1G) analog cellular networks, and the GSM standard originally described as a digital, circuit-switched network optimized for full duplex voice telephony. This expanded over time to include data communications, first by circuit-switched transport, then by packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution, or EGPRS).

V. ARCHITECTURAL FLOW

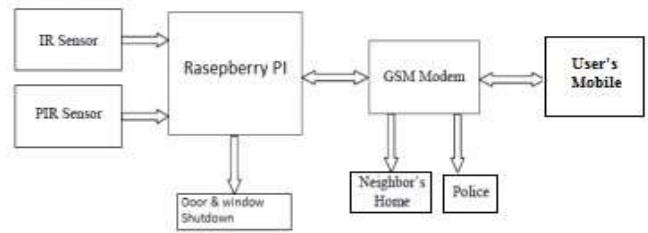The following figure shows the block diagram of the system.

Fig. 1 System Architecture

The following figure shows the Architectural flow of the system. Using this algorithm, a system can be created to prevent theft.

Fig.3 Installation Process

VI. CONCLUSION

We have designed and implemented a cost effective Raspberry PI based home security system. The proposed system provides home security and surveillance. Deploying sensors, GSM and android mobile IP webcam helps to detect, report and monitor intrusion events to users. Also the system informs to the neighborhood and alerts police, thereby reducing damages caused by burglary. The use of cloud network in the system allows for storage of captured images and recorded videos. Multiple PIR sensors may be used to obtain wider coverage. By integrating multi-touch mobile devices, cloud networking, wireless communication, and power-line communication, a fully functional home automation system can be designed and built.

VII. FUTURE SCOPE

This final section of the report outlines some features that could potentially be implemented in future releases. The current set of features implement is a minimum to what a consumer would expect. In future, we can store the images with help database and we can also increase the processing speed with help of advanced board.

REFERENCES

[1] Ashwini Patil, Shobha Mondhe, Tejashri Ahire, Gayatri Sonar Department Of Computer, Late. G.N. Sapkal College of Engineering, Nashik, Maharashtra, India., "AUTO-THEFT DETECTION USING RASPBERRY PI AND ANDROID APP"

[2] Umera Anjum, B. Babu, Avanthi Institute of Engineering Technology, "IOT Based Theft Detection using Raspberry Pi"

[3] Data sheets and the user manuals of ARM controller.