**Chapter - 1**

*Introduction:*

IoT or Internet Things refers to the network of connected physical objects that can communicate and exchange data among themselves without the need of any human intervention.[1] It has been formally defined as an “Infrastructure of Information Society”, because IoT allows us to collect information from all kind of mediums such as humans, animals, vehicles, kitchen appliances. Thus any object in the physical world which can be provided with an IP address to enable data transmission over a network can be made part of IoT system by embedding them with electronic hardware such as sensors, software and networking gear. IoT is different than Internet as in a way it transcends Internet connectivity by enabling everyday objects that uses embedded circuits to interact and communicate with each other utilizing the current Internet infrastructure. The term IoT and its conception can be traced back to 1985 when Peter T Lewis spoke about the concept during his speech at the Federal Communications Commission (FCC). Since then the scope of IoT has grown tremendously as currently it consists of more than 12 billion connected devices and according to the experts it will increase to 50 billion by the end of 2020. The IoT infrastructure has helped by providing real time information gathering and analysis using accurate sensors and seamless connectivity, which help in making efficient decisions. With the advent of IoT both manufacturers and consumers have benefited. Manufacturers have gained insight into how their products are used and how they perform out in the real world and increase their revenues by providing value added services which enhances and elongates the lifecycle of their products or services. Consumers on the other hand have the ability to integrate and control more than one devices for a more customized and improved user experience.

An important factor to consider when we talk about home automation is Security. Home security is a very important feature of home automation and maybe the most crucial one. Home security made a drastic changes in the past few decades and continue to advance much more in the coming years. Previously home security systems meant having an alarm that would go off when somebody would break in but a smart secure home can do much more than that. Therefore the main objective of our work is to design a system which can alert the owner and others of an intruder break-in by sending a notification to their smartphones. The owner will also have the ability to stop or start the alarm remotely using just his smartphone. This system will help the users to safeguard their homes by placing the system on the doors or windows and monitoring the activity through their smartphones.

There has been an unprecedented growth in the number of devices being connected to the Internet since past few years. All these devices connected to the internet are part of the IoT infrastructure which can that allows these devices to send and receive data among each other. This is why it is beneficial to use such an existing infrastructure for designing the proposed security system. An alarm system that sounds the buzzer is of no use when a user is not present in the home to take action. When the owner is away communicate with each other. The IoT network consists of embedded electronics, sensors and software from their home, they want to be assured that their home is protected by intruders and thieves while they are gone. This is why the proposed system keeps the owner informed in real time about the security status of their home. The designed system informs the user as there is a break-in so that the user can take necessary actions. We are making use of WiFi module as a probe sniffer which collects the digital footprints of all the nearby devices and sends them to the station to get processed which categorizes them as members or non-members of the home. The members are granted access to get into the home whereas the non-members are not. The log of all these activities is sent to the owner via email every minute whenever possible intruders or guests or anyone who is not in the members list is detected by the system. We are making use of tools like PyShark to capture the probe requests and using JSON to communicate between the module and the servers.

**Chapter - 2**

*Literature Review*

Author in [11] the IEEE 802.11 standard defines Wi-Fi probe requests as an active mechanism with which mobile devices can request information from access points and accelerate the Wi-Fi connection process. Researchers in previous work have identified privacy hazards associated with Wi-Fi probe requests, such as leaking past access points identifiers and user mobility. Besides several efforts to develop privacy-preserving alternatives, modern mobile devices continue to use Wi-Fi probe requests. In this work, we quantify Wi-Fi probe requests.

In [12] Wireless Sensors Networks (WSNs) combined with the use of Internet of Things (IoT) and Cognitive Internet of Things are expanding smart home concepts and solutions, and their applications is been addressed to.

In this paper [8,10,18] we present the idea of exploiting WiFi probe requests to de-anonymize the origin of participants in large events and proposed a technique for estimating the number of mobile devices present at a certain place and time, through analysis of WiFi probe requests from smart devices.

The paper [9,13,15] home operated by Android application wirelessly inside the home and also from anywhere in the world using GSM system. We decorated our project with

(i) smart electrical monitoring system where user can operate wirelessly their light, fan, TV, freeze etc. inside the house even anywhere in the world

(ii) smart Security system where user can maintain the security system using application.

The “Home Area Network” [15] in order to provide connectivity for data exchange and to perform their operations. In this paper, we present a Smart Home security system using Intel Galileo that employs the integration of cloud networking, wireless communication, to provide the user with features like gas leak detection, window and door break detection, motion detection through camera, smoke detection and smart lock etc. The system will automatically change based on sensors’ data.

In this paper [16], they propose a technique for estimating the number of mobile devices present at a certain place and time, through analysis of WiFi probe requests from smart devices.

The research paper is [14,19] to implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBee technology and GSM / GPRS network. The system can send abnormal images and warning messages through MMS and SMS, receive remote instructions, and remote monitor household appliances.

[8,20] Smart phones have become an important part of our daily lives due to their capabilities of accessing the web using WiFi and mobile data networks. These WiFi equipment are constantly sending out packets referred as probe requests, which can be tracked using wireless sniffers. In this thesis, first we investigate capturing of WiFi probe request packets using the help of WiFi Pineapple devices, and analyze how we can use signal strength information of probe request data for indoor occupancy monitoring. Applications of such occupancy monitoring into building surveillance and building energy management are also discussed.

In this paper [21] pyshark is used. Video calls are increasing at a significant rate along with the voice calls, and the demand for cheaper call rates and services with low cost intensive technology is increasing. The scope of the research paper is to analyse SIP (Session Initiation Protocol) network using python sniffer program with new python library modules like pyshark and dpkt.This rich library of protocol intensive modules can help in the analysis of data packets transmitting over the network. It also helps in analysing the SIP (Session Initiation Protocol) data and extraction of RTP (Real Time Transport Protocol) data from the captured data packets and helps in the preparation of an effective software to identify Man-in the middle attacks.

[19] To implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBee technology and GSM / GPRS network. The system can send abnormal images and warning messages through MMS and SMS, receive remote instruction, and remote monitor household appliances.

[10] Media Access Control (MAC) address randomization is a privacy technique whereby mobile devices rotate through random hardware addresses in order to prevent observers from singling out their traffic or physical location from other nearby devices. Adoption of this technology, however, has been sporadic and varied across device manufacturers. In this paper, we present the first wide-scale study of MAC address randomization in the wild, including a detailed breakdown of different randomization techniques by operating system, manufacturer, and model of device This flaw permits an active attack that can be used under certain circumstances to track any existing wireless device.

In this paper [7], we describe our approach that enables spatial human analytics using WiFi probes. Our approach works as follows: we first set up our beacons in the area. Then, we use our novel localization method, which operates in a smart-phone, to broadcast probe requests in a high frequency. Our beacons collect these probe requests and relate them to locations, as estimated from our localization method in the smartphone.

*Summary*

All the above mentioned papers take into consideration the use of IoT technologies and focus mainly on intrusion detection using camera based or infrared technologies. We learnt how to use wifi probing to catch the probe requests and used it in our model to detect identity of the intruder.

**Chapter - 3**

*System Design*

# Existing System[2]

## *IR sensors and camera (First Gen)*

The existing infra-red (IR) or Bluetooth remote controls present in the market are in general appliance specific and the same cannot be used interchangeably.

## *PIR sensors. (Second Gen)*

PIR motion sensors are installed at the entrances of buildings. These sensors detect the motion of human beings. This signal which detects their presence becomes the input trigger for the microcontroller. The owner, who may or may not be present in that building, will be receiving a message on his mobile phone. To turn ON the lights and alarm at house so that the intruder will be warned, the owner can press ’1’ from his mobile keypad. Moreover, if the owner finds that his building is not safe, he can send an SMS to the concerned authority in police department; explaining his situation. The module will turn OFF the alarm and lights after a fixed time delay. The call will be triggered again as soon as the module detects any unexpected motion and the owner will receive the call again and the process continues.

# Proposed System

The traditional systems of tracking the identity of a criminal is a slow process for example, extracting the photo or face of a person from a CCTV footage is a tedious job and not even that accurate. One can easily hide his face using masks while doing any criminal activity.

What we are proposing is a much advanced way which no one has heard of and the criminals are absolutely unaware of. We are going to track the digital footprints of any WiFi enabled devices used by the intruders. The WiFi module present inside the house captures the probe requests sent by the devices in order to connect to any wireless network. All the MAC addresses of the members living in the house are stored in a list. The non members like guests or intruders’ MAC addresses will be identified and emailed to the owner so that he can keep a track of the people entering his house.

# Summary

Wifi module is used to sniff the wifi probe requests from the visitor. Our system will identify the Members and Non-Members from the retrieved MAC Addresses. After differentiating them, the list will be shared via JSON and will be updated accordingly in the UI.

**Chapter - 4**

*Implementation*

## *Tools Used*

* PyShark[3] - Used to capture (sniff) WiFi probe packets from the interface

Python wrapper for tshark, allowing python packet parsing using wireshark dissectors. There are quite a few python packet parsing modules, this one is different because it doesn't actually parse any packets, it simply uses tshark's (wireshark command-line utility) ability to export XMLs to use its parsing.

This package allows parsing from a capture file or a live capture, using all wireshark dissectors you have installed. Tested on windows/linux.

.

* JOSN[4] - Used to share data between layers.

JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for evryone to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language Standard ECMA-262 3rd Edition - December 1999. JSON is a text format that is completely language independent but uses conventions that are familiar to programmers of the C-family of languages, including C, C++, C#, Java, JavaScript, Perl, Python, and many others. These properties make JSON an ideal data-interchange language.

* NodeJS[5] - Used to create web server for accessing UI.

As an asynchronous event-driven JavaScript runtime, Node.js is designed to build scalable network applications.This is in contrast to today's more common concurrency model where OS threads are employed. Thread-based networking is relatively inefficient and very difficult to use. Furthermore, users of Node.js are free from worries of dead-locking the process, since there are no locks. Almost no function in Node.js directly performs I/O, so the process never blocks. Because nothing blocks, scalable systems are very reasonable to develop in Node.js.

* AJAX[6] - For Synchronizing front-end and back-end.

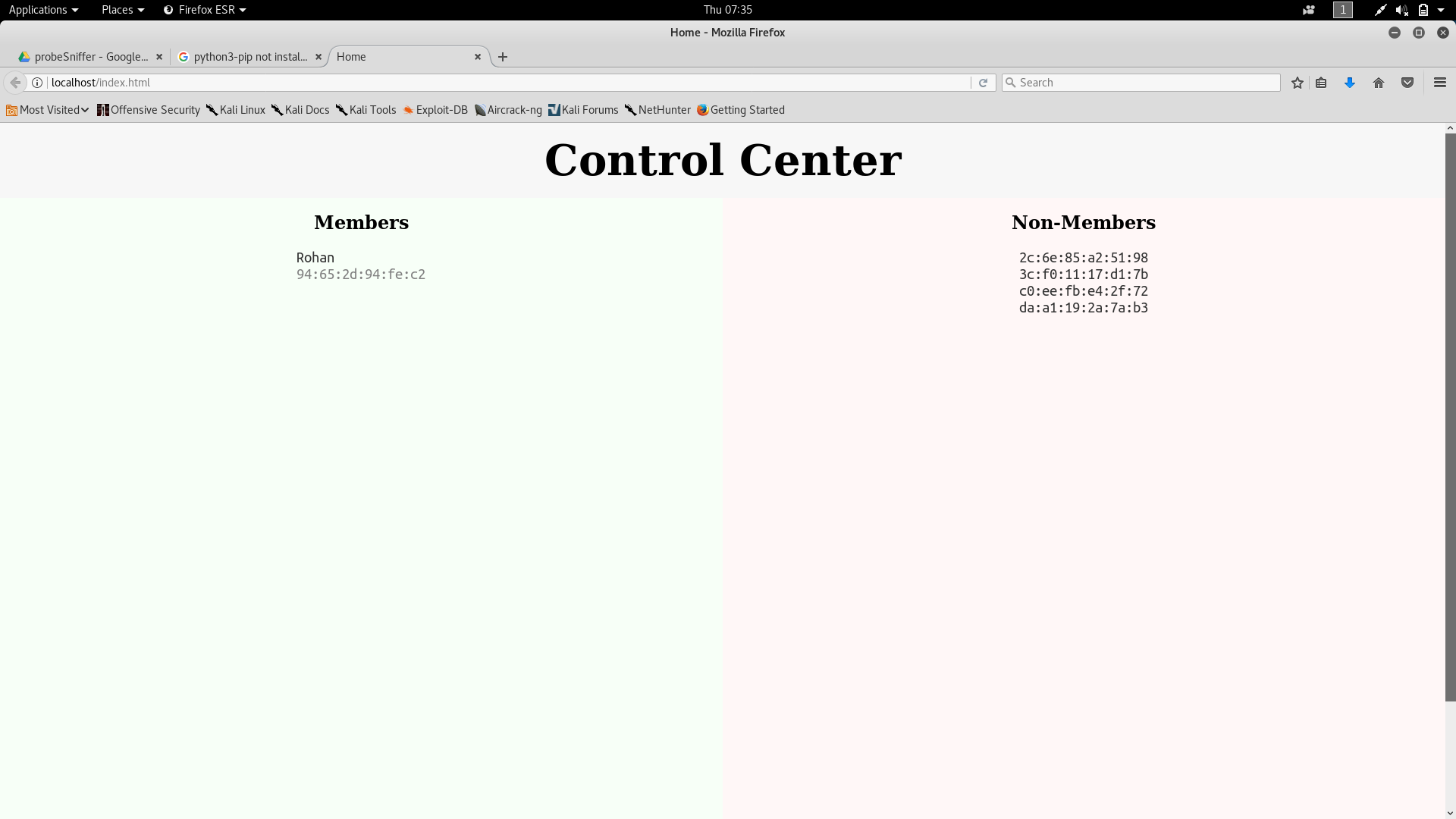
AJAX stands for Asynchronous JavaScript And XML. AJAX is not a programming language. AJAX just uses a combination of a browser built-in XMLHttpRequest object (to request data from a web server), JavaScript and HTML DOM (to display or use the data)

AJAX is a misleading name. AJAX applications might use XML to transport data, but it is equally common to transport data as plain text or JSON text. AJAX allows web pages to be updated asynchronously by exchanging data with a web server behind the scenes. This means that it is possible to update parts of a web page, without reloading the whole page.

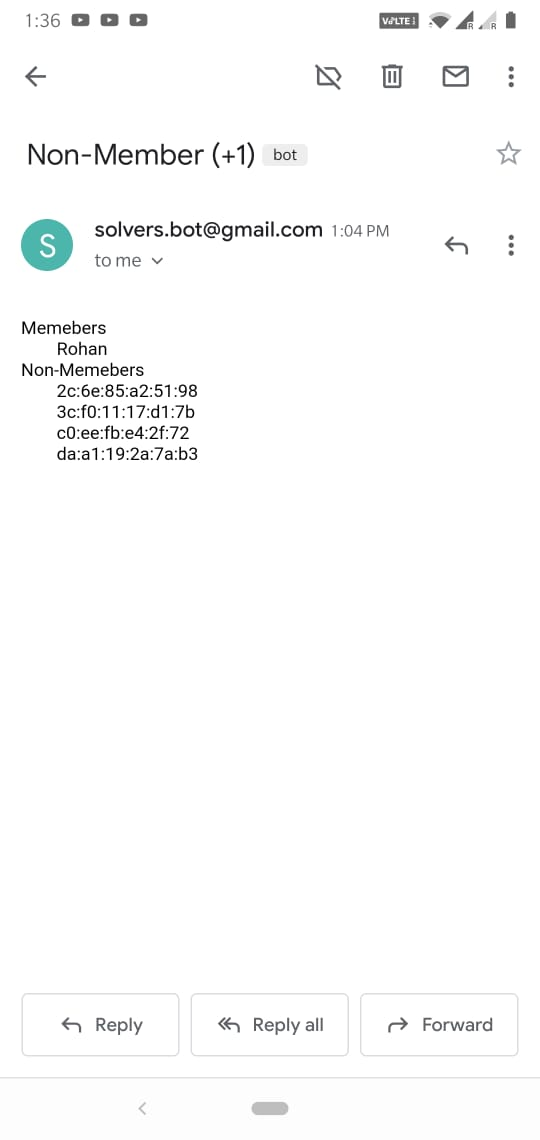
## *Screenshots*

## 

*Fig 1.1*

****

*Fig 1.2*

****

*Fig 1.3*

## *Summary*

Using PyShark, we can capture the probe packets sent by all the devices nearby and detect any intrusion. We can also keep a track of all the passing devices for safety purposes. We have a Node JS Server which differentiates the members from non-members and keeps on updating. We have implemented a python module which updates the owner with a list of all the new non - members and members near the house.

**Chapter - 5**

*Performance Evaluation*

##### 

##### 

*Fig 2.1*

##### 

*Fig 2.2*

##### 

*Fig 2.3*

##### 

*Fig 2.4*

*Summary*

This system is better than Camera based system in case of cost (fig 2.3), speed (fig 2.2), memory usage (fig 2.1) and has an extra feature of intrusion detection (fig 2.4).

It is also better than Motion Detection system in case of Cost and memory usage. Motion detection cannot be used for Identity detection and has low coverage which is resolved by using this Wifi Sniffing based system.

**Chapter - 6**

*Conclusion*

The WiFi module present at homes will identify the members and non-members by capturing the WiFi probe requests sent by their devices and checking with the database. The list of all the captured MAC addresses is sent to the owner for safety reasons.

By tracking the digital footprint of the people visiting the house it is easier to track the identity of the intruder in case of any criminal activity like theft.This setup can also be used in commercial offices where some areas are restricted for certain personnel, such a system will immediately inform the administrator of any unauthorized personnel trying to access such an area. Therefore the extensibility and applicability of such a system is only limited only by the imagination.The developed system can also be used in industrial and commercial applications such as offices, warehouses and other areas where some areas are reserved for authorized personnel only or other places where safety and precautions are of primary concerns such as internet server room of a big MNC from where corporate data can be stolen. The system can also be easily upgraded to add extra safety features such as cameras, motion detection sensors, etc. for increased safety.

*Future Works*

This can be extended to track the position of the intruder by using more than one sensor.

If more than two sensors are present, we can use the readings to triangulate the position of the target device. This triangulation can be real time and we can track the movements of the intruder in case of intrusion which would be of great help in case of intrusions.