

# CHAPTER 1

## 1.1 INTRODUCTION TO IOT

The Internet of Things (IoT) is the network of physical objects—devices, instruments, vehicles, buildings and other items embedded with electronics, circuits, software, sensors and network connectivity that enables these objects to collect and exchange data. The Internet of Things allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency and accuracy. IoT is able to interact without human intervention. IoT technologies are at their infant stages. Many new developments have been occurred in the integration of objects with sensors in the internet. Some preliminary IoT applications have been already developed in health care, transportation, and automotive industries.

IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A and Wifi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

1) **RFID** (radio-frequency identification). It provides simple, low- energy, and versatile options for identity and access tokens, connection bootstrapping, and payments. This technology employs 2-way radio transmitter-receiver to identify and track tags associated with objects.

2) **NFC** (near-field communication). It provides simple, low- energy, and versatile options for identity and access tokens, connection bootstrapping, and payments. NFC consists of communication protocols for electronic devices, typically a mobile device and a standard device.

3) **Low-Energy Bluetooth**. This technology replaces the hungriest aspect of an IoT system. Though sensors and other elements can power down over long periods, communication (I.e., wireless) must remain in listening mode. Low-energy wireless not only reduces consumption, but also extends the life of the device through less use.

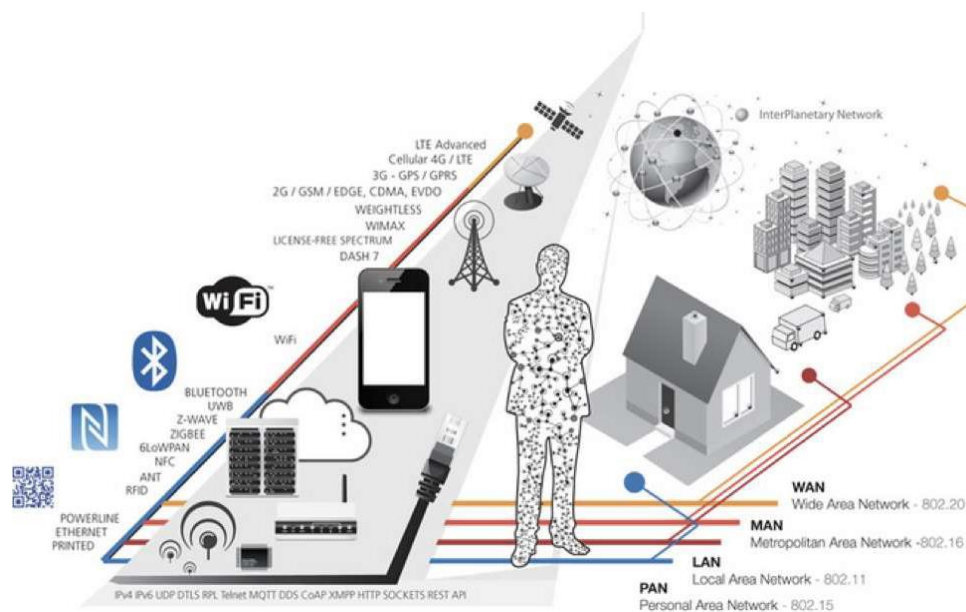
4) **Radio Protocols**. ZigBee, Z-Wav, and Thread are radio protocols for creating low-rate private area networks. These technologies are low-power, but offer high throughput unlike many similar options. This increase the power of small local device networks without the typical costs.

5) **LTE-A**, or LTE Advanced, delivers an important upgrade to LTE technology by increasing not only its coverage, but also reducing its latency and raising its throughput. It gives IoT a tremendous power through expanding its range, with most significant applications being vehicle, UAV, and similar communications

6) **WiFi-Direct**. eliminates the need for an access point. It WiFi, but with lower latency. WiFi-Direct eliminates an element of a network that often bogs it down, and it does not compromise on speed or throughput.

A critical requirement of an IoT is that the things in the network must be connected to each other. IoT system architecture must guarantee the operations of IoT, which connects the physical and the virtual worlds. Design of IoT architecture involves many factors such as networking, communication, processes etc. In

designing the architecture of IoT, the extensibility, scalability, and operability among devices should be taken into consideration. Due to the fact that things may move and need to interact with others in real-time mode, IoT architecture should be adaptive to make devices interact with other dynamically and support communication amongst them. In addition, IoT should possess the decentralized and heterogeneous nature.



**Figure 1.1** INTERNET OF THINGS -INFOGRAPHIC

## 1.2 SNMP

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes and routers. It comprises part of the TCP/IP suite. System administrators can remotely manage network performance, find and solve network problems, and plan for network growth by using SNMP. Instead of defining a large set of commands, SNMP places all operations in a *get-request*, *get-next-request*, *get-bulk-*

*request*, and *set-request* format. For example, an SNMP manager can get a value from an SNMP agent or store a value in that SNMP agent. The SNMP manager can comprise part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a router.

A network that uses SNMP requires three key components—managed devices, agents, and network management software (NMS).

1) **Managed devices.** Devices that contain SNMP agents and reside on a network. Managed devices collect and store information and make it available by using SNMP. The first node in the Cisco Unified CM cluster acts as the managed device. In Cisco Unified CMBE, the server on which Cisco Unified CM is installed acts as the managed device.

2) **Agents.** Software modules that contain local knowledge of management information and translates it into a form that is compatible with SNMP. Cisco Unified CM uses a master agent and sub-agent components to support SNMP. The master agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. It contains a few Management Information Base (MIB) variables. The master agent also connects and disconnects sub-agents after the sub-agent completes necessary tasks. Cisco Unified CM uses a sub-agent to interact with the local Cisco Unified CM only. The Cisco Unified CM sub-agents send trap and information messages to the SNMP Master Agent, and the SNMP Master Agent communicates with the SNMP trap receiver (notification destination).

3) **NMS**. SNMP management application that runs on a PC and provides the bulk of the processing and memory resources that are required for network management. It executes applications that monitor and control managed devices.

The NMS uses the Cisco MIB variables to set device variables and to poll devices on the inter-network for specific information. The results of a poll can get graphed and analyzed to help you troubleshoot inter-network problems, increase network performance, verify the configuration of devices, and monitor traffic loads. Three versions of SNMP exist: version 1 (SNMPv1), version 2 (SNMPv2), and version 3 (SNMPv3).

1) **SNMPv1**. It represents the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI) and operates over protocols, such as User Datagram Protocol (UDP) and IP. With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

2) **SNMPv2c**. It functions within the specifications of SMI. MIB modules contain definitions of interrelated managed objects. Be aware that the operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 trap.

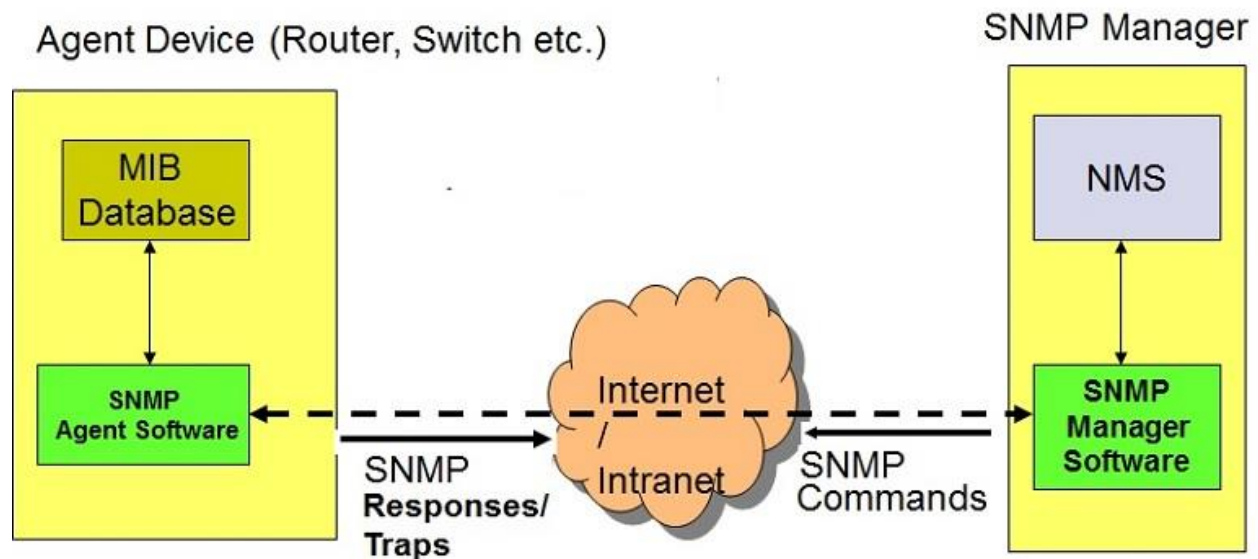
The Inform operation in SNMPv2c enables one NMS to send trap information to another NMS and to receive a response from the NMS.

3) **SNMPv3**. It provides the following security features:

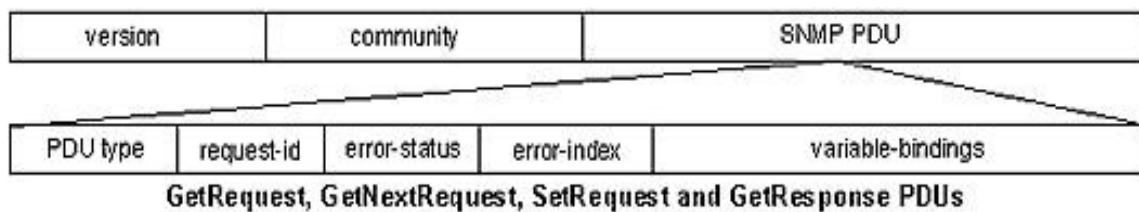
- Authentication—Verifying that the request comes from a genuine source.
- Privacy—Encrypting data.
- Authorization—Verifying that the user allows the requested operation.

- Access control—Verifying that the user has access to the objects that are requested.

# SNMP Architecture



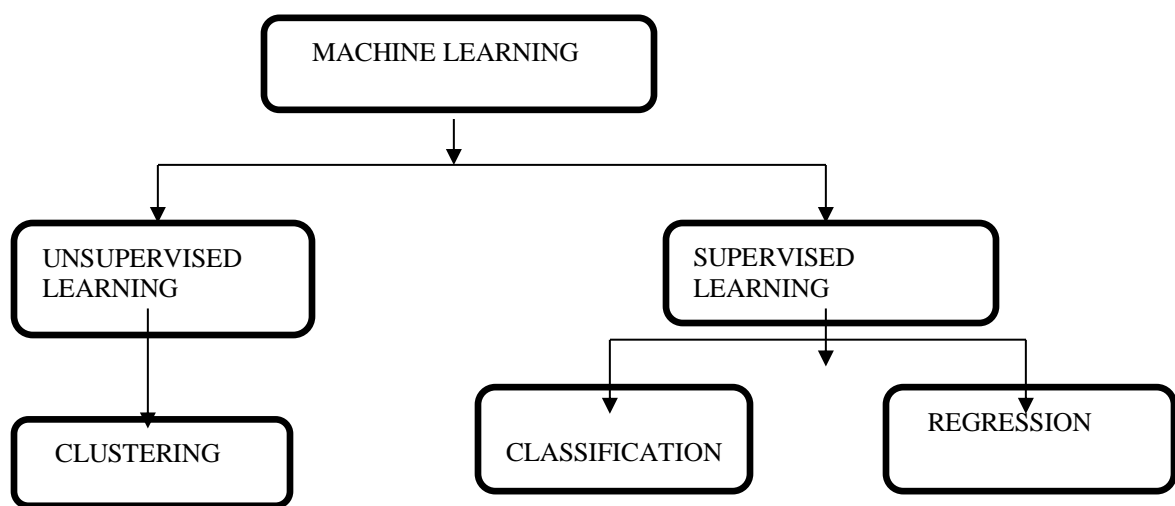
**FIGURE 1.2 SNMP ARCHITECTURE**



**Figure 1.3 SNMP PACKET FORMAT**

## 1.3 MACHINE LEARNING TECHNIQUES

Machine learning is a data analytics technique that teaches computers to do what comes naturally to humans and animals: learn from experience. Machine learning algorithms use computational methods to “learn” information directly from data without relying on a predetermined equation as a model. The algorithms adaptively improve their performance as the number of samples available for learning increases.



**Figure 1.4** Types of Machine Learning

### Unsupervised Learning

Unsupervised learning finds hidden patterns or intrinsic structures in data. It is used to draw inferences from datasets consisting of input data without labeled responses.

### Supervised Learning

Supervised learning builds a model that makes predictions based on evidence in the presence of uncertainty. A supervised learning algorithm takes a known set of input data and known responses to the data (output) and trains a model to generate

reasonable predictions for the response to new data. Supervised learning uses classification and regression techniques to develop predictive models.

## **Classification**

Classification techniques in data mining are capable of processing a large amount of data. It can be used to predict categorical class labels and classifies data based on training set and class labels and it can be used for classifying newly available data. The term could cover any context in which some decision or forecast is made on the basis of presently available information. Classification procedure is recognized method for repeatedly making such decisions in new situations. Classification techniques predict discrete responses—for example, whether an email is genuine or spam, or whether a tumor is cancerous or benign. Classification models classify input data into categories. Typical applications include medical imaging, speech recognition, and credit scoring. Common algorithms for performing classification include support vector machine (SVM), C5.0 decision tree, boosted and bagged decision trees,  $k$ -nearest neighbor, Naïve Bayes, logistic regression, and neural networks.



## **CHAPTER 2**

### **LITERATURE SURVEY**

You-Sun Hwan and Eung-bae Kim [1] presented” An Architecture of SNMP-based Network Management of the Broadband Wireless Access System” This paper discussed the ideas and implementation behind SNMP protocol for management of network in the Broadband wireless access network. The network management system consists of manager, SNMP agent, GUI and has functions of network monitoring and fault monitoring based standard MIBs and private MIBs. They consider the type of information that is of interest to a network monitor such as uplink channel frequency, power modulation and modulation type. Fault monitoring allows for the detection and reporting of faults. A fault-monitoring object will maintain a log of significant events and errors. They plan to extend the performance-monitoring module. The security is a big weakness that must be addressed when using SNMPv2. In order to improve security, they try to complement it. They implement this management system in a Sun workstation, so if that is they plan to, they can operate in the Web everywhere.

#### **DISADVANTAGES**

It cannot be operated everywhere using web as it is implemented in Sun workstations.

It is less secured that anyone can get access to use the internet.

Huiyi Zhang, Haibo Lu, Zhixiang Yuan, Qilong Zhou and Yong Tao [2] presented “Design and implementation of wireless sensor network management based on SNMP”. Aiming at the advantages of the traditional network management in SNMP, combined with the characteristics of wireless sensor network itself. A

method of wireless sensor network wireless management based on SNMP is given. That wireless network is abstracted as a virtual device as SNMP managed node, to achieve this wireless network management in the system level, Integrated configurations, operations and maintenance functionality in a traditional way. Adopting to a technology of wireless sensor network based on the protocol 802.15.4/ZigBee and the Embedded System, a ZigBee wireless sensor network management based on SNMP is designed and realized.

## **DISADVANTAGES**

It is less secure.

Lower speed compared to a wired network.

Junjiao Ye, Zenghua Zhao, Hao Li and Hao ChenIn [3] presented “Hierarchical Heterogeneous Wireless Sensor Network Management System”. In this paper, they design and implement a heterogeneous wireless sensor management system, and make a large number of experimental verifications in test-bed. Heterogeneous wireless sensor network is built up by multiple sensor nodes with different functions and processing capabilities. Experimental results show that this system implements system configuration management, performance management and fault management. This system can be used for the daily maintenance and management of heterogeneous wireless sensor network as well as the performance evaluation of network system.

## **DISADVANTAGES**

It is less secure.

It can communicate over short distance only.

H. Otok, A. Mourad, M. Debbabi and C. [4] presented “As Improving the Security of SNMP in Wireless Networks”. The protocol SNMPv3 with its existing security is not sufficient for wireless network, where the intruder has many tools to analyze and crack password. The protocol SNMPv3 uses the admin password for one-way authentication and from this password the keys are derived. If an intruder is capable of knowing the password, the intruder can easily manage all the devices in the domain of the manager whose password has been cracked. In our new architecture, we presented two-way authentication independent of the admin password using the certification authority. The latter is the entity that signs and issues the certificate both the manager and agent. Diffie-Hellman algorithm is used for secure key exchange between the manager and the agent. To ensure the security of Diffie-Hellman, time stamps and signatures are used in the key exchange protocol to prevent MITM attack. Finally, if an intruder wants to attack the Diffie-Hellman algorithm, the intruder needs to solve the discrete logarithm problem, which usually requires too much computation time.

## **I. DISADVANTAGES**

All the process is manual

Lots of time are needed to connect and for the secured connection.

J. Kantorovitch, P. Mähönen [5] presented “Case studies and experiments of SNMP in wireless networks”. The performance of an SNMP based network management system in a wireless environment is discussed in this paper. The simulation results are verified and compared with the measurements performed in real network conditions. It was found that the response time in notifying the network manager much depends on wireless link quality. For the same system load, the

response time for bad link quality is about 2-3 times longer compared with the environment with good channel conditions. Therefore, it is reasonable to consider channel conditions in the process of network design and planning. The system load must be taken into account, as well to consider network dimensioning. Also, the issues related with the nature of the SNMP manager - agent communication are presented in this research. The "concurrent" SNMP is compared with the "serial" one. The lessons learned from this experiment are that the response time for the management application is better for the "concurrent" mode, but the "serial" method is faster in task response time. Also, in the "serial" method there is much less scattering in task response time compare with the "concurrent" one and that can be important for some real-time non generic management applications.

## **DISADVANTAGES**

- Depends on the wire quality.

- It can be done only in serial and concurrent mode.

## **CHAPTER 3**

### **SYSTEM ANALYSIS**

#### **3.1 EXISTING SYSTEM**

Normally, Intranet is based on only wired connection. In Existing System, client-server architecture is used. The client running on your Network management solution will be responsible for polling data or setting data. The server running on your actual device will respond to client's call. It provides management capability for TCP/IP based networks. Through wired connection, it provides efficient connection but it is not secured enough. All the activities in the management is a manual process. The user has to do the things manually to connect to the intranet.

#### **DRAWBACKS**

Activities are manual, not automatic

The processing speed is little low.

## 3.2 PROPOSED SYSTEM

The number of WLAN networks has increased rapidly especially within companies and in education. WLAN networks are also provided as services in airports, hotels, and cafeterias. This fact will also mean that there is a need to manage those networks professionally and because of the sheer size of those networks, the amount and quality of management traffic is not insignificant.

Today, there is a diversity of wireless equipment based on different hardware solutions, running various operation systems and supporting all kinds of existing protocols. Reality shows that most of the wireless LAN products offer SNMP to support network management. SNMP-based system performance in real network conditions measuring the response time of the device to see if it depends, and how much, on the wireless link quality and system load. Consequently, specifying the particular polling interval, we estimate the largest number of mobile nodes that a single manager is able to manage. This knowledge can then be used in the WLAN network design and planning process. The measurements are usually dependent on the measurement platform used, such factors as hardware characteristics, software configuration, and even environment properties influence the performance of the system.

In this project, a new framework in an IoT environment by using a new strategy as SNMP in Wireless IoT environment is created, which works based on C5.0 Decision Tree Classification algorithm that makes automatic device identifier mechanism in Wireless intranet environment. The solution for implementing the wireless channel as “malicious” and “not-malicious” states is based on the C5.0 algorithm. The channel configuration node is aimed at providing the configuration of the bit error rate , entropy, information gain and response time. Because the

received signal quality is rapidly varying, it is possible that in the case of a large number of SNMP agents, some of the manager - agent sessions will fall into the fading regions, which would considerably extend the response time compared to a non-fading region of the signal. So, to measure the response time reliably, a single SNMP agent is polled continuously during five hours each time after the previous management task has been completed. In the following briefly review some relevant works to this project, including the algorithm and the process involved in the working of the system.

## **ADVANTAGES**

Automation

Performance speed has increased

## **CHAPTER 4**

### **SYSTEM SPECIFICATION**

#### **HARDWARE & SOFTWARE REQUIREMENTS:**

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It should what the system do and not how it should be implemented.

#### **HARDWARE REQUIREMENTS**

Toolkit	:	Raspberry pi3
Processor	:	BroadcomBCM2837B0,64-BitSoC@-@1.4GHz
Memory	:	GBLPDR2 SDRAM
RAM	:	GB

#### **SOFTWARE REQUIREMENTS**

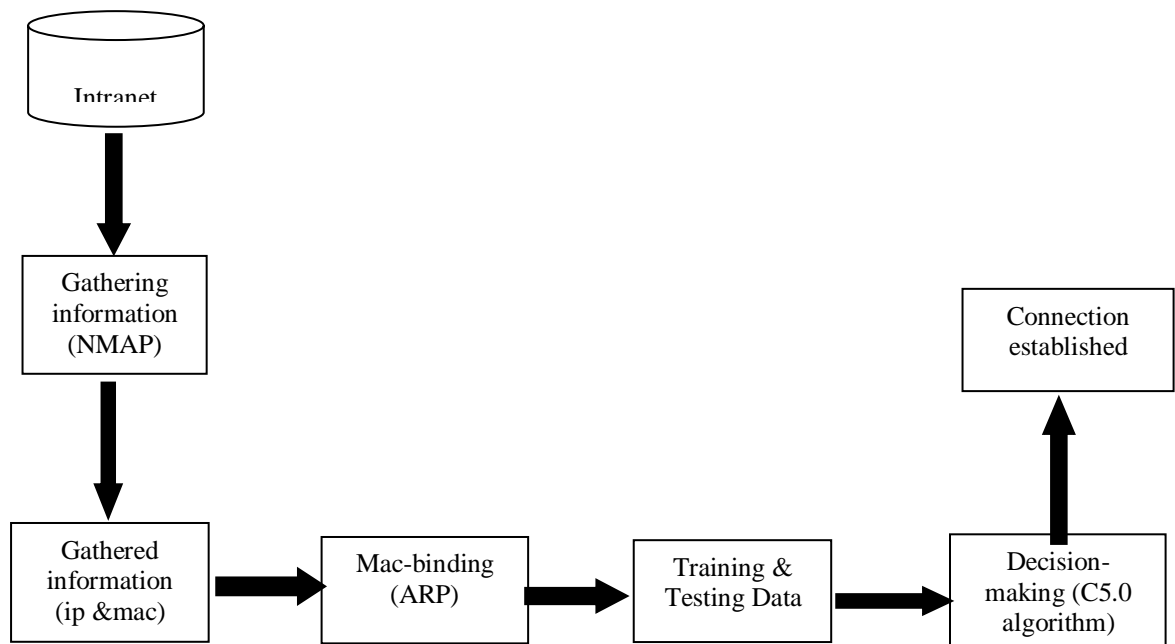
Language	:	Python
Operating system	:	Kali Linux
Tools	:	PyCharm



## CHAPTER 5

### SYSTEM DESIGN

#### 5.1 SYSTEM ARCHITECTURE



**Figure 5.1** SYSTEM ARCHITECTURE

## **5.2 MODULE DESCRIPTION**

The proposed system consists of three modules

- Creation of Smart Intranet Environment (SIE)
- Creation of IoT Environment enhanced to SNMP(IS)
- Integrating working of IS and C5.0 (Smart IS)

### **5.2.1 CREATION OF SMART INTRANET ENVIRONMENT(SIE)**

#### **RASPBERRY PI:**

It is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing, and to learn to program in languages like scratch and python. It's capable of doing everything you'd expect a desktop computer to do, from browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games. It has the ability to interact with the outside world, and has been used in the wide area of digital marker projects, from music machines and parent detectors to weather stations and tweeting birdhouses with infra-red cameras.

In our project, it has been used as a server in SNMP. It will manage the whole SNMP management process. When a device enters the region, Pi finds an arrival of new device is coming and it informs the SNMP about the new arrival. Being a server, it will send request messages and get the reply messages. It will then gather the information about the device without the user's knowledge and update the information to MIB. MIB is a database storage in SNMP. Raspberry Pi will act as both the server as well as the whole network management. In case of any failures in

SNMP, Raspberry pi will act as a server and network manager despite SNMP to run the working process without any failures in the system.

## **ARP**

The Address Resolution Protocol (ARP) feature performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses. ARP involves the process of mac-binding.

IP addressing occurs at Layer 2 (data link) and Layer 3 (network) of the Open System Interconnection (OSI) reference model. OSI is an architectural network model developed by ISO and ITU-T that consists of seven layers, each of which specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer. Layer 2 addresses are used for local transmissions between devices that are directly connected. Layer 3 addresses are used for indirectly connected devices in an inter-network environment. Each network uses addressing to identify and group devices so that transmissions can be sent and received. The most commonly used network types are Ethernet II and SNAP

By default, the Address Resolution Protocol (ARP) feature is enabled and is set to use Ethernet encapsulation. Perform the following tasks to change or verify ARP functionality:

- Enabling the Interface Encapsulation
- Defining Static ARP Entries
- Setting an Expiration Time for Dynamic Entries in the ARP Cache
- Globally Disabling Proxy ARP

- Disabling Proxy ARP on an Interface
- Verifying the ARP Configuration

After the Raspberry Pi finds the new device and nmap has been initiated, ARP plays a major role here. The Raspberry pi acts as a server and it will initiate the ARP. The mac-binding process is performed. It will convert the ip\_address to mac\_address. Then both their ip\_address and mac\_address is binded using the mac-binding concept. Then the server updates the MIB by the binded ip\_address and mac\_address to MIB. The updated information is stored in the MIB. The MIB has all the device's information that it is registered already and the safe device's information.

## **NETWORK TOPOLOGY**

Internet topology is the structure by which hosts, routers or autonomous systems (ASes) are connected to each other. The majority of existing Internet topology research focuses on the AS-level. There are three reasons for this. First, AS-level Internet topology is at the highest granularity of the Internet; other levels of Internet topology partially depend on AS-level topology. Second, the AS-level topology is relatively easy to obtain; other levels of topology are sometimes regarded as private information and are harder to get. Third, AS-level topology is not directly engineered by humans; instead, it is the aggregate result of technological and economical forces.

It is a structure that the host, ip\_address, mac\_address and the device all together are connected to establish a connection. This topology is maintained in the server. The server is the Raspberry Pi. It will collect the information about the device and update the MIB. The device, it's ip\_address and mac\_address are connected in this level (i.e., topology). After the connection, it will proceed for the next step.

## **5.1.2 CREATION OF IOT ENVIRONMENT ENHANCED TO SNMP(IS)**

### **PYCHARM:**

PyCharm is an integrated development environment (IDE) used in computer programming, specifically for the Python language. It is developed by the Czech company JetBrains. It provides code analysis, a graphical debugger, an integrated unit tester, integration with version control system (VCSes), and supports web development with Django. PyCharm is cross-platform, with windows, macOS and Linux versions.

### **NETWORK MANAGEMENT MODEL**

Intranet environment is created with SNMP (i.e., a network management system). Network management system's architecture consists of three parts: SNMP manager/GUI which can reside on any system and SNMP agent which resides on the managed element (ex. Base station).

SNMP Manager communicates with the SNMP Agent for SNMP protocol by defined WC1907. By integrating UDP Socket into 161 Port, SNMP manager sends SNMP Packets to SNMP Agent, and SNMP agent responds to any Port. For example. in the case of Trap, The Agent sends SNMP v2 Trap Message to Manager via 162 UDP ports, which is monitored by the manager. SNMP manager stores DB table in MIB, which originates from SNMP MI9 Query through DB schema. The manager also sends predefined SNMPv2 Trap information message to the GUI via UDP socket.

SNMP agent executes the orders given to the Manager by SNMP. SNMP agent also acts as a messenger to the Managers commands. The SNMP Agent Task receives SNMP Get/Get Next/Set Request commands from the SNMP Manager. Once the commands are received, the SNMP Packet is decoded into the SNMP PDU in the SNMP Protocol Processing Module. When the fault occurs in the Agent, it sends SNMP Trap PDU of changed management status information to the Manager. SNMPMib operates nearly every MIB and has methods that allow it to search required object by agent in the array. SNMPMibName contains each of the MIB node information.

GUI is designed for user's convenience. GUI provides two windows; one that presents network topology and the one that show BS status, channel's information and Subscriber station's information. One window is the SNMP Trap message that has the network's fault type. If fault occurs between BS and SS, right window shifts its color from green to red as an indicator. Organizing the network and managing the network faults are some of the functions of the Network management system.

## NMAP

Nmap is a tool used for determining the hosts that are running and what services the hosts are running on a network. Once the network is charted out using tools like Lan Map Shot, the Nmap can be used to determine the type of services and hosts running in the network.

Some of the Nmap options are explained below:

1) **TCP Connect Scanning.** Any host can issue a connect () system call to try and open an interesting port on a machine. If the port is open the call succeeds. Though it is the fastest scan it is easily detectable and blockable.

2) **TCP SYN Scanning.** The monitoring host attempts a three way hand shake but does not compel the third step, while negotiating a TCP connection. Once an acknowledgement is received from the target host, the connection is reset. SYN scanning is picked up by most firewalls and packet filters.

3) **TCP FIN Scanning.** FIN packets tend to be undetected by firewalls and packet filters. TCP property forces closed port to respond with an RST packet to a FIN packet. This property is used for scanning to determine the open and closed ports.

4) **Fragmentation Scanning.** The TCP header of the probe packet is spilt to smaller packets making it difficult for detection. But beware that this kind of scanning can cause many programs to be unstable.

4) **ICMP Port Unreachable Scanning.** Though many firewalls will discard ICMP echo request messages, they may permit other types of ICMP traffic to pass unhindered. In addition to ICMP request echo messages, recent versions of nmap allows other two types of ICMP messages to be sent. The scan uses the property of the closed port sending ICMP\_port\_unreachable error message for closed port for detection.

In our project, nmap is a program that gets the device's host information, ip\_address, and mac\_address. It is also used in getting ICMP request and reply messages and response time. Here, Raspberry Pi takes the main role. Raspberry Pi works as a server and all the SNMP management is done. The ICMP request message is a request message that is sent to the device that is entering the wifi range. The ICMP reply message is the reply message of the device to the server. The response time is the time the device is responding for the ICMP request.

When the Raspberry Pi finds a new device in the range, it will inform the MIB and initiates the Nmap. After the Nmap is initiated, the information about the device is gathered without letting the person knows and sends it to the Manager Information Base (MIB). The Nmap is initiated every time the Raspberry Pi founds a device and every five hours.

### **5.1.3 INTEGRATING WORKING OF IS AND C5.0 (SMART IS)**

#### **C5.0 ALGORITHM**

C5.0 algorithm is widely used as a decision tree method in machine learning. Initially we have ID3.0 algorithm. Based on ID3.0, people developed C4.5 algorithm, and finally develop C5.0 algorithm. This type of decision tree model is based on entropy and information gain.

Entropy is the impurity measurement of the devices (i.e.,) which separates the devices into malicious or not.

$$\text{Entropy}(S) = -P(\text{yes}) \log P(\text{yes}) - P(\text{no}) \log P(\text{no})$$

Information gain, which decides which attribute should be selected as the decision node. It is calculated by the formula

$$\text{Information Gain} = \text{Entropy}(S) - [(\text{Weighted average}) * \text{Entropy (each feature)}]$$

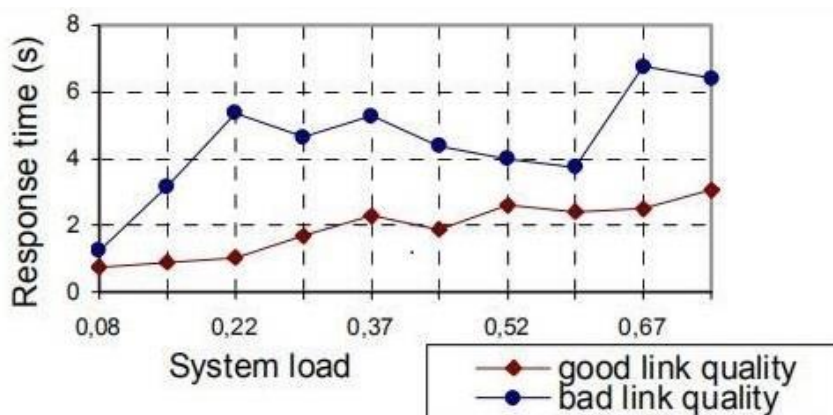
Pruning is the cutting of the nodes to find the best optimum solution. It reduces the complexity.

The working of the algorithm depends upon the entropy and information gain and response time. The response time is calculated from the time of response to the server by the device. The entropy and information gain are used for the selection of the root node. First calculating the entropy value for each feature of the dataset. Then the information gain for each attribute of the dataset are calculated and the root node



is selected. The pruning is made to find the best optimum solution(i.e.,) a decision tree is built.

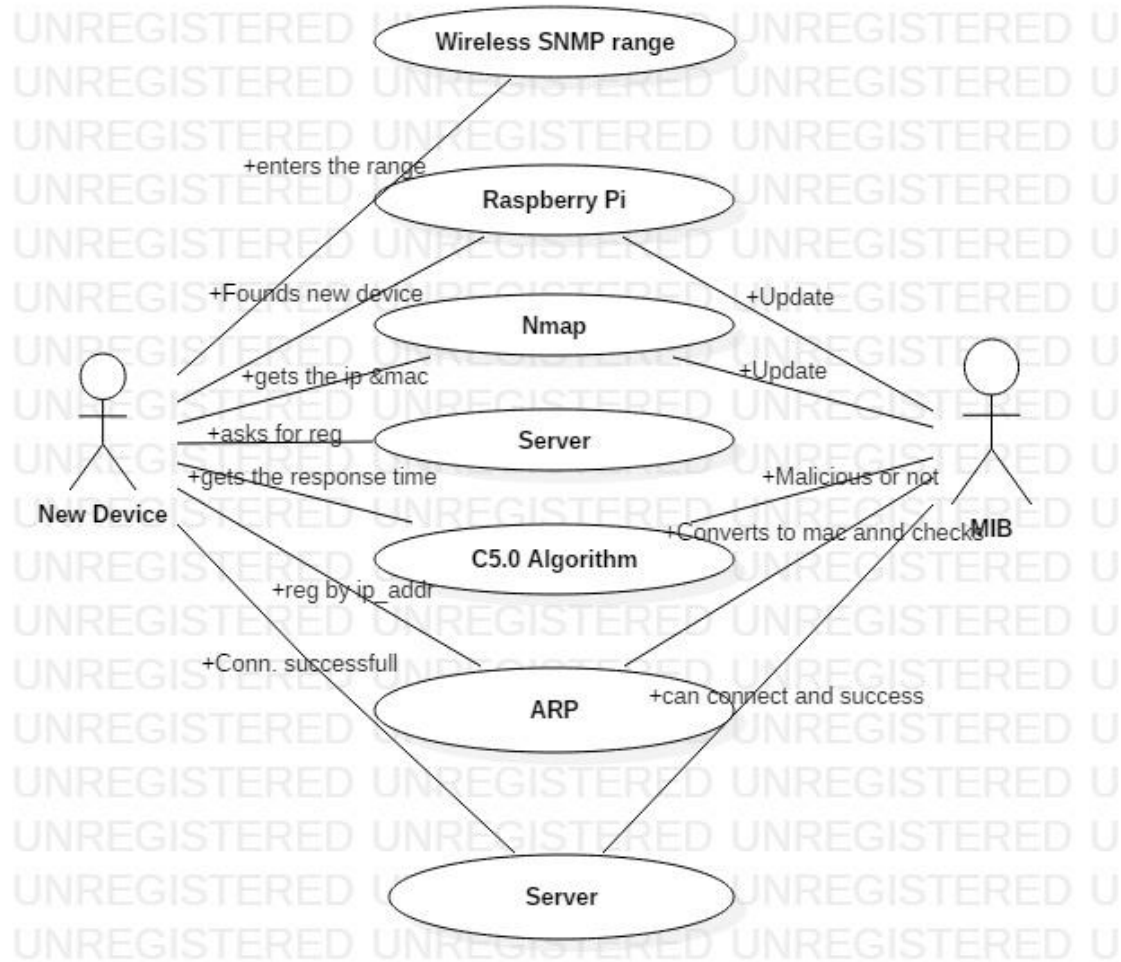
The working of the algorithm on the project is based upon the response time. The algorithm forms a decision tree based on the needs. The decision tree that is created will tell which nodes to sleep, switch on, execute first, eliminate and so on. The dataset is stored in a Management Information Base (MIB). Every time a new device arrives, the dataset will be updated with their response time, ip\_address, mac\_address and malicious or not. A response time will be setup manually in the program. The response time for the devices are stored with their ip\_address and mac\_address. While the server asks for the registration, the response time is contributing a main part here. The reply should be within the fixed response time. If the device response to the request made by the server within the allocated response time, it will be considered as not-malicious and allowed to make the further steps. If the device doesn't reply within the allocated response time, it will be considered as the malicious device and will not allow to do the further steps to make the connection. This algorithm makes the model find the device and the decision making automatic.



**Figure 5.2** Graph of the devices connected in Intranet and IoT

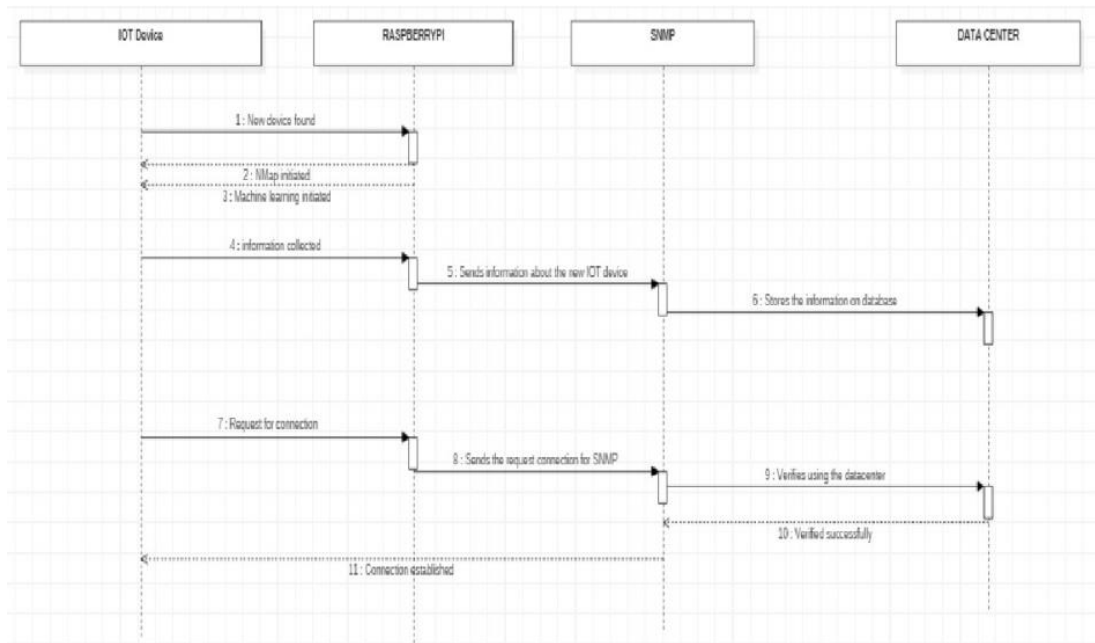
## 5.2 PROJECT DIAGRAMS

### 5.2.1 USE CASE DIAGRAM

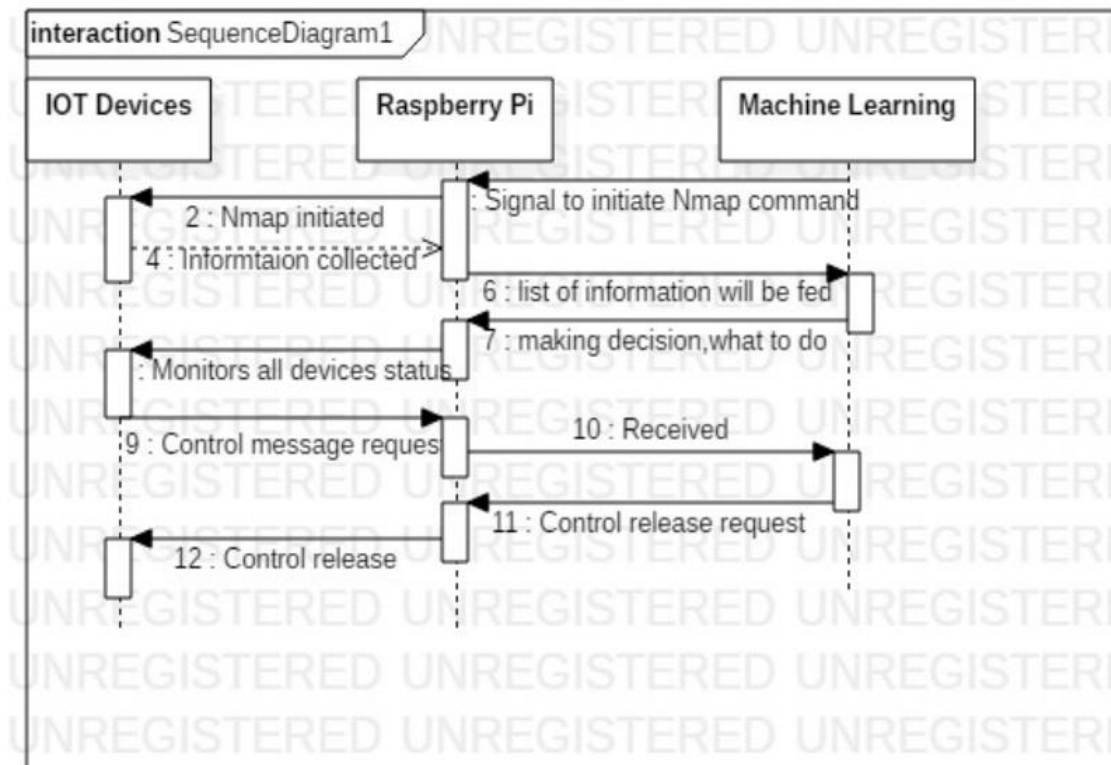


**Figure 5.3** USE CASE DIAGRAM OF THE SYSTEM

## 5.2.2 SEQUENCE DIAGRAM



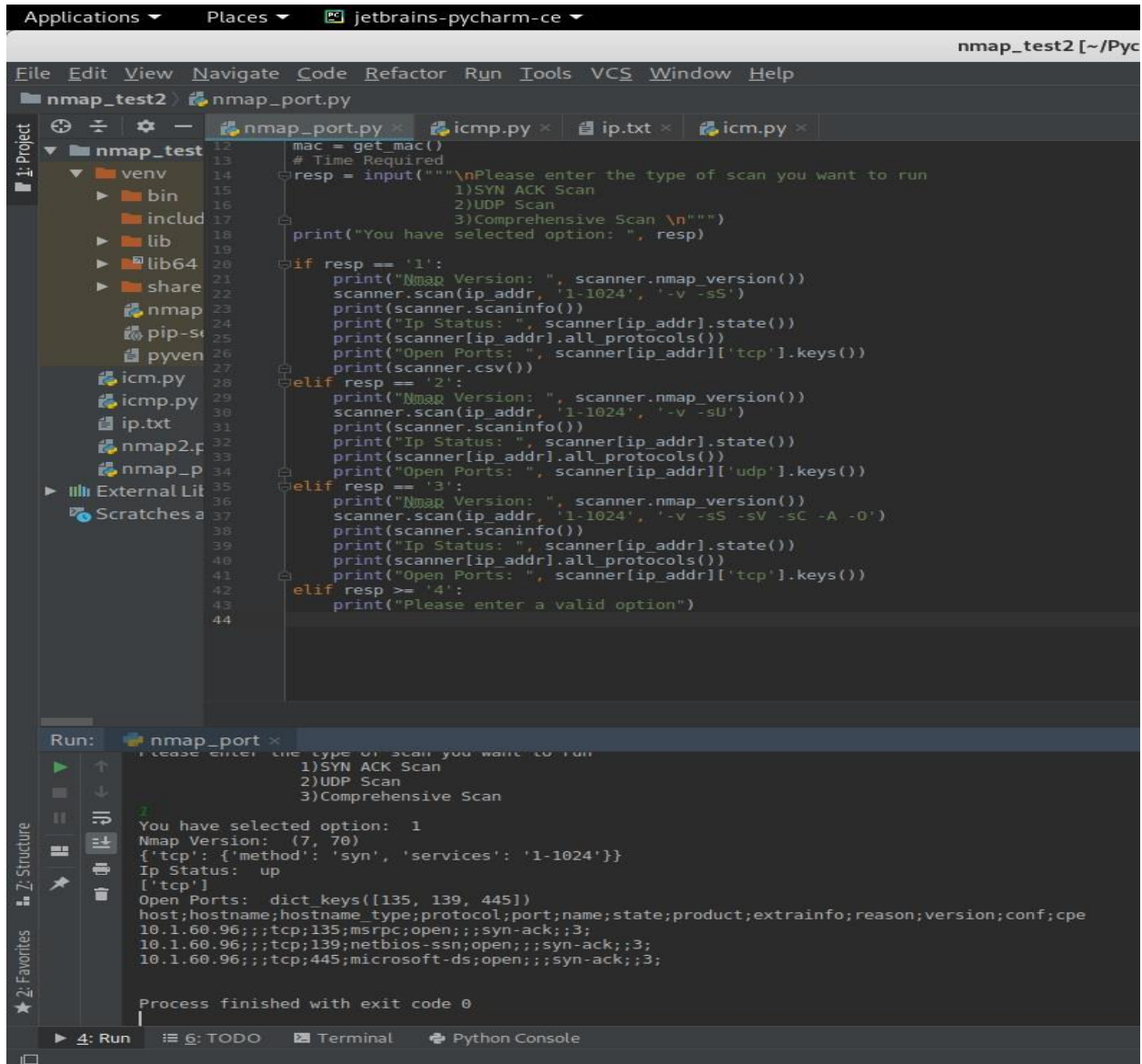
**FIGURE 5.4** SEQUENCE DIAGRAM OF THE SYSTEM



**FIGURE 5.5** SEQUENCE DIAGRAM OF THE WORKING PROCESS

## CHAPTER 6

### RESULT AND OUTPUT



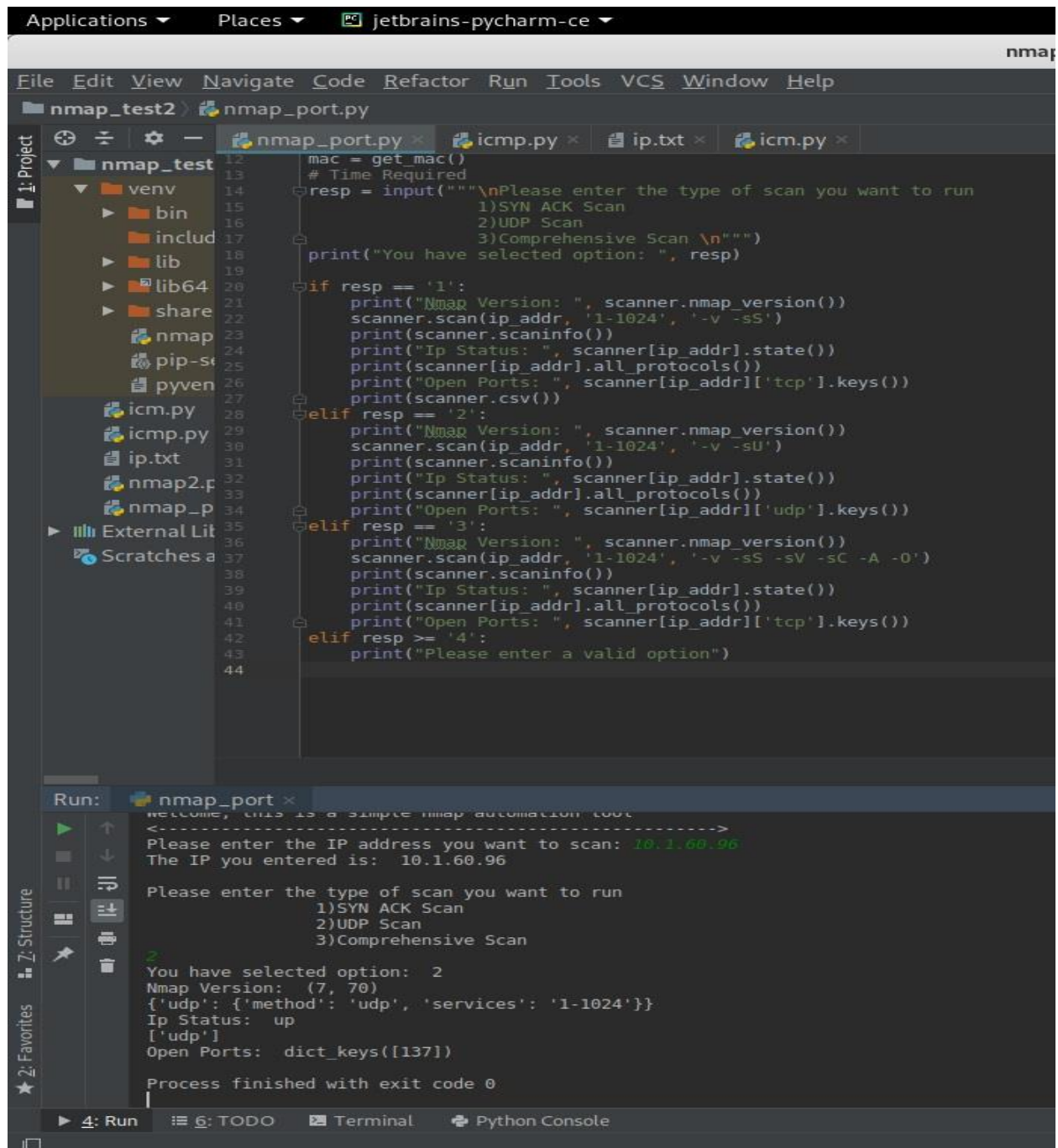
The screenshot displays the PyCharm IDE interface. The main editor window shows the `nmap_port.py` script, which is a Python program designed to perform an Nmap port scan. The script prompts the user to select a scan type (1 for SYN ACK Scan, 2 for UDP Scan, 3 for Comprehensive Scan) and then executes the scan using the `nmap` command-line tool. The output of the scan is printed to the console, showing the Nmap version, IP status, and a list of open ports with their associated services and state.

```
12 mac = get_mac()
13 # Time Required
14 resp = input("\nPlease enter the type of scan you want to run\n")
15 1)SYN ACK Scan
16 2)UDP Scan
17 3)Comprehensive Scan \n""")
18 print("You have selected option: ", resp)
19
20 if resp == '1':
21     print("Nmap Version: ", scanner.nmap_version())
22     scanner.scan(ip_addr, '1-1024', '-v -sS')
23     print(scanner.scaninfo())
24     print("Ip Status: ", scanner[ip_addr].state())
25     print(scanner[ip_addr].all_protocols())
26     print("Open Ports: ", scanner[ip_addr]['tcp'].keys())
27     print(scanner.csv())
28 elif resp == '2':
29     print("Nmap Version: ", scanner.nmap_version())
30     scanner.scan(ip_addr, '1-1024', '-v -sU')
31     print(scanner.scaninfo())
32     print("Ip Status: ", scanner[ip_addr].state())
33     print(scanner[ip_addr].all_protocols())
34     print("Open Ports: ", scanner[ip_addr]['udp'].keys())
35 elif resp == '3':
36     print("Nmap Version: ", scanner.nmap_version())
37     scanner.scan(ip_addr, '1-1024', '-v -sS -sV -sC -A -O')
38     print(scanner.scaninfo())
39     print("Ip Status: ", scanner[ip_addr].state())
40     print(scanner[ip_addr].all_protocols())
41     print("Open Ports: ", scanner[ip_addr]['tcp'].keys())
42 elif resp >= '4':
43     print("Please enter a valid option")
44
```

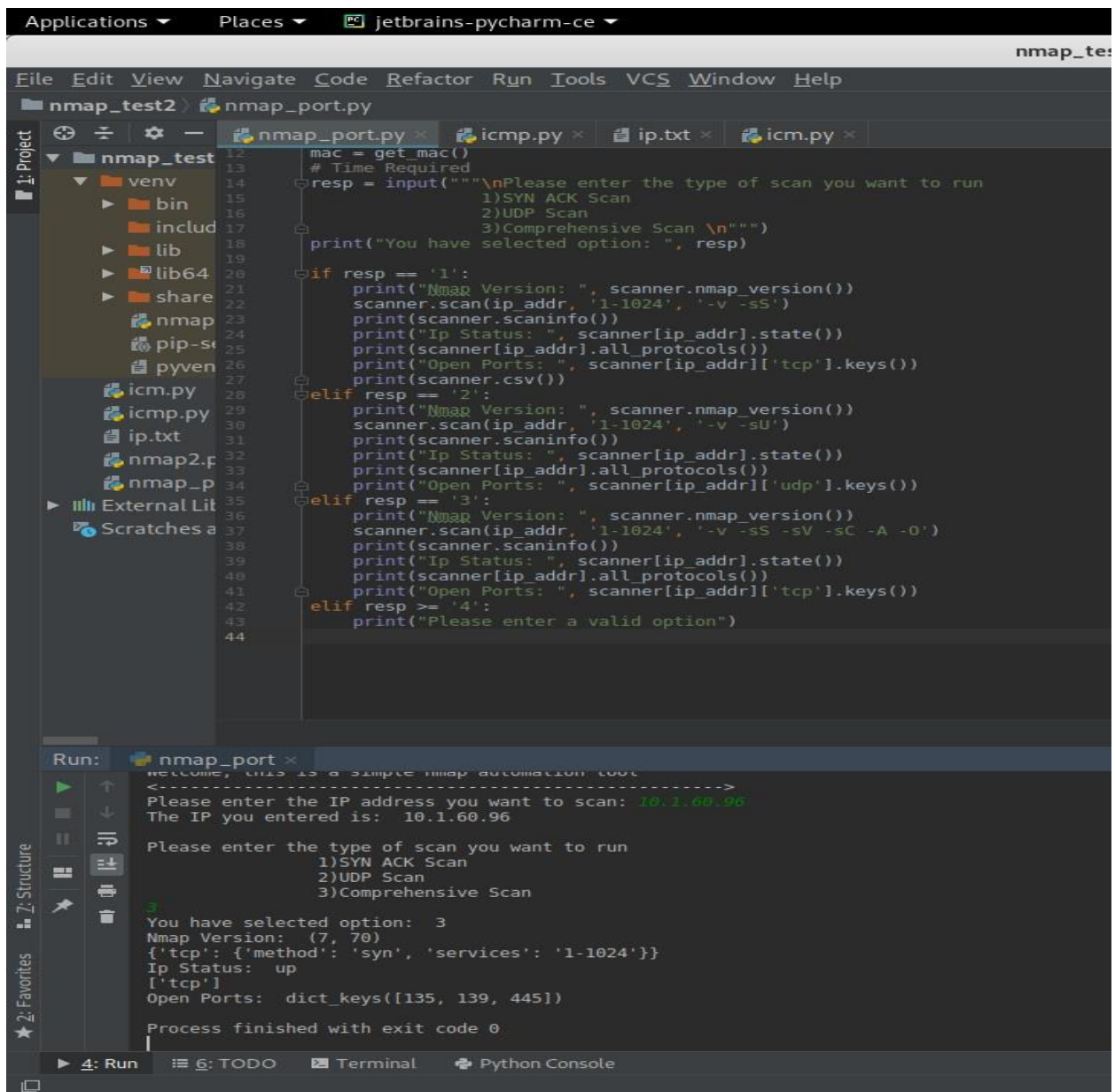
The Run window shows the execution output:

```
Please enter the type of scan you want to run
1)SYN ACK Scan
2)UDP Scan
3)Comprehensive Scan
3
You have selected option: 1
Nmap Version: (7, 70)
{'tcp': {'method': 'syn', 'services': '1-1024'}}
Ip Status: up
['tcp']
Open Ports: dict_keys([135, 139, 445])
host;hostname;hostname_type;protocol;port;name;state;product;extrainfo;reason;version;conf;cpe
10.1.60.96;;;tcp;135;msrpc;open;;;syn-ack;;3;
10.1.60.96;;;tcp;139;netbios-ssn;open;;;syn-ack;;3;
10.1.60.96;;;tcp;445;microsoft-ds;open;;;syn-ack;;3;
Process finished with exit code 0
```

Figure 6.1 NMAP-PORT SCAN

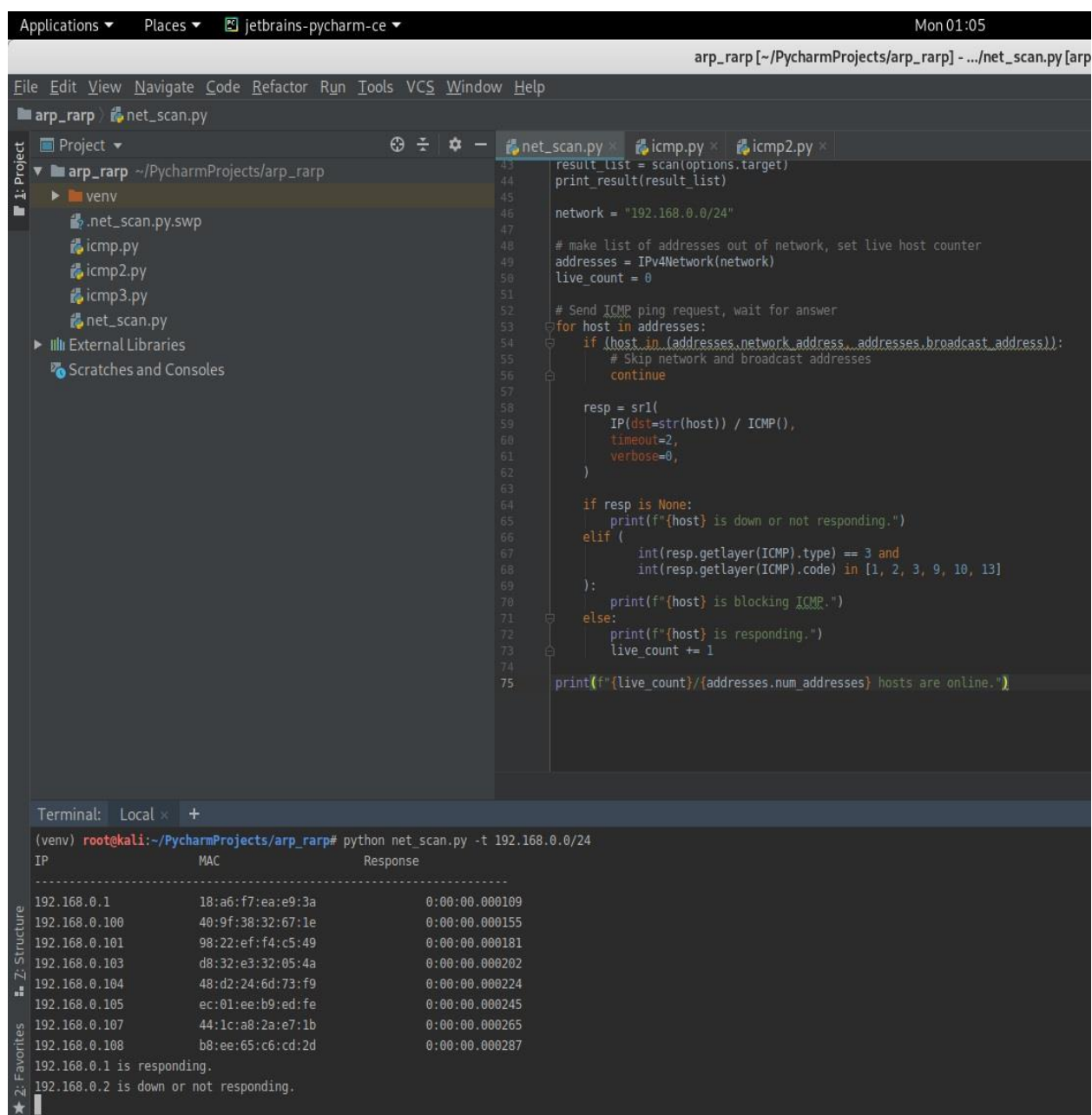


**Figure 6.2** NMAP-PORT SCAN



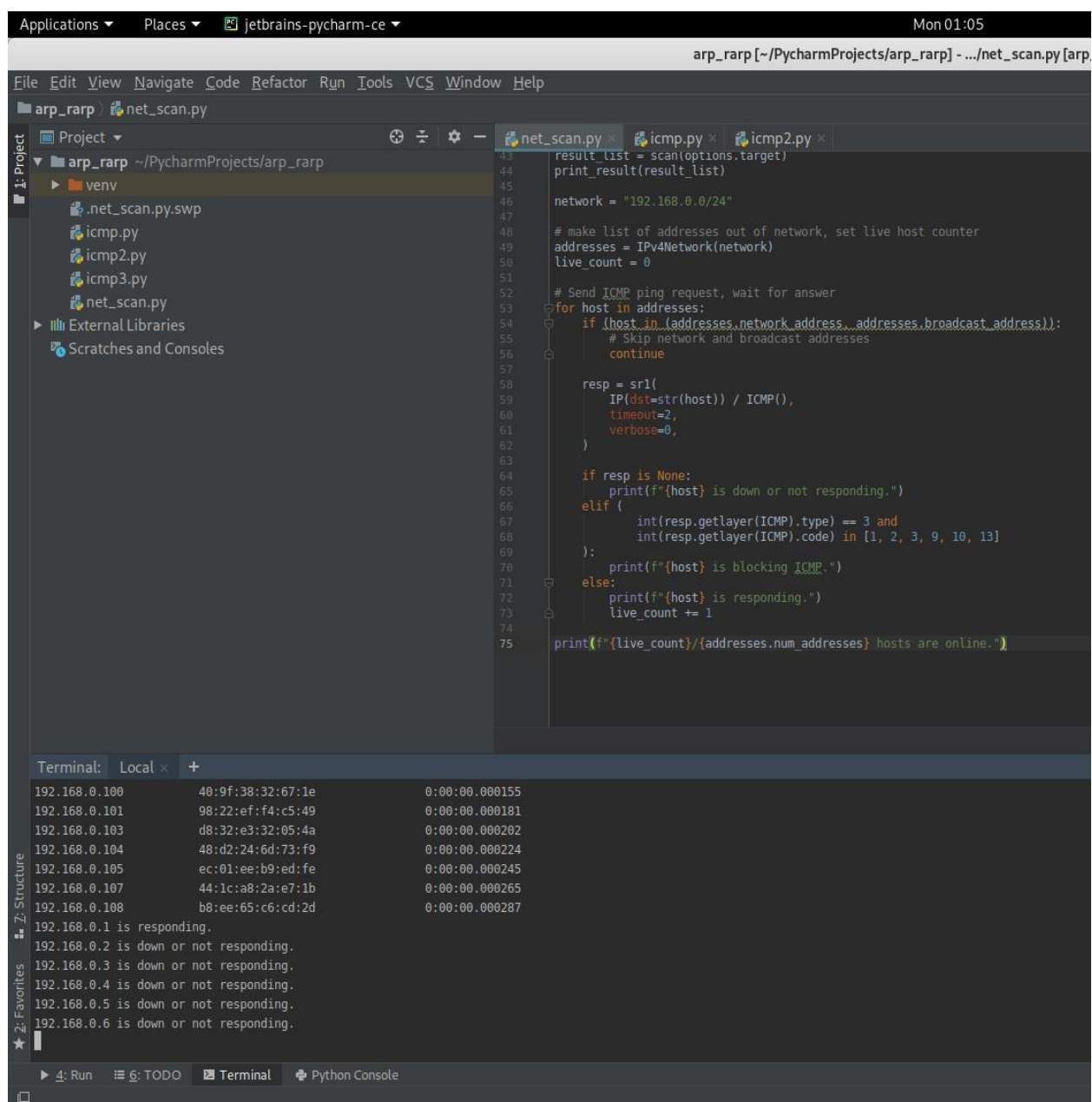
**Figure 6.3** NMAP-PORT SCAN



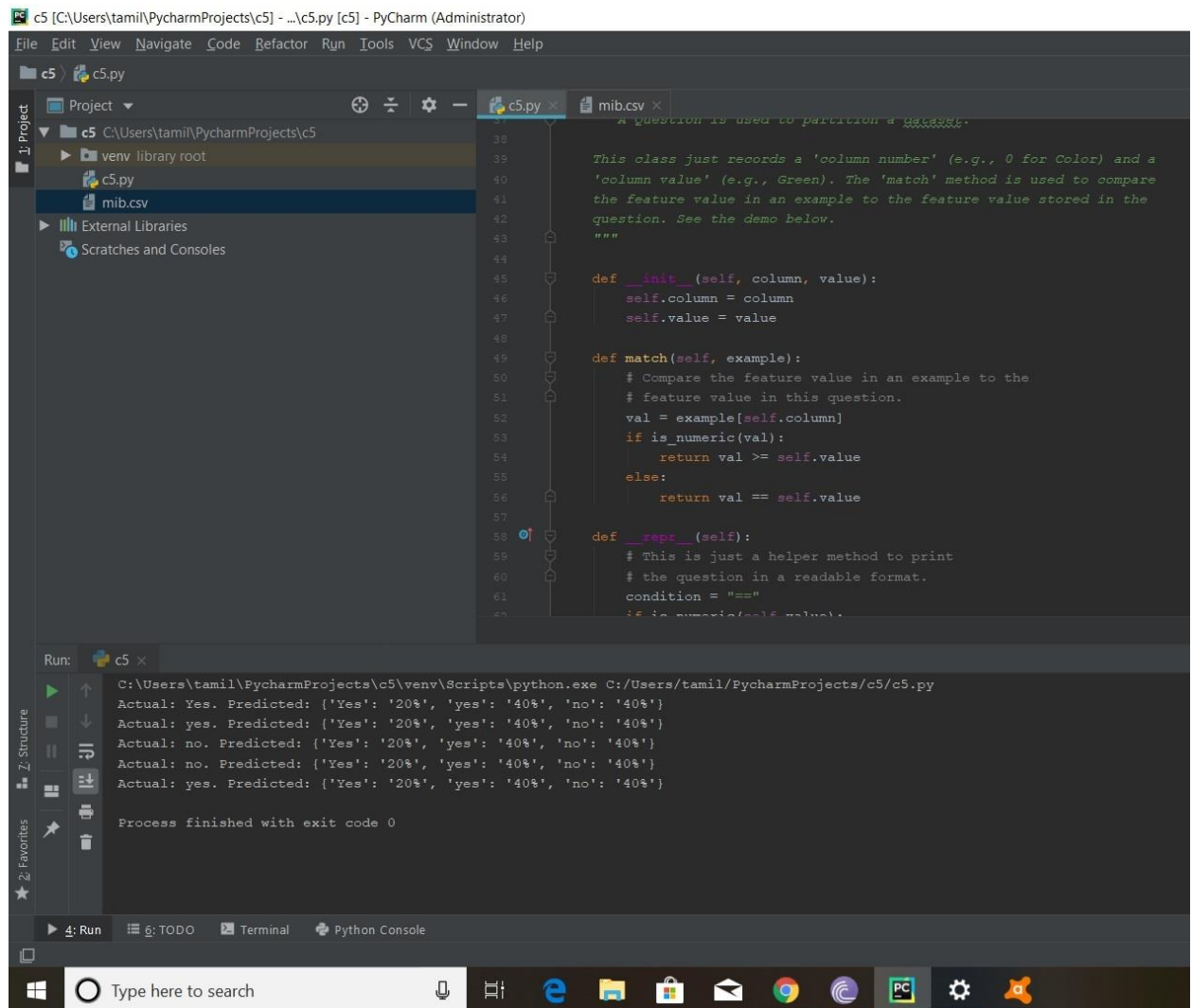


**Figure 6.4** ARP MAC-BINDING

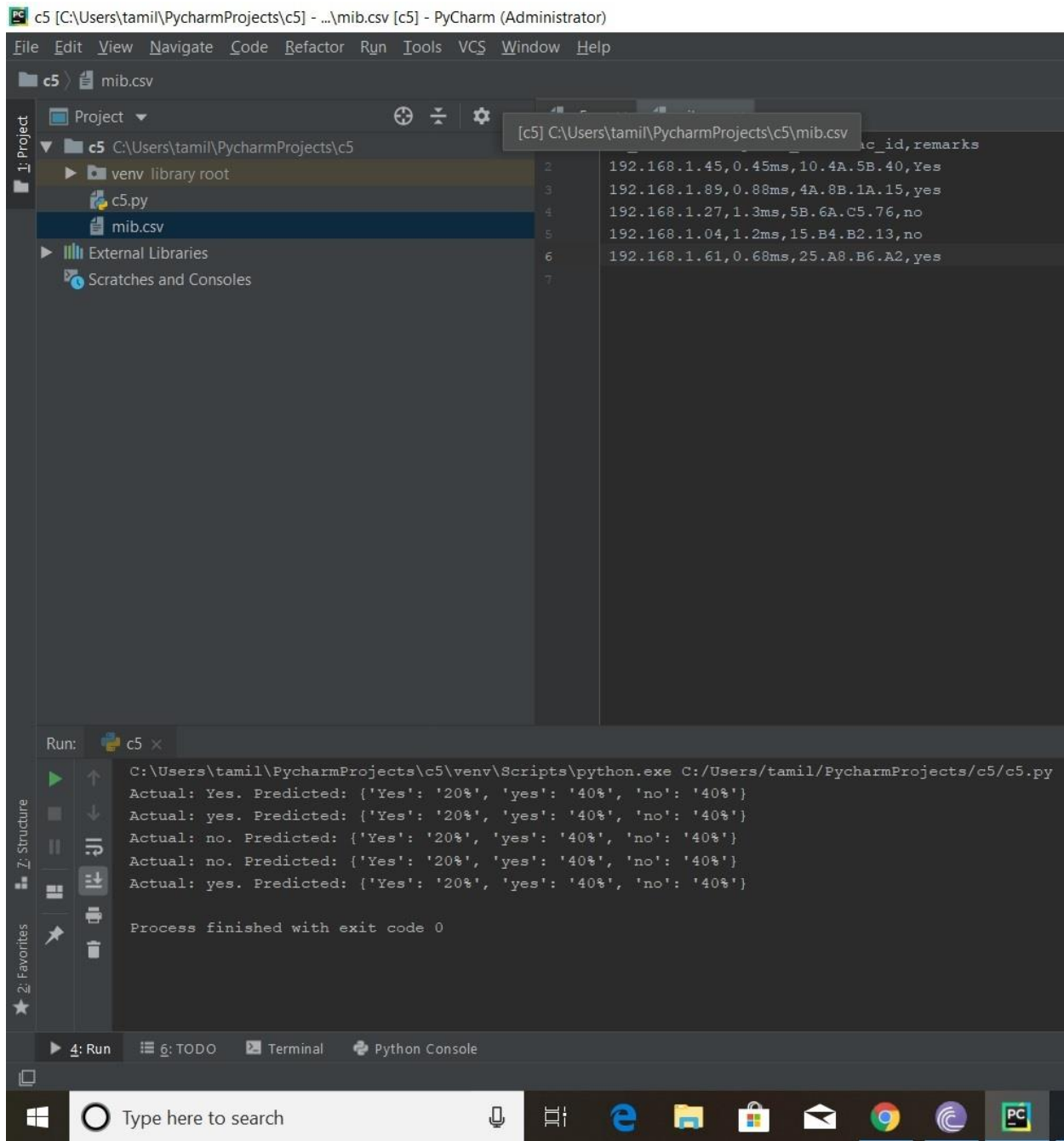




**Figure 6.5** ARP MAC-BINDING



**Figure 6.6 C5.0 ALGORITHM IMPLEMENTATION**



**Figure 6.7 C5.0 ALGORITHM IMPLEMENTATION WITH CSV**

## **CHAPTER 7**

### **CONCLUSION**

Minimizing the intervention of software, an efficient network management and security solutions are modeled. For ensuring the security and making the network management system automatic, a new framework has been proposed, which uses the Machine Learning algorithm to make the system function automatic and securely. The research about the SNMP and IoT which are implemented in this work facilitate an Enterprise by reducing the human work. A partial SNMP model is designed and developed. It will help revolutionizing the industry by its automation technique and the network secured with its AI authentication technology.

### **FUTURE ENHANCEMENT**

A partial SNMP model is designed and developed in this project. In future there is an idea of implementing the full SNMP model in IoT environment. This implementation will result in the fully automated wireless SNMP without using the software and hardware.

## **APPENDICES**

### **PSEUDOCODE FOR C5.0 ALGORITHM:**

- (1) Compute Class Frequency(T);
- (2) if OneClass or FewCases  
    Return a leaf;  
    Create a decision node;
- (3) ForEach Attribute a  
    ComputeGain(a);
- (4) N.test = AttributeWithBestGain;
- (5) If N.test is continuous  
    Find Threshold;
- (6) ForEach T' in the splitting of T
- (7) if T' is Empty  
    Child of N is a leaf  
    Else
- (8) Child of N = FormTree(T');
- (9) Compute Errors of N  
    Return N

### **PSEUDOCODE FOR ARP:**

**BEGIN:**

if (ARP cache contains MAC address) then

Data packet will be delivered directly to the destination host

else

Broadcast ARP Request Frame in the network

if (the source network has destination host) then

Broadcast the ARP Reply Frame

else

```

if (not source itself)
Update the ARP cache
else
Destination host is in other network
if (routing table has entry) then
Broadcast the ARP Request in destination network
else
Update the Routing Table using ARP Frame and recheck
if (the destination network has destination host) then
if (IP and MAC of destination host in ARP Reply is valid) then
Broadcast the ARP Reply Frame
else
Invalid combination
else
if (not source itself)
Update the ARP cache
else
Router will forward the frame to another network
if (the Routing Table contains correct source network address) then
ARP Reply Frame will be broadcasted in the source Network.
if (the MAC address in the frame is same as destination host MAC) then
Deliver the message to the destination host
else
Host not found
if (the source host match found) then
Acknowledge delivered successfully
END: //end of procedure

```

## REFERENCE

- [1] J. Case, R. Mundy, D. Partain, and B. Stewart, "Introduction to version 3 of the internet-standard network management framework," RFC2570, April 1999.
- [2] Isael Koffman, Vincentrie Roman, "'Broadband Wireless Access Solutions Based on OFDM Access in IEEE 802.16." pp.96-103, BEE Comlmications Magazine, April 2002.
- [3] U. Blumenthal and B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) RFC3414, December 2002.
- [4] ZHAO Zhong-hua, Wireless Sensor Network Management Technology COMPUTER SCIENCE[J], vol.38, pp.8-14,2011.
- [5] Li Jianzhong, Gao Hong, Survey on Sensor Network Research JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT [J], vol.45, pp.1-15,2008
- [6] J. Kantorovitch, Z. Shelby, T. Saarinen, and P. Mähönen, "Wireless SNMP," INET conference, June 2000.
- [7] Juntao Liu, Jianwei Niu, Jingjing Liu, Limin Sun, "Management in wireless sensor networks," Computer Science, vol. 34(6), pp. 34-38, 2007.

[8] Chen Ahi, Wang Ruchuan, Sun Lijuan. SNMP-based Management System Model for Wireless Sensor Networks [J]. COMPUTER SCIENCE, vol.34, pp,405-408,2007.

[9] X. Shen, Z. Wang, and Y. Sun, “Wireless sensor networks for industrial applications “in Fifth World Congress on Intelligent Control and Automation, vol.4.Hangzhou, China,2004, pp.3636-3640.

[10] K. McCloghrie, and M. Rose “Management Information Base for network management of TCP/IP based internets. MIB||”,RFC1213,March1991.