and online in real time. According to offline analysis, precision and recall for sliding window algorithm were 60%, while for neural network precision amounted to 30% and recall to 38%. However, since sliding window algorithm is easier for implementation and showed better performance, it was chosen to be implemented on M2M device for online analysis.

[4] Dragos Mocrii, Yuxiang Chen, Petr Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security", Internet of Things 1–2 (2018) 81–98.

Due to costs, complexity, and lack of awareness among the general public, home automation is not a mainstream choice. Lack of interoperability between devices, high complexity of setting up a smart home network and absence of unified interfaces for device management are issues that have to be solved. Security and privacy is an important factor for successful dispersion of smart homes. Along with developing implementation platforms for tasks necessary for smart home operation, it is required to make them well integrated systems that can respond to occupant needs and environmental events, and evolve with changing priorities of the users.

[5] Shubhangi K. Gawali, Mukund K. Deshmukh, "Energy Anatomy in IoT Technologies", 2018 5th International Conference on Power and Energy Systems Engineering, CPESE 2018, 19–21 September 2018, Nagoya, Japan.

To establish communication between devices, IoT exposes many challenges such as energy, power constraints, noise, interference, etc. Some technologies such as, RFID, Networking and Communication, WSN, RTS, Machine to Machine interaction (M2M), etc., can be used to connect all objects through internet for remote sensing and control. In an attempt to address the challenges, several barriers have slowed down the development of IoT, one of which includes the transition from IPv4 to IPv6 and developing energy sources for every sensor used. Technologies considered with regard to energy anatomy would be RFID for providing the unique identifier to objects through tags, making Networking and Communication autonomous, WSN for low profile, low power, energy efficient and self-sustainable sensor networks, RTS, and Cloud Computing to overcome limitations due to lack of software, firmware, memory, hardware and data processing capability.

CHAPTER 3

SYSTEM ARCHITECTURE

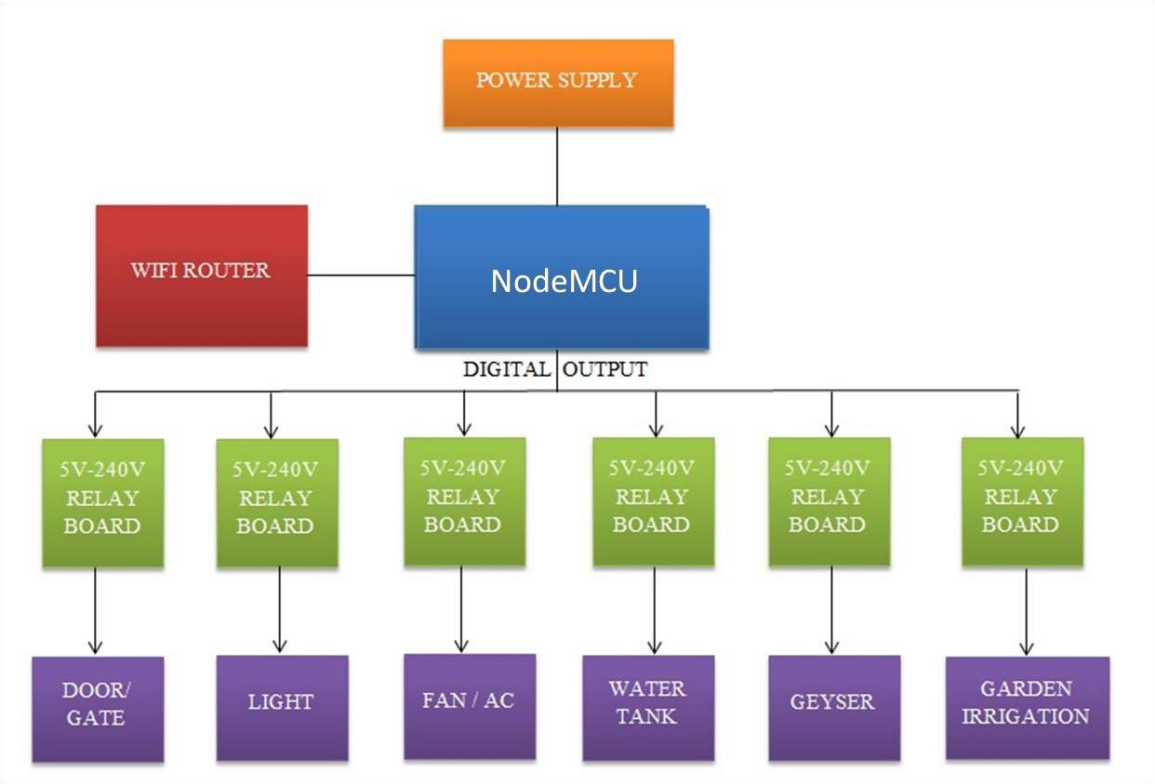

Figure 3.1: System Architecture

The figure represents the architecture of the proposed system. The master device used here is NodeMCU, which is an open source IoT platform. It includes firmware which runs on the ESP8266 WiFi-SoC from Espressif Systems, and hardware which is based on the ESP-12 module. The modules such as Door/Gate, Light, Fan/AC, Water level Control, Geyser and Garden Irrigation are connected to the NodeMCU and the communication is wireless via WiFi router. The master device is connected to these modules using an electromagnetic switch called relay, which is used to control high voltage circuits with the help of low voltage signals. This plays a very important role in providing safety critical logic. In other words, relay is an electromagnetic switch operated by a relatively small electric current. Relay is connected to each and every appliance so that the failure of any appliance does not affect any other component in the system.

CHAPTER 4

TECHNOLOGIES USED

4.1 WiFi Technology

Figure 4.1: WiFi Technology

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi is probably the most exploited wireless technology nowadays. Wi-Fi is a popular wireless networking technology. Wi-Fi stands for “wireless fidelity”. The Wi-Fi was invented by NCR corporation/AT&T in Netherlands in 1991. By using this technology we can exchange the information between two or more devices.

Working Principle:

Wi-Fi is a high speed internet connection and network connection without use of any cables or wires. The wireless network is operating three essential elements that are radio signals, antenna and router. The radio waves are keys which make the Wi-Fi networking possible. The computers and cell phones are ready with Wi-Fi cards. Wi-Fi compatibility has been using a new creation to constituent within the ground connected with community network. Wi-Fi allows the person in order to get access to web any place in the actual provided area.

The radio signals are transmitted from antennas and routers that signals are picked up by Wi-Fi receivers, such as computers and cell phones that are ready with Wi-Fi cards. Whenever the computer receives the signals within the range of 100-150 feet for router it connect the device immediately. The range of the Wi-Fi is depends upon the

environment, indoor or outdoor ranges. The Wi-Fi cards will read the signals and create an internet connection between user and network. The speed of the device using Wi-Fi connection increases as the computer gets closer to the main source and speed is decreases computer gets further away.

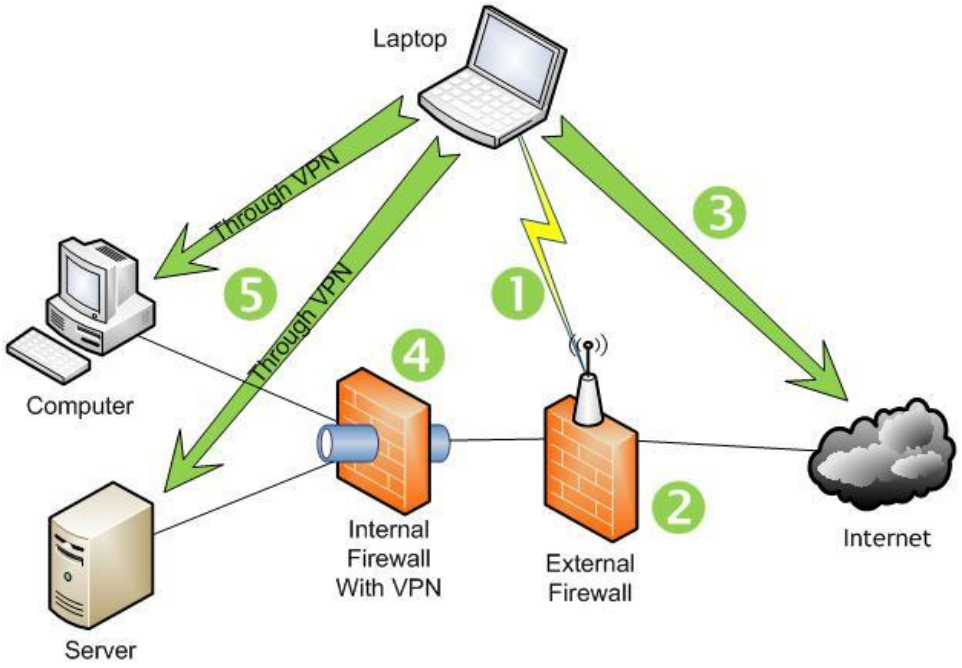

Figure 4.2: Wi-Fi Connections

Security

Security is impartment element in the Wi-Fi technology. All routers have a web page that users can connect for configuring the Wi-Fi security. And turn on WEP (Wire Equivalence Privacy) and enter a password and remember this password. Next time when laptop is connected, Wi-Fi router will ask to enter the connection password and the password can be entered.

4.2 RFID Technology

RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels are captured by a reader that stores the data in a database. In other words, RFID is a technology based identification system which helps identifying objects just through the tags attached to them, without requiring any light of sight between the tags and the tag reader. All that is needed is radio communication between the tag and the reader. Radio-Frequency