CHAPTER TWO

LITERATURE REVIEW

2.1 Overview of Relevant Technology

Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver and transmitter. When triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data, usually an identifying inventory number, back to the reader. This number can be used to track inventory goods.

Passive tags are powered by energy from the RFID reader's interrogating radio waves. Active tags are powered by a battery and thus can be read at a greater range from the RFID reader, up to hundreds of meters.

Unlike a barcode, the tag does not need to be within the line of sight of the reader, so it may be embedded in the tracked object. RFID is one method of automatic identification and data capture (AIDC).

RFID tags are used in many industries. For example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line, RFID-tagged pharmaceuticals can be tracked through warehouses, and implanting RFID microchips in livestock and pets enables positive identification of animals. Tags can also be used in shops to expedite checkout, and to prevent theft by customers and employees.

Since RFID tags can be attached to physical money, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns. These concerns resulted in standard specifications development addressing privacy and security issues.

The NodeMCU is a low-cost open source IoT platform. Its initial versions included firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems. The firmware uses the Lua scripting language and is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson and SPIFFS.

ESP8266 is a highly integrated chip designed for the needs of a new connected world. It offers a complete and self-contained Wi-Fi networking solution, allowing it to either host the application or to offload all Wi-Fi networking functions from another application processor. This module comes with a built in USB connector and a rich assortment of pin-outs. With a micro USB cable, you can connect the NodeMCU devkit to your laptop and flash it without any trouble, just like Arduino. It is also immediately breadboard friendly.

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems began production of the ESP8266. NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub. Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9.

In the summer of 2015, the original creators abandoned the firmware project and a group of independent contributors took over. By the summer of 2016 the NodeMCU included more than 40 different modules.

2.2 Review of Related Work

For the study of an existing system or technology, Take RFID Door Lock Access Control System as a case of study

This is a popular project for Arduino hobbyists. RFID door lock systems are very common for access control, as they provide a reliable, consistent experience with trackable data. Unlike other forms of traditional access control such as swipe cards,

RFID locking systems are contactless, meaning that the credential doesn't have to touch the reader for it to work.

Similar to a barcode reader, RFID readers work by sending and receiving data, but instead of having to scan a code, the data is transmitted over radio frequencies. An RFID door locking system requires RFID tags, antennas, an RFID reader, and a transceiver in order to function as a complete system.

In an RFID door lock access control system, the user's credential (usually a keycard or fob with an RFID chip) contains unique identifying information called a tag. When the user comes within proximity of a reader, the reader's signal locates the information stored on the user's RFID tag, and sends it through antennas and transceivers to authorize the tag in the access control system. Once read, the system will either accept or deny the request to unlock the door. Data from an RFID-enabled system is automatically stored, making it possible to track entry activity in an access control system.

2.3 Summary of the Problem of Existing Systems

1. The machine is very rigid. The keys are stored directly on the hardware.
2. There are no means to monitor how the system is being used, microcontrollers aren't known for having much storage memory
3. The data is not persistent, in case of a power outage all data is lost.
4. It is very difficult to update/maintain. Any required changes mean the lock has to be dismantled down to the microcontroller

2.4 Summary

Microcontroller/IoT technology can be used to build powerful applications. The power of the internet when combined with this brings about interesting results. This

study will make use of an online web app and an RFID scanning machine. When a card/tag is presented to it, operations/communication occur between the server and the machine, both of them covering each other’s weaknesses.