

Security Issues and Solution-Home Automation using RFID

¹Mayuri Mundada, ²Radhika Zanwar

^{1,2}MCA III, Department of Research and PG studies in Science & Management, Vidyabharti Mahavidyalya, Amravati, India

Abstract - IOT has become a buzzword nowadays. It is a pretty simple concept which means taking all things in the world and connecting them to the internet. It is vastly used in smart homes, manufacturing, agriculture and many other industries. Now for these items to communicate with each other the devices should have a unique identification. Unique identification is the foremost requirement in IOT. RFID technology helps in solving these identification issues an object around us. The system will help in reducing the possibilities as well as manual operations.

Keywords: RFID, RFID Tags, RFID Reader, Antenna, Security.

I. INTRODUCTION

RFID (Radio Frequency Identification) is an important technology to implement the internet of things. It is an automatic technology. "RFID is the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked". It also helps the machine to identify objects, record metadata or control individual targets through radio waves. The functionality of RFID is close to bar-coding, the digital data encoded in RFID tag are captured and stored in the database through a tag. RFID is used for security purposes for many years. Based on nature off RFID tags the existing RFID protocols primarily focus on "Tag Identification".

II. COMPONENTS AND WORKING OF RFID

RFID consists of some group of technologies which is known as AIDC. AIDC stands for Automatic Identification and Data Capture. Radio waves are utilized by RFID to determine the object, collect all the data related to the specific objects and save the data in the computer systems with little or no intervention of humans. Basically, the RFID systems consist of three major components:

1. RFID Tag
2. RFID Reader
3. An Antenna

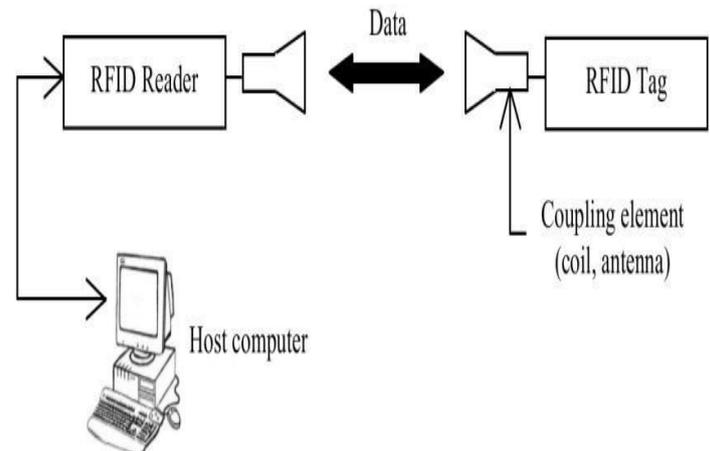


Figure 1: Components of RFID

2.1 RFID Tags

There exist multiple types of RFID tags that can be distinguished by shapes, sizes and unique capabilities. They are also called as Transponder. Tags are attached to any object so that it could be determined easily.

There are two types of RFID tags Active tags and Passive tags. Active are those tags that are fully or partially charged and can communicate with other tags. Whereas passive tags are those tags which do not require battery or any power source, they get charged by the tag reader.

2.2 RFID Reader

The Reader is also called a transmitter or receiver. The role of the reader is to activate the tags, arrange the sequence with the tags and then transmit the data between the software and tags. The RFID Reader is also known as the term interrogator.

2.3 An Antenna

Data can be transmitted to the RFID reader by an antenna.

There is a unique identity code assign to each RFID tag. RFID reader produces a low-level radio frequency through which the tag gets charged. Reader requests a tag and tag give a response to it and declare its presence by transmitting its unique identify code. The code is further decoded by the

reader and passed to the application. For this transmission, it uses middleware which acts as an interface between the reader and an RFID application system.

The system will search and match the code with information which was previously stored in our database. After this complete process the authorization and access is granted or refused.

III. APPLICATION OF RFID

RFID has become very popular now a day as it is an easy technology to implement.

- Payments
- Access Control
- Logistics
- Identification
- Asset management
- Home automation
- Product Tracking

IV. RFID SECURITY THREATS

Like various security devices and their mechanisms. RFID has some flaws that one faces while using RFID. RFID has some issues that should be addressed before the deployment of RFID for its efficient working.

4.1 RFID Counterfeiting

Basic tags of RFID do not use any encryption mechanism that the reason why they can counterfeit so easily In supply chain management system, attackers can misuse the tags, And modify the information which is already saved in the tag so that can get the access to it and to become the authenticated user of the specific product.

4.2 RFID Sniffing

To get the information from the identity tag RFID reader sends to request to the RFID tag. All the information which is sent by the tag is first read by the Reader. As soon as the reader read the information compares it with the data which is stored in the database. Some tags do not have a way to differentiate between the request which is sent by the valid reader and the fake reader. In this context, the attacker can use his own reader for his own purpose to read the specific tag.

4.3 Tracking

An attacker can read the information which is received by the RFID tag and can easily track any person or object. While attaching any tag to any object be aware of the fact that the attacker can identify and track your object anytime and

anywhere even though you have applied any secret message to communicate between RFID tag and RFID reader. Mobile robots can also be used by an attacker to track the location.

4.4 Denial of Services

When a reader request for particular information to the tag, it receive in identification code and compares it with the existing Id in the backend server or database. When the Denial of Services attacks takes place, the tags fail to verify its own identity and as a result, the specific service gets interrupted.

4.5 Spoofing

In this attack, an attacker frame himself as an authorized user to the database or any services. If the attacker gets access to the RFID data successfully with his spoofed credentials he can do anything with details, Attacker can change the id of the tag or reader, give the response to invalid services and can denying normal services and cam denying normal services.

4.6 Replay Attacks

An attacker can stop the communication flow between tags and the reader and can record the communication between them.

4.7 Physical Attacks

This attack can happen physically in the number of ways in this attack, the attacker obtains the tag information physically and alters it. Here the attacker can remove the tag attached with the object, by doing this the RFID object remains unrecognized.

V. PROPOSED SYSTEM

The architecture of the proposed system consists of an Arduino Board an Ultrasonic Sensor, RFID tag and RFID reader the idea behind "HOME AND HOSED" Is that we can provide secured and a smart way.

Working of model:

- RFID tags will be given family members with unique id code.
- The RFID reader will be installed on the Arduino board near the door.
- The reader will detect the RFID tags in its vicinity and will check its authenticity.
- If an unauthorized RFID tries to open the door the alarm and alert message will be delivered to family members.
- When an authenticated RFID is sensed within the vicinity of the RFID reader then it will provide

necessary instruction to an ultrasonic sensor through Arduino to check whether the distance of tags to open/close the door.

- This will be checked by the mobile application to verify both the IDs that are door as well as the mobile application.

VI. FLOW CHART

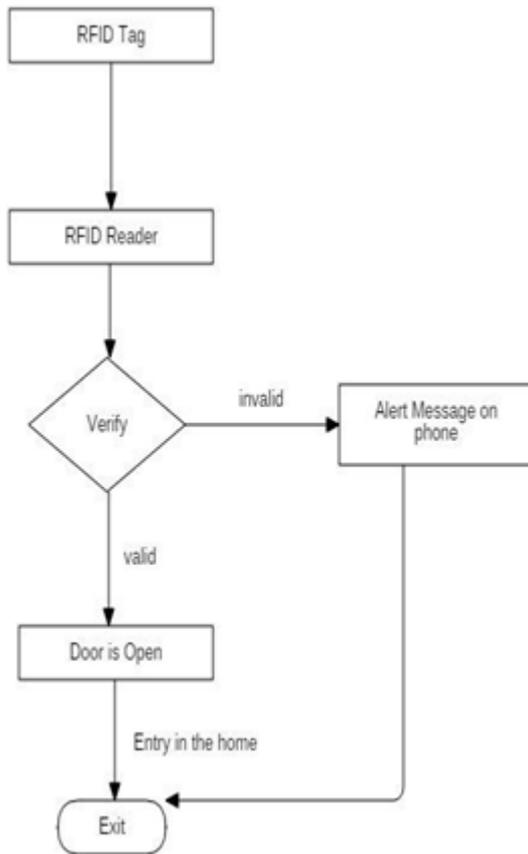


Figure 2: Flow Chart for Home Automation System

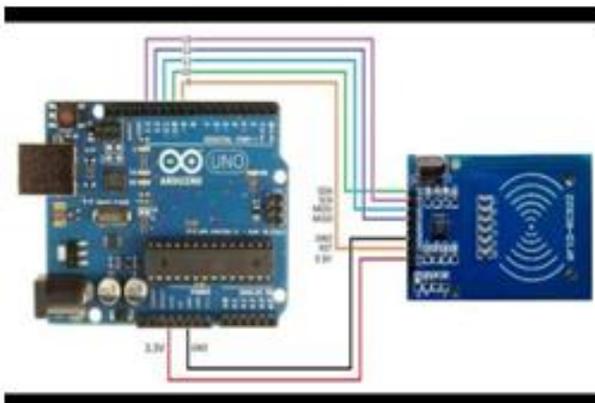


Figure 3: Arduino Connected to RFID

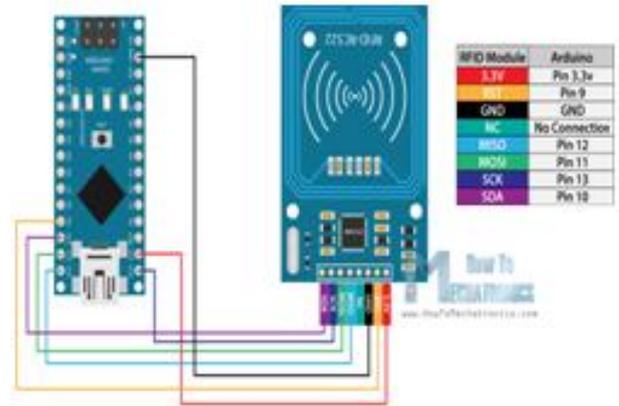


Figure 4: Arduino Connected to Ultrasonic Sensor



Figure 5: Home Automation using RFID

VII. CONCLUSION

As all information leads to a conclusion, home automation using RFID we can say that it will reduce manual operations and will provide theft security. This mechanism does not require any human intervention and it helps to reduce human overhead. The home automation using the Internet of things has been experimentally proven to work satisfactorily by connecting simple appliances to it and the appliances were successfully controlled remotely through the internet.

REFERENCES

- www.infosec.gov.hk/english/technical/files/rfid.pdf
- <https://securitywing.com/top-10-rfid-security-concerns-threats>
- <https://www.elprocus.com/home-automation-systems-applications/>
- <https://circuitdigest.com/microcontroller-projects/rfid-based-security-system>
- <https://electronicsforu.com/electronics-projects/hardware-diy/rfid-based-security-system>
- BCC Research, "Sensors: Technologies and global markets,"

- [7] Bill N. Schilit, Norman Adams, and Roy Want, "Context-Aware Computing Application. International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 3, September 2013.
- [9] Duc,D.N.,etal.OpenissuesinRFIDsecurity Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for. 2009. *IEEE*.

Citation of this Article:

Mayuri Mundada, Radhika Zanwar, "Security Issues and Solution-Home Automation using RFID" Published in *International Research Journal of Innovations in Engineering and Technology (IRJIET)*, Volume 3, Issue 12, pp 14-17, December 2019.
