International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

RFID Security in IoT

Dr. Gayathri Rajakumaran[1], Shola Usharani

Vellore Institute of Technology, Chennai, India
[1]*gayathri.r[at]vit.ac.in*
[2]*sholausha.rani[at]vit.ac.in*

Abstract: ***The Internet of things involves high risk in terms of security and privacy act because of its usage through many public networks. ManyIoT applications using RFID from home to warehouse. Smart Ration Card is one of the applications used in order to prevent corruption and malpractices in the distributed ration system. RFID tag is used for providing unique identification for ration card. Once the card is identified the authentication process is done by Generating the OTP. After the authentication is done the database is updated to reduce human efforts. This RFID card may be affected by security threat as there is no security module integrated with RFID cards. In this paper various security threats are identified to provide security of the RFID based system. Integrity and data protection are the main concern for security and to prevent it we can take consider measures. Cryptography is one of thetechniques that confirms secure transaction between sender and receiver for better security.To protect Smart Ration Card using RFID in IoT used ECC which is cheap, secure and fast. ECC is integrated with RFID system in order to protect the data from malicious attack***

Keywords: IoT, RFID, Raspberry Pi, DOS, ECC

1. Introduction to IOT

Internet of things is basically how the physical devices like a small phone to aero plane are connected to internet and help in collecting the data is also used to share the data [2]. Nowadays we use a computer chip that makes a wireless connection. Any physical object that comes under IOT is connected to internet for communication or for sharing of data. For example, a simple toy to a self-driving car can be created using IOT. IOT helps in creating a network connection for such devices that could never have a connection normally and they can work without human instructions [12].

The devices that have built in sensor are connected to IOT. It gives us information to help in increasing the market value of our products by connecting them and analyzing their performance. One of the examples for IOT is automatic alarm clock. Suppose due to heavy rainfall the train route gets canceled and for going to the college we need to get up more early so that the student can go to college from their personal vehicle. IOT plays an important role in it by seeing the weather and adjusting the time of waking up accordingly. And automatic coffee maker can even make the coffee accordingly.

RFID is one of the large open door's technologies in the world of data innovation, which will change the communication extensively and profoundly. RFID is frequently considered an essential for the IOT. In the event that all objects of day-to-day existence were outfitted with radio tags, they could be distinguished and stocked by PCs [5].RFID has 3 components- RFID tag, RFID reader and the application system [5]

RFID Tag – it is also known as transponders /transmitter/ responder. Used to identify or count. It can be active or passive. The purpose is to store data and it has antenna that is coiled and microchip. Active tags are fully/partially powered and have communication with other tag. Tags that are Passive are powered by tag reader.

RFID Reader – it is also known as transmitter/ receiver/ transceiver. It consists of control unit and radio frequency interface (RFI) module. It is used to activate and structure the communication sequence of tags and it is used to transfer information between the tags and the software of application.

Application System – which is also known as data processing system it can be either a database or application. It initiates all tag and reader activities.

IoT consists of four basic layers perception, network, middleware, and the application layer. The perception layer is responsible for collecting data and its collaboration. The network layer has two layers inside its access and internet so one of its sublayers collects the data and another sends it to the next layer respectively. Middleware is used for data collection and its filtering and transformation. And the last layer that is application layer uses the data to provide service to the user. For Security threats in different layers which consists of various technology involved in it. [2].

2. Literature Review

1) Indian public distributed system takes data from ration card. The distribution of Ration is done by central and state government. Some criteria are made for families below poverty line and above poverty line. Due to no record the seller keeps the fake ration card and take more ration and sell it in higher rate or people are not aware of fixed rate price and the seller sell it in higher price. It uses RFID tag and IoT in digitalizing ration card. For application, Cloud computing is used as storage database and OTP service, MongoDB is used to create database and save it in JSON format. [3]

2) RFID uses electromagnetic field it is a wireless communication and core technology. IoT service is provided by providing location information and identification information and is exchanged automatically through internet. RFID includes HF RFID technology used in banking and hospital application. It can also be used for

authentication and tracking of location. RFID technology is classified into three types active, passive and semi-active. To the object RF tag is attached and includes EPC code. While using a RFID service application is run then RFID reader activation is done and Information of EPC is acquired from the RFID tag and then goes to communication network through which it goes to application server then goes to user terminal and then displays it on screen and checks the authentication by checking Password if it is matched from the tag then response is displayed [6].

3) Tracking for a particular shipment is much needed in financial and logistic system. It reduces expenses as the particular order can be tracked easily. It reduces the delay in the package that increase the good experience of the customers. RFID uses electromagnetic field to track the object using the tags in it and the objects contains the electronic information in it. For this architecture Passive RFID tag is used that collects energy form the readers that are near to it and it is a non- volatile. It communicates with the nearby tags in logistic chain and tell the location of the shipment it is created by sending the radio link with the unique ID. The module incorporates RFID RC522 with Raspberry Pi utilizing SPI convention [4].

4) IoT establish a connection between people and things through any path/network. So, it provides less human error and more intelligence network. Smart home system that is controlled by Internet that includes fire alert, turning off appliances or opening/ Closing of gates. Localization in environments or indoor domains act as an important role in IoT. RFID is useful to identify movement of object through wireless communication channel. RFID has tags which captures the information and readers which takes information from tags and do further processing and back-end servers. Two different ways by which readers can be introduced – static place where tags are joined to individual or item and second portable place where consistent label position is recognized by reader. RFID procedures for limitation are – Triangulations (distance estimations), Proximity and Scene Analysis. [1]

3. RFID system using IOT Technology

Smart ration card system which will reduce the malpractice that are done by shopkeeper. For application Cloud computing is used as storage database and OTP service, MongoDB is used to create database and saved in JSON format. So, by using smart ration card it needs to be scanned in reader when authentication is done and OTP is generated with details of item and its quality. A text message is sent with item listed and at end of transaction database of government is updated [3].

3.1 Block Diagram

Block diagram showed in Figure 1 describes that WI-FI connects the AWS component through internet. Transmitting pin of Ardunio (At Mega 2560) processor is connected to WIFI shield. To Ardunio with LCD is used to display the content, A keyboard that is 4*4 is connected to enter input. So, by swapping a card the RFID reader will generate the hex code of 12 bit. [3]. The data processed from the processor is updated into Data base through AWS cloud system. The user remotely connected uses the web application for accessing the RFID data.

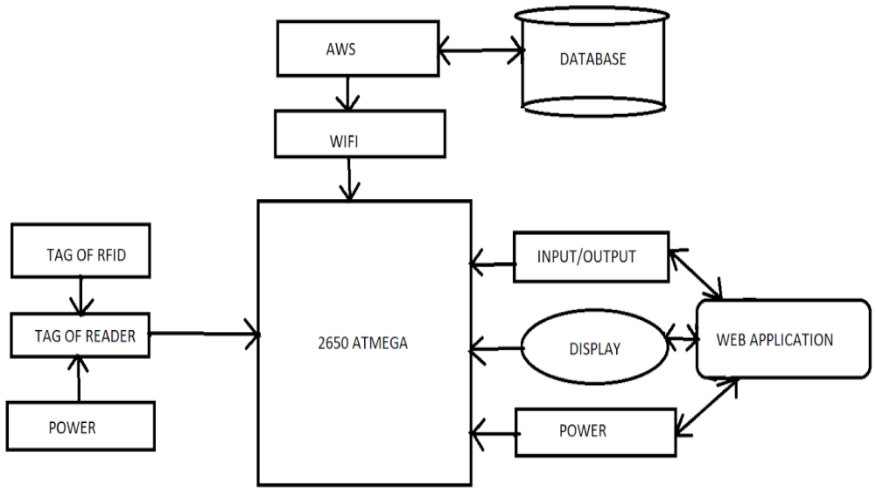

Figure 1: Block diagram for smart ration card system using RFID technology

Flow chart shown in Figure 2 describes the flow for the system. The user will swipe his RFID tag, the reader reads the tag, then itwill generate a hex code and is given to Arduino. Arduino match the code with database entry of the tag through WI-FI module. The authentication process is verified by generating the OTP to the user. So, this idea reduces the malpractice and daily check can be there by government authorities [3]. If the authentication is not matched the user will be prompted as card invalid. Otherwise, once the code matches with database entry the data will be displayed. In the display screen the details of quantity for the user will be shown, so user has the choice to confirm the purchase or cancel the transaction. the transaction details are also updated into the database for further processing.

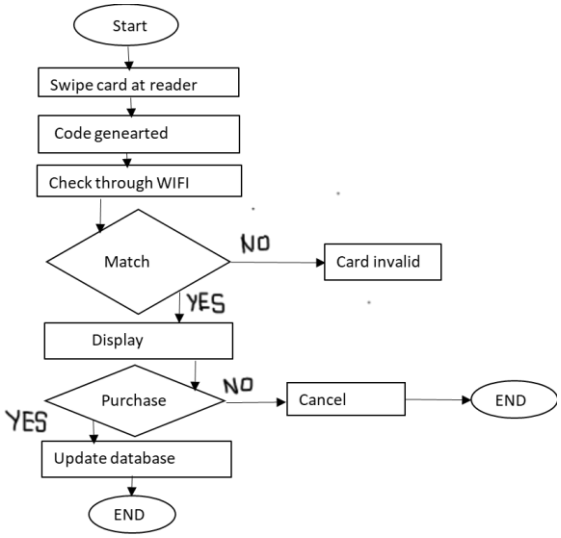

Figure 2: Flow Chart for smart ration card using RFID

Besides, RFID is considered to be the trendy technology usedin many countries. The use of RFID technology in several applications includes supply chain, healthcare, transportation, education and many other fields have significant advantages includes the flexible way of deployment with low cost, the possibility of integration and cooperation with Wireless Sensor Network nodes. However, despite its numerous advantages, RFID technology still brings out many challenges including technical problems, customer privacy issues, coexistence of heterogeneous RFID standards [16] and more importantly security and privacy concerns. Several types of attacks can target the RFID system depending on each part is more vulnerable to the attacker. For example, the modification of the data, Cloning technique, and impersonation can be applied at level tags, whereas the reverse engineering, Eavesdropping Side Channel Attacks can affect the communication between backend servers, readers and tags. From the literature survey some of important security threats in terms of RFID is listed in the given table 1. The solution for each attack is shown.

Security Issues with RFID Technology

Table 1: Comparison of Security threats and its solution [12][17]

Security threat	Description about attack	Solution
MitM (Man in the middle)	it is attack where hacker attack the communication channel. The attacker acts as a sender. Example – When needed a temperature for a machinery wrong information can lead to lot of damage.	Using digital certificates for things Using digital certificates for VPN For migrating attack use GlobalSign solution
Eavesdropping	Where a fake reader is used by attacker which in turn helps attacker to get information that is transferred in original communication	Authentication, Monitoring of Network, Encryption, Awareness and security best practices
DOS (Denial of Service)	his attack aims to shut down the system or network. It targets the big organization.	By preventing from spoofing and Protect endpoint
Spoofing	attack in which an attacker pretends to be an organization or person from trusted source and send mail by which they can collect sensitive data.	Use smart tools like spam filter and Use packet filtering to avoid Ip spoofing.
Malware attack	Malicious attack where attacker can have access to victim system and perform actions.	Have antivirus, Update system, don't click on any link without trust and Download app from trusted organization.

4. Asymmetric Algorithm for RFID Security Threats

Asymmetric algorithm mainly focuses on public key generation. There are two thing public and private keys associated with it one use for encryption and other use for decryption. From the literature survey identified the following security algorithms.

4.1 Elleptic Curve Cryptography (ECC)

ECC is Key-primarily based method for encrypting facts. It basically focuses on pairs of public and private keys for decryption and encryption of net visitors. It is Smaller, faster, and more efficient.

4.2 RSA (Rivest-Shamir-Adleman)

RSA is based on mathematics modulo huge numbers. It can be sluggish in constraining environments. Reducing modules in modular exponentiation is a method to speed up the RSA decryption. The safety of RSA comes from integer to find. Generation of random top numbers offers the set of rules greater energy and performance.

4.3 Elgamal Cryptosystem

The El-Gamal set of rules is a public key cryptosystem based totally at the discrete logarithm hassle. It includes the encryption and signature algorithms. ElGamal set of rules is finished in 3 elements: Key era for public keys and personal key, encryption for original plaintext message to achieve cipher text and Decryption for cipher text to generate proper plaintext

5. Proposed Model

The existing system consists of RFID tags and readers that will help in communicating the data from the database when the card is scanned. Through the reader and with the web application all the data will be displayed with the correct amount of price and products allocated to the registered person. The site will contain the details of person identity, personal detail and card details that need to be protected in order to maintain the integrity of the system. The security threats that effect integrity would be solved using different prevention methods and algorithms. The related algorithms are discussed in the previous section under table2. Based on the integrity need to the exiting sytem the related detailed block diagram is shown in Figure 3. As shown in the figure

3 once the user is authenticated from the server the details of RFID card details are scanned. The reader send the details using data integrity module. The data integrity module is implemented via ECC algorithm. This will ensure the secure, privacy and protection to the user data that is communicated through the server.

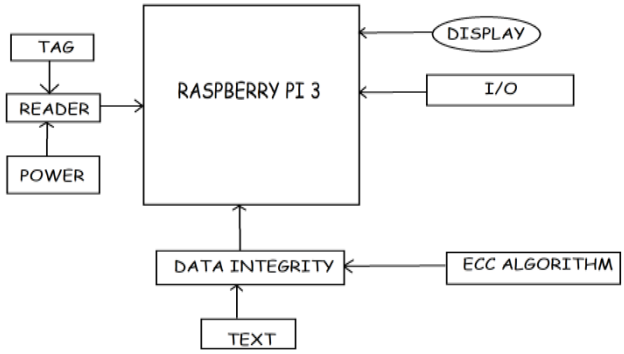

Figure 3: Proposed Block Diagram

6. Implementation Details & Results Discussions

As the system is proposed for IoT data security of RFID tags. The IoT system is implemented through low energy efficient devices like Arduino, Raspberry Pi etc.,. To implement the proposed system it needs server application, data base connectivity, Wi-Fi modules for remote access and security module. To support these features the system is implemented using Raspberry Pi. The system includes the following components

6.1 ECC based hybrid Security System –

It is a hybrid encryption process which is implemented using ECC. This process is implemented using hybrid design with ECC cryptograhy, key exchange through ECDH and symmetric encryption algorithm. Normally in RSA based cryptosystem using asymmetric encryption which uses asymmetric encryption. Where the encrypts the data using private key generates the ciphertext and will decrypt the data by its public key. In ECC uses this process hybrid encryption using Elliptic curve Diffie Helman (ECDH) key method. This method uses the shared secret key for symmetric data encryption and decryption.

6.1.1 Encryption –

RFID encryption has the following functionalities

KEY GENERATION – Here the input text message is given. The text message is given with public key generated using tinyec library and obtain result of output for ciphertext, nonce, authTag and ciphertextPubkey.

SYMMETRIC AES – It is used with Asymmetric ECC along with nonce and authTag to generate the ciphertext.

ENCRYPTED TEXT – The encrypted message can be obtained with the help of ciphertextPubKey.

6.1.2 Decryption

RFID de-cryption has the following functionalities

KEY GENERATION - Encrypted message is given with the private key generated using tinyec library and along the data produced during encryption that is ciphertext,nonce,authTag and ciphertextPubkey is used.

SYMMETRIC AES- Decryption key is used to verify the cipher text.

DECRYPTED TEXT – If the Decryption key is matched and verified then the plain text is obtained.

6.2 RFID System

In order to connect the RFID with system first Raspberry pi we used bread board with connecting wires. Using the appropriate connecting pins with Raspberry pi3 connecting it with proper pin attached to breadboard and Raspberry pi with all the necessary steps. After that we can write the python code for ECC in a python file for taking the input and getting it read by Tag and displaying it using a read file.

6.3 Integration System

Connect the raspberry pi with the system using the SD card inserted in the raspberry pi that has OS already installed in it. Connect the Raspberry pi using HDMI to give it power. Using VNC viewer The OS can be displayed in the laptop and we can run the code.

ECC Algorithm Implementation Details and Results

Image shown below describes the result for ECC code with a plain python code that generates a private and a public key with the help of the message given and the decryption and encryption process is being performed.

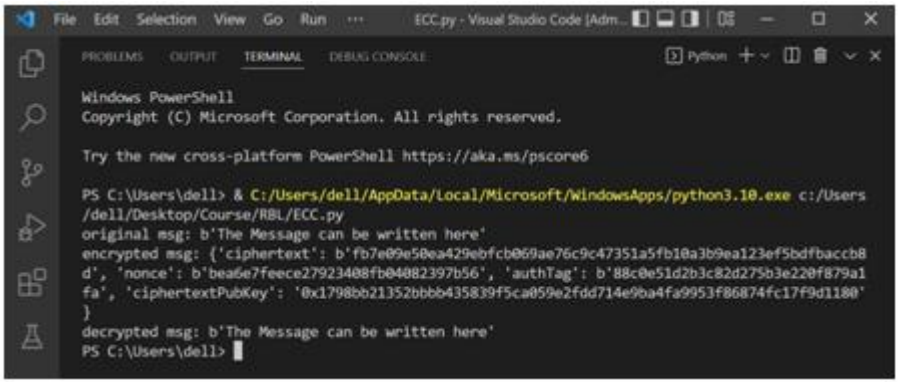

Figure 6: Simulation of ECC code in Node JS

Image shown below describes the result for ECC integrated with Raspberry pi. Necessary connection is been made and Raspberry pi is connected to the system and then putting all the necessary libraries for running the code and installing those libraries with pip statement.

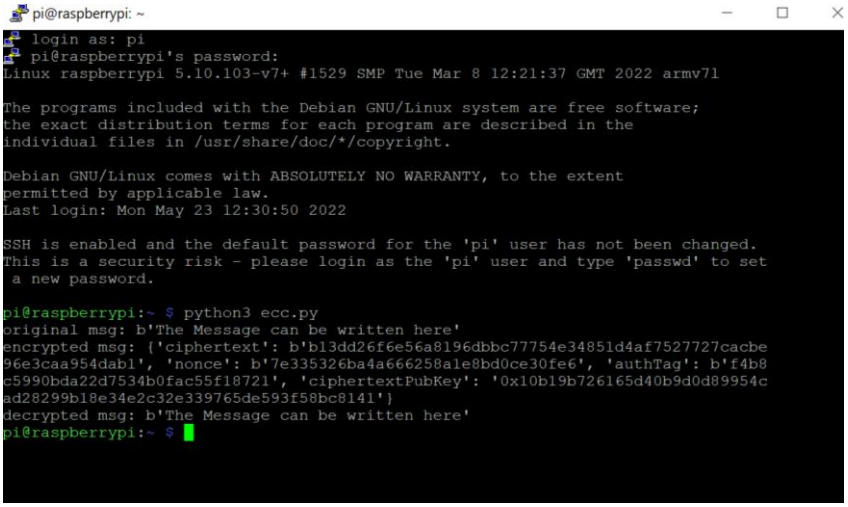

Figure 7: Implementing ECC Codein RASPBERRY PI

7. Conclusion

Understanding security issue for RFID technology in terms of smart ration-based system. And see what issue that are faced by RFID reader and tags. Prevention methods and algorithm that can be taken to protect the system. Using ECC algorithm for implementing Integrity and connecting Raspberry pi and integrating ECC algorithm code in it.

References

[1] ZouheirLabbi, Mohamed SenHadji, Ahmed Maarof, MostafaBelkasmi , "IoT Smart Homes based on RFID Technology: Localization Systems Review", ACM, June 19–21-2018.
[2] PradyumnaGokhale, OmkaraBisht, SagarBhat, "Introduction to IOT ", IRAJ SET,1, January 2018.
[3] SubhasiniShukla, AkashPatil, BrightsonSelvin, "A Step Towards Smart Ration Card System Using RFID & IoT", IEEE,5 Jan. 2018.
[4] Aishwarya Raj Laxmi, Ayaskanta Mishra, "RFID based Logistic Management System using Internet of Things (IoT) ", IEEE ,2018.
[5] MarwaChamekh, Mohamed Hamdi, Sadok El Asmi, Tai-Hoon Kim, "Security of RFID Based Internet of Things Applications: Requirements and Open Issues", IEEE, 19-22 March 2018.
[6] SeongSoo PARK," An IoT Application Service Using Mobile RFID Technology", IEEE, 24-27 Jan. 2018.
[7] Bing-Qing Zhao, Hui-Ming Wang and Jia-Cheng Jiang, "Safeguarding Backscatter RFID Communication against Proactive Eavesdropping", IEEE, 1 Aug 2020.
[8] Santiago Figueroa Lorenzo, Javier Añorga Benito, Pablo GarcíaCardarelli, Jon AlberdiGaraia andSaioaArrizabalagaJuaristi, "A Comprehensive Review of RFID and Bluetooth Security: Practical Analysis", MDPI, 24 Jan 2019.
[9] C. Patel and N. Doshi, "Security Challenges in IoT Cyber World", Springer, January 2019.
[10] Atul Kumar, Ankit Kumar Jain, MohitDua, "A comprehensive taxonomy of security and privacy issues in RFID", Springer, 12 February 2021.
[11] RozanKhader, DerarEleyan, "Survey of DoS/DDoS attacks in IoT", ARDA, January 2021.
[12] H. Damghani, H. Hosseinian, and L. Damghani, "Investigating attacks to improve security and privacy in RFID systems using the security bit method," IEEE, 2019.
[13] XiaolinJia, QuanyuanFeng, Taihua Fan, Quanshui Lei "RFID Technology and Its Applications in Internet of Things (IOT)", IEEE,2019
[14] 12. Chintan Patel and Nishant Doshi, "Security challenges in IOT world",springer,2019.
[15] FatmaMallouli, AyaHellal, NahlaShariefSaeed and Fatimah AbdulraheemAlzahrani, "A Survey on Cryptography: comparative study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms", IEEE, 2020
[16] ZarniSann ,ThiThiSoe and KhaingMyat New ," Comparison of Public Key Cryptography in Different Security Level ", IJRDET, 2019
[17] ZeinabVahdati , Ali Ghasempour and Mohammad Salehi ,"COMPARISON OF ECC AND RSA ALGORITHMS IN IOT DEVICES", Jatit, 2020.
[18] Mohamed El Beqqal*, MostafaAzizi," Review on security issues in RFID systems", December 2017 Advances in Science Technology and Engineering Systems Journal 2(6):194-202.
[19] AikateriniMitrokotsa , Michael Beye , Pedro Peris-lopez, " Classification of RFID Threats based on Security Principles", 2010. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.173.3852.
[20] https://github.com/nakov/Practical-Cryptography-for-Developers-Book/blob/master/asymmetric-key-ciphers/ecc-encryption-decryption.md