IoT Applications on Secure Smart System

Shaikh Faizan Hussain [1], V.V.Yerigeri[2]

[1]*PG Student, Digital Communication Department, MBES College of Engineering, Ambajogai, Maharashtra, India.*
[2]*Professor, Digital Communication Department, MBES College of Engineering, Ambajogai, Maharashtra, India.*

Abstract - *In our day to day life, all things are going towards smartness. As IoT is introduced all devices are connected to each other via the internet. In a supermarket or stores, all things or product is associated with each other framing a shopping framework in such a system. In this system, all the item is attached by their respective RFID tag which is inexpensive, when customers want to buy some item it takes that product which is attached by RFID tag and put it on their smart cart or trolley which is read that tag information by their RFID reader and show their billing amount on display. Which is also an advantage of this the system that no need to wait on a long queue at checkout point.it also track its product stock by this process and inventory management become easier and time-consuming because of no need to scan item by laborer manually. This is a smart shopping system is proposed with security under consideration.*

Key Words: **IoT, RFID, Smart Cart, Raspberry Pi**

1. INTRODUCTION

Now everyday objects can be fitted with computing power and communication capabilities, allowing to link objects everywhere. This has brought a new revolution to manufacturing, political, and environmental systems and sparked significant challenges in data processing, wireless communications, and choice-making in real time [1]. In fact, many security and privacy concerns have arisen, with strong demand for lightweight cryptographic methods to fit in with IoT applications. A lot of IoT work has been conducted on various technologies, such as smart homes, e-health system, connected apps [2]-[3].

In this project, we focus on a system which is based on IoT application and RFID technology [4]. In this system all sailing item is attached to RFID which is read-only by the smart cart which is having RFID reader and also generates its billing info on display. The smart shelves also monitor all stocks and send item status update to the server. By this updating feature it's easy to do work for inventory management by only logged.

In the previously proposed system, there is no consideration of security but in this project, it's in a security consideration because in this project we are using UHF RFID tag [5] which is an ultra-high frequency radio frequency identification passive tag which is having a range around 1 to 12 meter. Which makes it easy to use and less vulnerability. Hence also LCD touch screen/without touch screen display is used for user interfacing and as per user convenience, their respective device is we can use and it communicates with the server. In smart cart RFID reader as well as the microcontroller is used which is scanned the RFID tag by RFID reader and microcontroller process the data. Zig-Bee is used which is low power and inexpensive technology. Weight scanner is also using for sensing product total weight because if the customer peel off tag and put it on the cart it can also show by its total weight at checkout point by RFID reader hence it gives more security on this system.

Selecting a realistic protection approach for a smart shopping network poses a few constraints. For an IoT device, there has to be low power usage. With respect to the contact with the client-server if the smart cart needs to send a message to the server after reading an item in the cart, it needs a lightweight, asymmetric scheme for signing and encrypting, in order to protect confidentiality and integrity. We chose to use ECC-based cryptosystems in this stage, since the key size is much smaller compared to other cryptosystems, such as RSA. As shown in Table I, a 163-bit ECC system will achieve the same degree of protection as a 1024-bit RSA system. If developed, we move to use a symmetric key scheme during subsequent communications to reduce overhead computational expenses. To do so, the smart cart prepares a pair of symmetric keys as session keys before contact with the server starts, and adds them to the post. The server uses one of the two keys to encrypt, and the other key to establish a message authentication code (MAC). Therefore, computing overhead is minimized considerably as symmetric encryption / decryption and MAC is more effective computationally than asymmetric encryption / decryption [8].

1.1 Existing System

Past work on developing smart shopping networks concentrated primarily on low / high frequency RFID [6]-[7], with limited ranges, leaving shoppers with RFID scanner to scan products manually. Throughout the current method, humans are used in the supermarket to control the quality and quantity of the goods, so that manual faults can occur.

1.2 Proposed System

Every smart cart in our proposed system is fitted with a UHF RFID reader, a micro controller, an LCD touch screen, a Zigbee adapter, and a weight sensor. The Smart Cart will read the products put in a cart automatically from the RFID reader. A micro controller is mounted on the data processing cart and the user interface is fitted with an LCD touch-. We have chosen Zigbee technology (data sharing purpose) for the smart cart to connect with the server, as it is low-power and inexpensive. We also mounted a weight scanner for measuring things on the smart cart. This program continuously tracks the consistency and quantity of the goods, in order to obtain customer loyalty by using this definition.

2. ARCHITECTURE DESIGN

2.1 System Architecture

The following components make up our current smart shopping system:

1) Server: Both products are reported to the registry until moving to the shelf. The server stores all items' records, such as location and price, in a database. The server interacts via Zig-Bee with all other organizations inside the smart shopping network.
2) Smart Cart: As shown in Fig. 1, the modules below are mounted on a smart trolley.

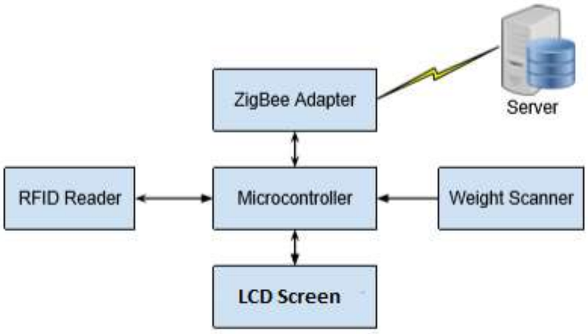


Fig -1: Cart Component

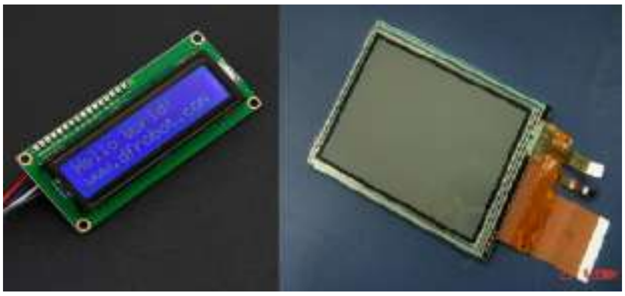
- Microcontroller: Coordinates to execute computational functions with the RFID reader, Zig-Bee converter, weight sensor, and LCD touch screen.

- Zig-Bee Adapter: Zig-Bee is a low-cost and low-power protocol which costs significantly less energy than Wi-Fi [9].

- Weight Scanner: The weight scanner will check items placed into the cart to make sure the tag fits the right object. It can also assist with a security check: if a malicious user peels the RFID tags before placing them in the cart, it can be identified by the cart because no weight is sensed.

- RFID reader: We use an ultra-high frequency (UHF) RFID reader which allows a reading range up to 10 meters. By tuning the transmission power of the reader, we can control its reading range.

- User Interface (LCD display): Displays product information, possible navigation choices, billing information, and coupons etc



3) Smart Shelves: Installed with RFID readers that monitor the status of the items.

4) Smart Checkout Point: The checkout point is installed with a Point of Sale (POS) for the customer to make a purchase. After making the payment, a customer has to go through a lane, where a RFID reader can read all the items in the cart, and check with the server if all the items have been purchased. Any overpay or underpay will trigger an alert.

2.2 Hardware Architecture

Each trolley in supermarkets or malls is attached with one device which consists of hardware components such as RFID reader, micro-controller, EEPROM memory and Liquid crystal display (LCD).

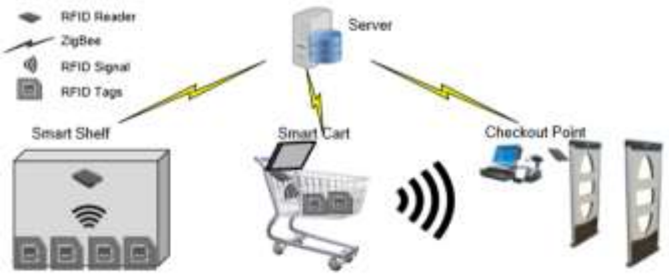


Fig -2: System Model

3. DISCUSSION

All trolleys in the supermarket are attached with the device which contains the RFID reader, microcontroller, Zigbee. So each trolley will send the item information to the main billing server for calculating the final bill of purchased items.

To send information of each trolley we are using Zigbee as it has some advantages over Bluetooth and Wi-Fi. Working is started when the customer enters to the supermarket and takes the trolley. The RFID reader in the trolley is paired to android app for bill generation. When the customer puts the items the RFID reader reads the data, then it is send to the EPROM through the microcontroller. By using Zigbee this data is get sent to main server for fetching cost of the item, so that cost details are displayed on the LCD attached to the trolley. If the customer wants to remove the item from the trolley, then cost of that item gets subtracted from the total bill during the process. At last the bill gets calculated in the main server.

A- Elliptic Curve Cryptography (ECC)

In 1985 Koblitz [10] and Victor [11] discovered elliptic curve cryptography (ECC). It is a cryptographic public-key structure created on the algebraic structure of elliptic curves over finite fields. Compared to other asymmetric cryptographic schemes, it is lightweight based on simple finite fields such as RSA, since it needs smaller key sizes to provide equivalent security [12].

Let Fp represent the field of integers module p and an elliptic curve E over Fp is defined by the equation: $y2 = x3 + ax + b$ (1)

Where $a,b \in Fp$ and $4a3+27b2 \neq 0 \pmod p$

$\langle P \rangle = \{\infty, P, 2P, 3P, ..., (n - 1)P\}$ (2)
From the interval [1, n-1], a private key will be chosen uniformly and randomly, with the corresponding public key Q= dP.

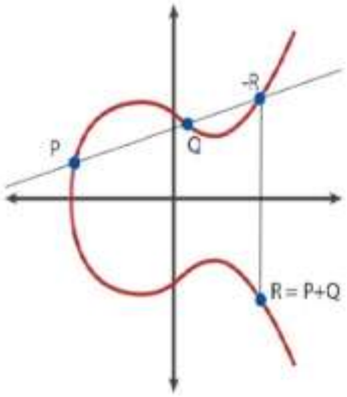


Fig -3: Group Law on Elliptic Curve

B- Elliptic Curve Discrete Logarithm Problem (ECDLP)

In this find d with dp = Q. where P,Q belongs to set E on curve. Its support similar level of safety as RSA but with small key size.

C- Elgamal Encryption based on ECC

On message m the Elgamal cryptosystem's encryption and decryption operations are demonstrated as follows:

Encryption: C1 = kP, C2 = M + kQ, return C1, C2.
Decryption: m = C2 − dC1, return m,

D- Elliptic Curve Digital Signature Algorithm (ECDSA)

In 1992 Scott Vanstone [12] initially proposed ECDSA as an ECC-based authentication scheme. Since of the reduced key length of the ECC system it's much more powerful than RSA.

Table -1: Security Comparison of Various Algorithm [9]

Symmetric	ECC	RSA
80	163	1024
112	233	2240
128	283	3072
192	409	7680
256	571	15360

4. ALGORITHM

Step1: START

Step2: Initialize System

Step3: Put item appended with RFID tag into smart pushcart

Step4: RFID reader reads the tag information

Step5: RFID Reader sends the data to the microcontroller

Step6: Microcontroller send the data to the sever using Zig-Bee

Step7: Server calculate the bill and send back to smart cart

Step8: Final Bill get displayed on LCD

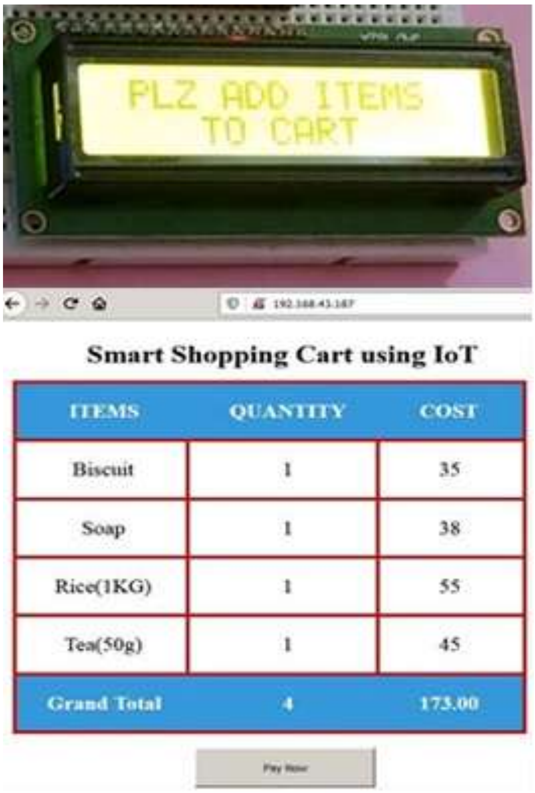
Step9: If customer wants proceed then go to Step10 else go to Step11

Step10: Server generates the bill and prints the bill

Step11: Stop

5. RESULT

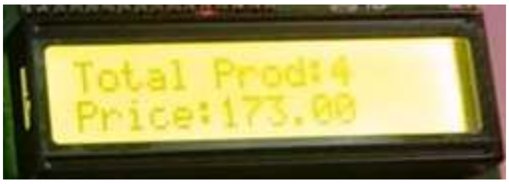
As result as concerned, its show on LCD Screen to add items on cart .when item is added it shows quantity and amount on display as well as total amount and processed further to display on the computer screen as well we can remove the item as well by pressing the button and re-scanned that purchased item tag on the RFID reader. Hence after all this process finally shows its result that customer can pay their bill amount without fault.

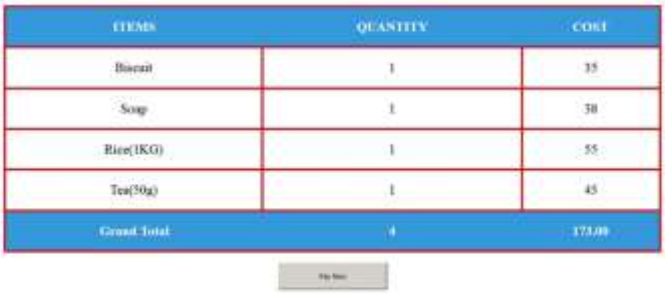


Smart Shopping Cart using IoT

ITEMS	QUANTITY	COST
Biscuit	1	35
Soap	1	38
Rice(1KG)	1	55
Tea(50g)	1	45
Grand Total	4	173.00

Fig -4: Before adding item in cart





ITEMS	QUANTITY	COST
Biscuit	1	35
Soap	1	38
Rice(1KG)	1	55
Tea(50g)	1	45
Grand Total	4	173.00

Fig -5: After adding item in cart total amount

6. CONCLUSION

The projected safe smart shopping system uses RFID technology, Zig-Bee technology that is utilized in adlibbing shopping encounters by making it smart and coordinating security highlights into the system simultaneously.

REFERENCES

[1] F. Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” International Journal of Communication Systems, vol. 25, no. 9, p. 1101, 2012.

[2] P. Castillejo, J.-F. Martinez, J. Rodriguez-Molina, and A. Cuerva, “Integration of wearable devices in a wireless sensor network for an e-health application,” IEEE Wireless Communications, vol. 20, no. 4, pp. 38–49, 2013.

[3] T. Song, R. Li, X. Xing, J. Yu, and X. Cheng, “A privacy preserving communication protocol for iot applications in smart homes,” in to appear in International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) 2016, 2016.

[4] S. Shepard, RFID: radio frequency identification. McGraw Hill Professional, 2005.

[5] D. M. Dobkin, The rf in RFID: uhf RFID in practice. Newnes, 2012.

[6] D. Klabjan and J. Pei, “In-store one-to-one marketing,” Journal of Retailing and Consumer Services, vol. 18, no. 1, pp. 64–73, 2011.

[7] A. Yewatkar, F. Inamdar, R. Singh, A. Bandal et al., “Smart cart with automatic billing, product information, product recommendation using rfid & zigbee with anti-theft,” Procedia Computer Science, vol. 79, pp. 793–800, 2016.

[8] W. Dai. (2009) Crypto++ 5.6. 0 benchmarks. http://www.cryptopp.com/benchmarks.html.

[9] P. Kinney et al., “Zigbee technology: Wireless control that simply works,” in Communications design conference, vol. 2, 2003, pp. 1–7.

[10] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of computation, vol. 48, no. 177, pp. 203–209, 1987.

[11] V. S. Miller, “Use of elliptic curves in cryptography,” in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1985, pp. 417–426.

[12] D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.

BIOGRAPHIES

Shaikh Faizan Hussain, has completed his Bachelor's Degree and Diploma from Electronics and Telecommunication Department & pursuing Masters in Digital Communication Department in MBES College of Engineering, Ambajogai, India.

Prof. V. V. Yerigeri, has completed B.E in Electronics & Communication Engineering & M.E. in Power Electronics & Perusing Ph.d in Signal Processing. He has teaching experience of more than 24 Years. He has presented many papers in National & International Conferences & Published more than 50 papers in National & International Journals.