MANTECH Publications
Journal of Networking, Computer Security and Engineering
Volume 4 Issue 1

A Review on Smart Cart Shopping System Using IOT

Anusha B G*, Dr Nagaveni V**
Student, Professor***
Department of CSE
Acharya Institute of Technology Bangalore
Corresponding author's email id: *nagaveni@acharya.ac.in*
DOI: *http://doi.org/10.5281/zenodo.2581203*

Abstract

The internet of things (IOT) is changing human lives by connecting everyday objects together. Nowadays shopping at big malls is a daily activity in metro cities. One can see a huge rush at malls on holidays and on special discount days. People purchase different items and put them in trolleys and go to billing counter for payments. In that time, they have to wait in a long queue to get their products scanned using RFID reader with help of barcode scanner and get their billed. To modify that customer has to purchase in smart way in shopping malls. Each and e very product is attached with a RFID tags, when placed into a smart shopping cart, can be automatically read by a cart equipped with a RFID reader, so that the billing can be conducted from the shopping cart itself. In this way, customer can avoid waiting in a long queue at the checkout points. For this system, additional smart shelving can be added and equipped with RFID reader and can monitor stock, also updating central server, server knows the status of the items in the store. The inventory management also becomes much easier, because all the items can be automatically read by a RFID reader instead of manually scanned by the laborer.

Keywords: *Internet Of Things (IOT), Security, Cloud Computing, RFID, Smart Shopping, Zigbee Adapter.*

INTRODUCTION

Internet of Things has brought a new uprising in industrial, financial and environmental systems. So let's us know about it. IOT refers to the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and connectivity which enables these objects to connect and exchange data between the devices. In this era of Internet of Things, interactions among physical objects have become a reality. Every object in this world are on the verge of getting connected together with the help of Internet.

In this paper let us try to focus on a Smart Shopping System [4] using ultra high frequency RFID tags which have not been well implemented in the past. The major advantage of such system is that people can get rid of standing in long queues waiting for their turn for billing the items. So here RFID is introduced meaning Radio Frequency Identification Tag which uses electromagnetic fields to automatically identify and track tags attached to objects. In the implementation couple of components is used such as the Ultra High Frequency RFID Tags which is very inexpensive and has a range up to 12m followed by the Micro Controller which is primarily used for Data Processing.

LCD Touch Panels which are equipped with User Interface, Zig Bee Adapter which is used to communicate with the Cloud or the Server and most significantly a Weight Sensor which is used for weighing the items.

Cloud or the main server is used for storing all the updated prices of the items, this prevents sticking or writing the cost of each product on all the items. So the moment the customer grabs his byte, the cart will search in for the price of the item from the cloud and display it on the LCD panel, due to which the customer can decide whether their item is worth for his penny or not.

Existing

The existing system of shopping is a long process and consumes lot of time like choosing the products, waiting in the queues, scanning the products and checking out. This is a lengthy process and it can use the trending cutting edge technology of IOT to reduce the time and solve the problem. Most of the time is wasted in a never ending queues and billing of the items which creates havoc in the shopping malls.

Hence if it is possible to reduce time in scanning by automating long queues problem can be reduced. More significantly the dynamic range of the RFID's has been increased when compared to the past. These minor tweaks help us to move further and solve the problem.

Proposed Method:

Smart shopping cart is the solution for the above existing problem, this cart is equipped with sophisticated microcontroller and sensors which reduce the time in billing as it would be scanning the items instantly as and when the item is added to the cart and this would totally eliminate the queues in the shopping centers.

Sensors and microcontrollers is easily available at a very cheap rate and could be equipped to each and every cart and at the exit a scanner would be placed for security which would alert if payment has not been processed. This would overcome the difficulties currently present in the market.

SYSTEM ARCHITECTURE

The Components of the Smart Shopping System from the below shown figure 1 include:

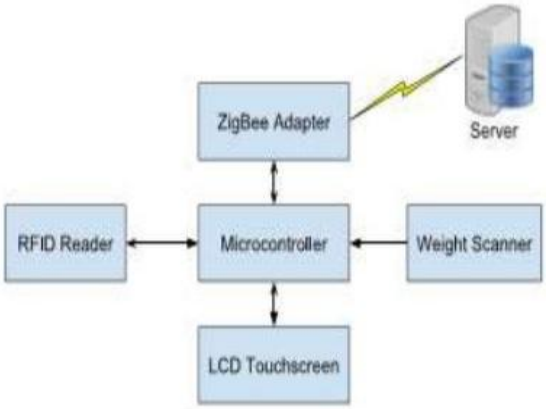

Figure 1: System Architecture of Smart Shopping System

1) Server: All items are registered to the server before moved to the shelves. The server stores all items' information, such as location and price, in a database. The server communicates with all the other entities in the smart shopping system through Zig-Bee.

2) Smart Cart: As shown in Figure above, the following components are equipped on the smart cart.

- **Microcontroller:** Coordinates with the RFID reader, ZigBee adapter, weight scanner, and LCD touch screen to perform computing functions.

- **Zig-Bee Adapter:** Zig-Bee is a low-cost and low power protocol that costs much less energy than Wi-Fi

- **Weight Scanner:** The weight scanner can weigh items that are put in the cart to ensure the tag corresponds to the correct item.

- **RFID Reader:** UHF RFID reader is used that allows a reading range up to 10 m by tuning the transmission power of the reader.

- **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 item.

4) **Smart Checkout Point:** The checkout point is installed with PoS for the customer to make a purchase. After making the payment, a customer has to go through a lane, where an RFID reader can read all the items.

Building Functional Smart Cart

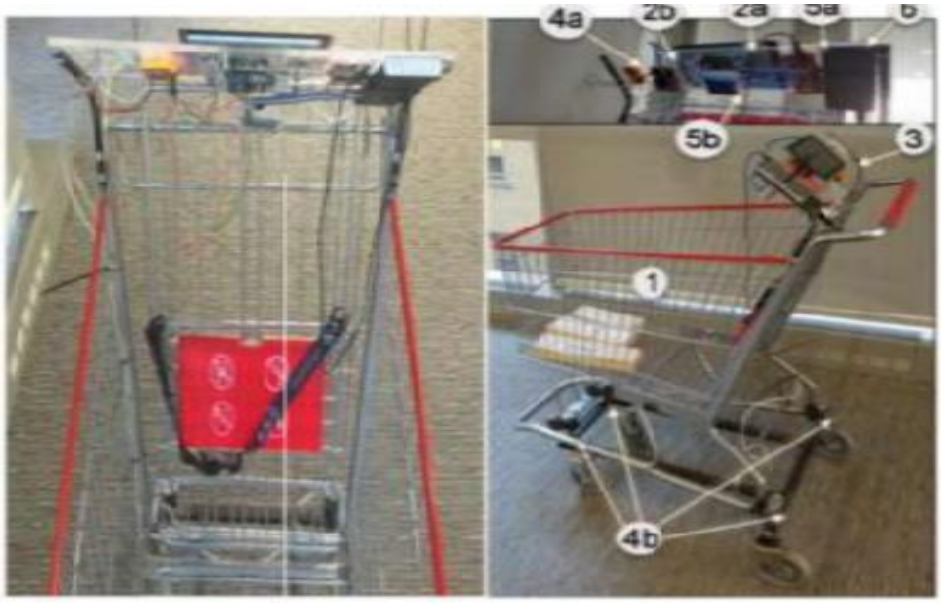

Figure 2: Smart Cart

The prototype is built to test our design and functionality. Figure 2 shows the components of our designed smart cart. According to our tests, when putting an item into the smart cart or removing an item from the cart, the smart cart is able to accurately read it.

One surprising result is that, the metal outside the cart blocks the signal to a pretty high extent that, when the reader is inside the cart, no item outside the cart can be read. This clearly indicates that an item put into a smart cart will not be read by a nearby cart accidently.

It is also possible to test how to set an RFID reader at the checkout point so that the items in the cart can be accurately read. In the design, information such as price, location and coupon are stored in a database of the server, rather than in the tags, because such information might change over time, and it is more convenient for the server to manage them.

PRELIMINARIES

A. Elliptic Curve Cryptography

ECC was invented by Koblitz and Miller in 1985. It is a public-key cryptographic system based on the algebraic structure of elliptic curves over finite fields. It is lightweight compared to other asymmetric cryptographic systems based on plain finite fields, such as RSA, as it requires smaller key sizes to provide equivalent security. Let Fp denote the field of integer's module p and an elliptic curve E over Fp is defined by the equation

$$y2 = x3 + ax + b \quad (1)$$

Where a, b ∈ Fp and $4a3+27b2 \equiv 0 \pmod{p}$

The set of points on an elliptic curve forms a group and Fig. 1 describes the geometric addition operations of adding P and Q: if a line passing through P and Q is drawn, then this line will intersect a third point on the curve R, and the inverse of this point, −R, is the result of P + Q. The idea behind this group operation is that the three points P, Q, and −R are aligned on the curve and the points that form the intersection of a function with the curve sum to zero.

Suppose E is an elliptic curve defined over a finite field Fp, and P is a point in E (Fp) with a prime order n. To generate a public key pair, a cyclic subgroup of E (Fp) will be generated by P

$$(P) = \{\infty, P, 2P, 3P,...,(n-1)P\}. \quad (2)$$

A private key will be selected uniformly and randomly from the interval [1, n − 1], and the corresponding public key is Q = dP.

B. Elliptic Curve Discrete Logarithm Problem

Elliptic curve discrete logarithm problem (ECDLP) refers to finding d with dP = Q, where the points P, Q belong to a set of points E on an elliptic curve. ECDLP is known to be computationally infeasible; and as discussed before, an elliptic curve group could provide the same level of security afforded by RSA with a smaller key size.

C. Elgamal Encryption Based on ECC

There are different ways to implement encryption operations-based ECC, such as ECC Diffie–Hellman (ECCDH) and Elgamal encryption on ECC. ECCDH suffers from man-in-the-middle attacks and is not suitable for our application.

Upon generating a pair of public keys Q and d based on ECC, the encryption and decryption operations of the Elgamal cryptosystem on message m are illustrated as follows.

Encryption: C1 = kP, C2 = M + kQ, return C1, C2

Decryption: m = C2 − dC1, return m

D. Elliptic Curve Digital Signature Algorithm

Elliptic curve digital signature algorithm (ECDSA) was initially proposed in 1992 by Vanstone [34] as an authentication scheme based on ECC. It is much more efficient than RSA because of the smaller key length of the ECC system. The parties involved in the application of ECDSA need to agree upon elliptic curve domain parameters in order to process ECDSA.

SYSTEM MODEL

Figure 4 depict the system model. The server communicates with the smart shelves, smart carts and the checkout points. The smart shelves are able to monitor the items on the shelves by reading the RFID signals from the tags, the smart carts are able to read and retrieve information of the items inside the carts; finally, the checkout points can validate the purchase made by a customer.

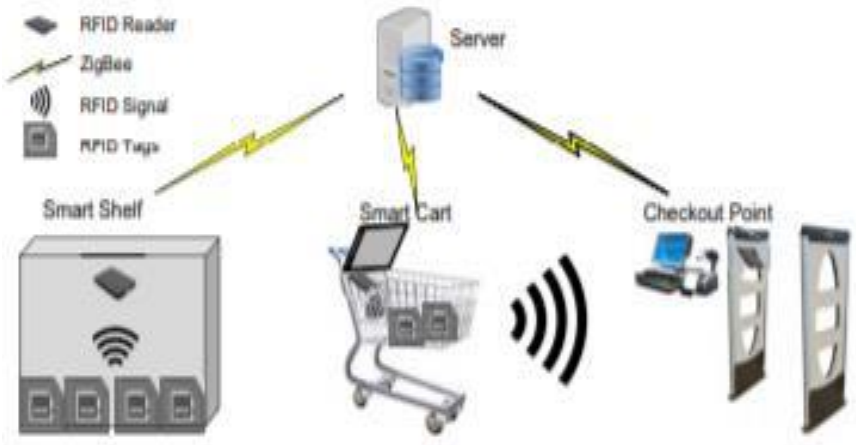

Figure 4 System Model

An asymmetric key crypto system is adopted. The server is assigned with a pair of asymmetric keys Ps and Ss. Each smart cart is assigned a unique ID i and a pair of asymmetric key Pi and Si. Each checkout point is assigned a unique ID j and a pair of asymmetric key Pj and Sj .The encryption to cipher text c of data d with public ke y P is denoted by c = EP (d), and decryption of cipher text c with private key S by d = DS(c).

REGISTRATION

Before moving all items to the shelves, the store needs to register all items. A design of the RFID tags here is as shown in **Figure. 5**.

In our design, some information, such as price, location and coupon information are stored in the database of the server, rather than in the tag, because these kinds of information might change overtime, and it is more convenient for the server to manage them.

To pre vent a malicious user from rewriting a tag, digital signature is used to protect the tag information. The store will use its private key Ss to sign all the tags during registration phase. When a cart or the checkout-point reads one tag, it will verify the signature using the store's public key. A failed verification will trigger an alarm.

The tags must be tamper-proof, so that any action on taking off the tag or switching tags between items will leads to a failure. Finally, after utilizing the weight scanner on the carts prevents a dishonest customer from underpaying. If the weight of the items in the cart is greater than they should be, an alarm will be triggered.

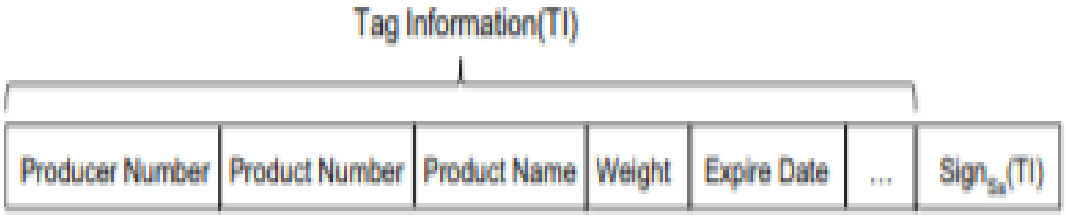

Figure 5 Tag Design

BILLING GENERATION ON SMART CART

When an item is put into a smart cart, the RFID reader on the smart cart will read the tag and sends the tag information to the micro-controller that will communicate with the server via Zig-Bee requesting product information. The communication is protected by an asymmetric encryption scheme and all messages are signed to protect integrity.

The following three algorithms are proposed to complete the billing generation process. In Algorithm 1, the smart card reads an item, and checks if the signature of the item is valid. If the tag is not signed with a valid key, the smart cart will send an alarm notifying the officer that the tag has been modified by a malicious entity. Otherwise, the smart cart will sign the tag with its own ID i and a time stamp, encrypts the message, and sends the message to the server.

CHECKOUT AND VERIFICATION

Even though the smart cart can generate a billing statement, checkout point equipped with a PoS be installed is insisted at the store exit. This is used to prevent physical attacks on the PoS that become moving targets in places without supervision.

Finally, a RFID reader installed on each exit of the store can help to verify the purchase. All items in the store can have two possible status:”for sale” or”sold”.

After an item has been paid, the server will be notified by the smart cart to change its status from for sale” to ”sold”. When a customer is about to leave the store, the RFID reader on the exit door will read all items in the smart carts passing by and check with the server that if all items status are ”sold”. Only if all items scanned by the RFID reader are ”sold”, the exit door will open to let a customer pass. In this way, a valid payment of a customer can be verified.

SECURITY ANALYSIS

Analysis of the security of the communication between the smart cart and the server is done.. The communication between the checkout point and the server are the same.

A. Confidentiality

In each communication between the smart cart and the server, the message sent from the smart cart to the server is encrypted using the smart cart's public key. The security is based on ECDLP, which is known to be computationally infeasible to break. The message sent back to the smart cart is encrypted using a session key, which is only known to the server and the client. Therefore, no outside adversary is able to figure out the data in the communications. This also indicates that the privacy in the smart shopping system is well-protected.

B. Integrity

The message sent from the smart cart to the server is signed with the smart cart's private key Ss, thus integrity is protected. When the server sends a message back to the smart cart, it creates an MAC using the secret shared with the smart cart s2, and no outside adversary is able to modify the message while passing the check of MAC. Therefore, data integrity is wellprotected.

C. Replay Attack Resistance

In our proposed system, all communication messages include a time stamp T, making it hard for an attacker to perform a replay attack. If a malicious customer replays a message from a server that contains an item's price lower than current price, the smart cart can detect that the message is replayed immediately by checking the time stamp: if T in the message is not consistent with the system time, the message will be discarded. If a malicious customer would like to pass the verification of the server, he must be able to change the value of the times stamp T included in the ciphertext, which is not possible. Therefore, replay attacks are not practical.

D. One-Time Key

Each time a smart cart requests information from the server, it randomly creates a pair of session keys and sends them to the server. The server uses one key to encrypt data and the other to create an MAC. The session keys are generated for each request and are unrelated to the previous keys. By adopting the session keys, the data sent from the server to the smart carts is well-protected.

E. Tag Security

Based on our design, the security of the RFID tags is wellprotected. First, physically destroying the tags or blocking the RFID signal from a tag can be detected by the scales on the smart cart. A small camera can also be installed on the smart cart to cooperate with the scale for this function: if the smart cart fails to read a tag and the scale or camera detects that a new item is put into the cart, it will send an alarm. Second, any rewriting to the RFID tags will be detected by checking the HMAC, which cannot be counterfeited by an outside adversary without the secret key. Finally, switching the tags on different items does not work because peeling off the tamper-proof tags will break them.

APPLICATIONS

Applications of this system would be a smart shelf. Intuitively this brings the following benefits .

1. Items put into a smart shopping cart (with RFID reading capability) can be automatically read and the billing information can also be generated on the smart cart. As a result, customers do not need to wait in long queues at checkout.
2. Smart shelves that are also equipped with RFID readers are able to monitor all stocked items and send item status updates to the server. When items become sold out, the server can notify employees to restock.
3. It becomes easy for the store to do inventory management as all items can be automatically read and easily logged.

CONCLUSION

In this paper, we propose a secure smart shopping system utilizing RFID technology. This is the first time that UHF RFID is employed in enhancing shopping experiences and security issues are discussed in the context of a smart shopping system. The design of a complete system and build a prototype is done to test its functions, also design a secure communication protocol and present security analysis and performance evaluations.

It is believed that future stores will be covered with RFID technology and our research is a pioneering one in the development of a smart shopping system. Our future research focus on improving the current system, for example,

by reducing the computational overhead at the smart cart side for higher efficiency, and how to improve the communication efficiency while preserving security properties.

REFERENCES

I. Ruinian Li, Tianyi song, Nicholas Capurso, Jiguo Yu, Jason Couture, and Xiuzhen Cheng, "IOT Applications on secure smart shopping system",IEEE Journal,vol 4,no.6,Dec 2017.

II. Ruinian Li, Tianyi song, Nicholas Capurso, "IOT Applications on secure smart shopping" 2016 International Conference on Identification and knowledge in the Internet of Things.

III. Suhas B.M, Tanu.N.Prabhu, "Applications On Secure Smart Shopping System", International Research Journal of Engineering and Technology (IRJET) volume:05: Issue: 02 Feb-2018.

Cite this Article

Anusha B G, Dr Nagaveni V (2019) **A Review on Smart Cart Shopping System Using IOT** Journal of Networking, Computer Security and Engineering, 4 (1), 27-37

http://doi.org/10.5281/zenodo.2581203