Indian J.Sci.Res. 17(2): 360-370, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

IOT APPLICATIONS ON SECURE SMART SHOPPING SYSTEM

[1]N.Gowtham,[2]G.RamachandraKumar,[3]K.Narasimha
[1,2,3] Department of Electronics and Communication Engineering, Sreyas Institute Engineering &Technology, Hyderabad

***Abstract*—**The Internet of Things (IoT) is changing human lives by connecting everyday objects together. For example, in a grocery store all items can be connected with each other, forming a smart shopping system. In such an IoT system, an inexpensive RFID tag can be attached to each product which, when placed into a smart shopping cart, can be automatically read by a cart equipped with an RFID reader. As a result, billing can be conducted from the shopping cart itself, preventing customers from waiting in a long queue at checkout. Additionally, smart shelving can be added into this system, equipped with RFID readers, and can monitor stock, perhaps also updating a central server. Another benefit of this kind of system is that inventory management becomes much easier, as all item scan be automatically read by an RFID reader instead of manually scanned by a laborer. To validate the feasibility of such a system, in this work we identify the design requirements of a smart shopping system, build a prototype system to test functionality, and design a secure communication protocol to make the system practical. To the best of our knowledge, this is the first time a smart shopping system is proposed with security under consideration.

***Keywords*—**IoT; Smart Shopping; Smart Cart; Security.

I. Introduction

IntheeraoftheInternetofThings(IoT),interactionsamong physical objects have become a reality. Everyday objects can now be equipped with computing power and communication functionalities, allowing objects everywhere to be connected. This has brought a new revolution in industrial, financial, and environmental systems, and triggered great challenges in data management, wireless communications, and real-timedecision making [1]. Additionally, many security and privacy issues have emerged and lightweight cryptographic methods are in highdemandtofitinwithIoTapplications.

There has been a great deal of IoT research on different applications, such as smart homes, e-health systems, wearable devices, etc. [2]–[4]. In this paper, we focus on a smart shopping system based on Radio Frequency Identification (RFID) technology [5], which has not been well-studied in the past. In such a system, all items for sale are attached with an RFID tag, so that they can be tracked by any device equipped with an RFID reader in the store - for example, 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 needtowaitinlongqueuesatcheckout.2).Smartshelvesthat are also equipped with RFID readers are able to monitorall 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.

We propose the use of ultra high frequency (UHF) RFID technology [6] in the smart shopping system, as UHF passive tags have a longer range, from 1 to 12 meters. Previous research on the design of smart shopping systems mainly focused on using low/high frequency RFID [7]–[14], which have inadequate ranges, and leave customers to manually scan itemswithaRFIDscanner.Inourproposedsystem,eachsmart cart is equipped with a UHF RFID reader, a micro controller, an LCD touchscreen, a Zig-Bee adapter, and a weight sensor. The smart cart is able to automatically read the items put intoa cart via the RFID reader. A micro controller is installed on the cart for data processing and a LCD touchscreen is equipped as the user interface. In order for the smart cart to communicate with the server, we have chosen Zig-Bee technology as it is low-power and inexpensive. We also have a weight scanner installed on the smart cart for weighting items. The weight scanner can also help do a security check, for example, if a malicious user peels off one item's RFID tag and puts it into the cart, extra unaccounted weight will be added. When a customer finishes shopping, they pay at the checkout point using the generated billing information on the smart cart. We also set a RFID reader before the exit door to check that all theitemsinthecarthavebeenpaidfor.

We consider security and privacy issues related to smart shopping systems as no previous research has tackled it. In such a system, wireless communications

[1]Corresponding Author

among the server, smart carts, and items are vulnerable to various attacks; an adversary is able to interfere with the communications if no proper security method is applied. Privacy issues also exist in such a system: the competitor of a store might get easy access to the circulation of commodities for financial strategy; and customer preferences can be inferred by easily collecting the product information in shoppers' shopping carts. Therehas been much related work on security and privacy in other areas [15]–[24], but none exists in the context of a smart shopping system.

There are a few restrictions in choosing a practical security method for a smart shopping system. As an IoT application, the power consumption must be low. In regards to the client-servercommunication:ifthesmartcartneedstosenda*Corresponding Author.message to the server after reading an item in the cart, it needsa lightweight, asymmetric scheme for signing and encrypting, in order to protect confidentiality and integrity. At this step we choose to use ECC-based cryptosystems, as the key size is much smaller compared to other cryptosystems, such as RSA. As shown in Table I, an ECC system with 163-bit key can achieve the same security level as an RSA system with a1024- bit key. Once established, we switch to using a symmetric key scheme to reduce computational overhead during subsequent communications. To do this, before communication with the server begins, the smart cart prepares a pair of symmetric keys as session keys and appends them to the message. The server will use one of the two keys for encryption, and the other for creating a message authentication code (MAC). Therefore, computational overhead is greatly reduced as symmetric encryption/decryption and MAC is more computationally effi- cient than asymmetric encryption/decryption[25].

We have built a prototype to test the functions of the smart cart. We have also closely monitored the reading rangeto guarantee only the items put into a smart cart can be read. We test the placement of the RFID reader in the smart cart and of the reader at the checkout point. We also give a security analysis and performance evaluation to prove this system is practical. Finally, we take into consideration the cost of the required components and we find the cheapest RFID reader are at 150 USD and UHF passive tags are at 2 cents in the current market. We believe in the future, grocery stores will beIoT-based with RFIDtechnology.

This paper is a pioneer work in the design of secure smart shopping system. We list our contributions as follows.

1) We propose a complete design of the smart shopping system, and we give a description of the designs and corresponding functions indetail.
2) We are the first to propose using UHF RFID technology to support connections in a smart shopping system. Our system is the first system to achieve automatic reading oftheitemswithaproperrange.
3) We are the first to design a secure protocol for the com- munications in the smart shopping system. To evaluate the protocol, we give a security analysis andperfor- mance evaluation in terms of computational complexity and communicationcomplexity.
4) We have built a prototype of the smart shopping system and major functions, such as accurate and automatic reading, areachieved.

Thepaperisorganizedasfollows.SectionIIsummarizesthe most related works. Section III introduces the preliminaries. Section IV presents the design of the smart shopping system. In Section V, we present the system model. In Sections VI, VIII and IX we describe the registration phase, billing generation phase and checkout phase, respectively. A security analysis is provided in Section X and the evaluation of computation and communication complexities are presentedin

XI. We conclude this paper with a future research discussion in SectionXII.

Table Isecurity Comparison For Various Algorithm [26]

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

II.RelatedWork

Study on IoT applications is a popular topic in recent years, but smart shopping systems have not been well-investigated. There are some research works being published in recentyears regarding improving customers' shopping experience. In2011, Klabjan*et al.* [7] proposed the idea of tracking a customer in the store and discovering customers' interests in order to offer personalized coupons. The idea of smart shelves and smart carts were also discussed in their work. Smart carts can be tracked using RFID technology and smart shelves can monitor thelocationandstatusesoftheitems.

There were multiple attempts made in 2003. Shanmuqapri- van *et al.* proposed a basic design using RFID and a barcode reader for product identification, while using Zig-Bee for communication [8]. Kumar *et al.*

represented the first physical implementation with RFID and Zig-Bee [9]. Gupta *et al.* gave a very unconventional design for a smart cart, and they are one of the first examples to address the anti-theft issue [10]. Their design was similar to a mail receptacle: a chute where items are inserted and scanned, then dropped into a closed chamber. The chamber had a door on the top which could only be opened if the user had paid for the items. The design indirectly guarded against wireless communication security threats by not allowing any wireless communication - the cart was physically wired up to a point-of-sales systemto pay when the user was done shopping. Ali *et al.* designed a smart cart system with navigation [11]. Their design included the implementation of smart shelves, which determined when smart carts enter an aisle (using infrared sensors) anddelivered product information tocarts.

There are more designs in this area in the last three years [12]–[14], but none of them included novel ideas. In all the previous designs, a customer had to scan the items one-by-one manually, which is not convenient. Furthermore, security issueshaveneverbeenexploredinanypastwork.

RFID technology has been widely studied in recent years and it is a major technology applied in IoT applications [27]– [29]. Amendola*et al.* reviewed the RFID technology and its use for applications on body-centric systems [30]. Welbourne*et al.* developed an RFID ecosystem with a suite ofweb-based, user-level tools and applications [31]. For grocery marketing, most stores are using barcodes nowadays, but we have reason to believe that RFID over barcode is a general trend as RFID can achieve distance reading, which intellectually brings the propertyofIoTandconnectalltheobjectsinastoretogether.

III.Preliminaries

A. Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) was invented by Koblitz[32] and Victor [33] 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 cryptographicsystemsbasedonplainfinitefieldssuchasRSA, as it requires smaller key sizes to provide equivalent security [34].

Let $F_p$curvedenote the field of integers module p and an elliptic

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

Decryption: $m = C2 - dC1$, return m.Eover$F_p$is defined by the equation:

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

where$a$, b $F_p$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 we draw a line passing through P and Q, 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, 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 F_p, and P is a point in $E(F_p)$ with a prime order n. To generate a public key pair, a cyclic subgroup of $E(F_p)$ will be generated by P :

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

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

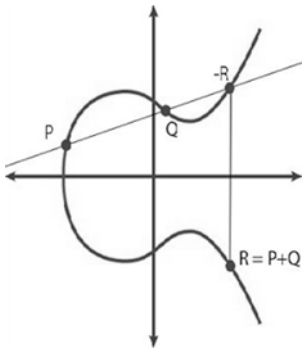

Fig. 1. Group Law on an Elliptic Curve

B. Elliptic Curve Discrete Logarithm Problem (ECDLP)

ECDLP refers to finding d with $dP = Q$ where the points P ,Qbelong 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 Elliptic Curve Cryptography Diffie-Hellman (ECCDH) and Elgamal encryption on ECC. ECCDH suffers from Man-in-the-Middle (MITM) 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 (ECDSA)

ECDSA was initially proposed in 1992 by Scott Vanstone[35] 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. For the sake of space, we will notdiscussthedetailsofECDSAhere.

IV.SmartShoppingSystem

A. DesignGoals

Our proposed smart shopping system should achieve the following major goals:

1) Item reading: The smart cart should be able toaccurately read items put into or removed from the cart. An item put into one cart should not be able to be read byanothercartnearby.

2) Items tracking: The server should maintain the state of items in the store. With RFID readers installed on the shelves, the items can be monitored and the item stock canbeupdatedtotheserver.

3) Payment verification: We propose installing RFID read- ers before the exit door, which can scan all the items in the smart cart, and check with the server if everything in the cart has been paid. If a dishonest customer tries to leave the store without making a payment, he will not pass theverification.

Apart from the major goals, many other functions can be achievedinfuture,suchasnavigation,advertising,coupon recommendation, etc. Advertising and coupon recommendations can be easily added to the functions of the smart cart, and navigation can be reached by utilizing the Zig-Bee gatewaysto determine the location of a shopping cart through triangulation techniques[36].

B. Challenges

1) Tag Tamper-Proofing (Tag Security): The tag design mustberesistanttothefollowingmisuses:

a) re-writesinordertopayless.

b) obstructionsandreplacementbyfaketags.

c) swappingthetagsofdifferentitems.

d) breaking or tampering to avoid paying the price altogether.

In Section VI, we give a standard regarding how the tags can be designed for secure use.

2) Reading Collision: Intuitively, the reading range of the RFID reader should be carefully set to avoid collisions with othercarts.

3) Communication Security: The communication in the smart shopping system needs to be protected. For ex- ample, to guarantee the confidentiality and integrity of a transaction, lightweight cryptographic systems need to be utilized to prevent an attacker from eavesdropping data or modifying data sent between the carts and the server.

C. Components

Our proposed smart shopping system consists of the follow- ing components:

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 thesmartshoppingsystemthroughZig-Bee.

2) Smart Cart: As shown in Fig. 2, the following compo- nentsareequippedonthesmartcart.

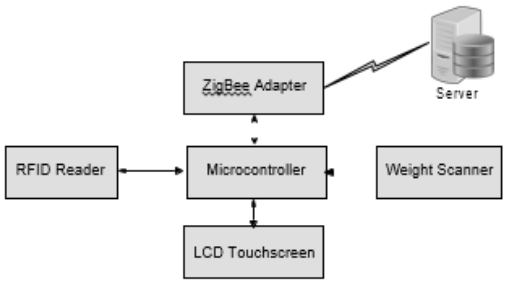

Fig. 2. Cart Components

- Microcontroller: Coordinates with the RFID reader, Zig-Bee adapter, weight scanner, and LCD touch- screen to perform computingfunctions.
- Zig-Bee Adapter: Zig-Bee is a low-cost and low- power protocol that costs much less energy thanWi- Fi[37].
- Weight Scanner: The weight scanner can weigh items that are put in the cart to ensure the tag corresponds to the correct item. It can also helpwith a security check: if a malicious user peels off the RFID tags before putting it into the cart, the cart candetectitasnoweightissensed.
- 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,wecancontrolitsreadingrange.
- User Interface (LCD display): Displays product information, possible navigation choices, billing in- formation, and couponsetc.

Smart Shelves: Installed with RFID readers that monitor

the status of theitems.

3) 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 analert.

D. Building a Functional SmartCart

We built a prototype to test our design and functionality. Fig. 3 shows the components of our designed smart cart and the specific descriptions of each component can be found in Table II. The workflow of our smart cart is illustrated through Fig. 4. 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. We are also able to test how to set a RFID reader at the checkout pointsothattheitemsinthecartcanbeaccuratelyread.

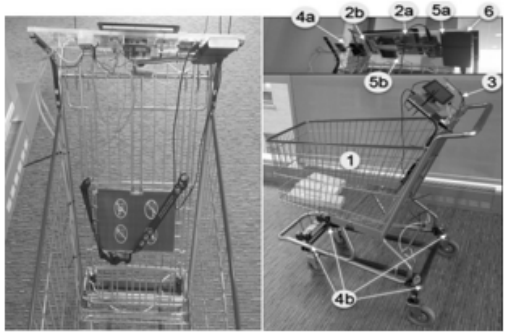

Fig. 3.Smart Cart

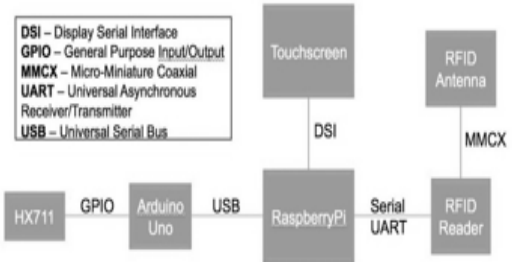

Fig. 4. Workflow of the Smart Cart

V. SystemModel

Fig. 5 depicts the system model. The server communicates with the smart shelves, smart carts, and the checkout points.

Table II:SpecificationsOfThe Components

	Function	Components	Description
1	Cart	Shopping Cart	Standard Metal Frame
2	Micro-processing	a) Raspberry Pi3 b) Arduino Uno as an interim so-lution for weightsensor	1.2GHz 64-bit quad-core ARMv8 CPU; 802.11n Wireless LAN; Bluetooth 4.1 Bluetooth Low Energy (BLE); 1GB RAM; 4 USB ports; 40 GPIO pins; Full HDMI port; Ethernet port; Combined 3.5mm audio jack and composite video; Camera interface (CSI); Display interface (DSI); Micro SD card slot (now push-pull rather than push-push); VideoCore IV 3D graphics core
3	Display	Raspberry Pi Foundation 7” Touchscreen LCD Display	RGB 800480 display @ 60fps; 24-bit color; FT5406 10 point capacitive touchscreen; 70 degree viewing angle; Metal-backed display with mounting holes for the Pi
4	Weight Sensing	a) HX711 ADC b) 4xHalf Bridge Load Sensors	Signal Amplifier; Analog-to-Digital Converter;
5	RFID Reader	a) Cottonwood Long Range UHF RFID Reader b) Circularly Polar-ized Antenna (5dB)	EPC Gen2 Compatible; Global Frequency Capable (840-960MHz); 20dBm Max Antenna Power; 1.5-2W Power Consumption; GPIO programmable; UART Serial

			Interface;
6	Power Supply	Polanfo 12000mAh Power Bank Universal Ultra Compact External Battery	Charge input of 5V/1 A; Two USB output ports (2.1A and 1A)

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.

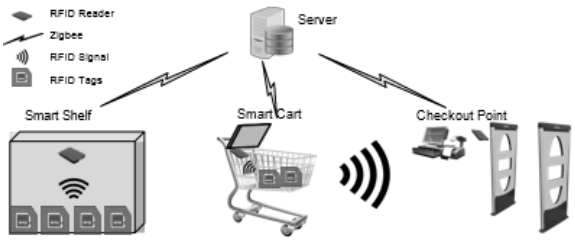

Fig. 5. System Model

We adopt a combination of symmetric and asymmetric cryptographic systems. The server is assigned with a pair of asymmetric keys $P_s$andS_s. Each smart cart is assigned a unique ID $i$and a pair of asymmetric keys$P_i$andS_i. Each checkout point is assigned a unique ID j and a pair of asymmetric keys $P_j$andS_j. For asymmetric encryption and decryption, we denote the encryption to ciphertext$c$of data d with public key P by $c = E_P(d)$, and decryption of ciphertext$c$with private key S by $d = D_S(c)$. For symmetric encryption and decryption, we denote the encryption to ciphertext$c$of data d with key s by $c = E_s(d)$, and decryption of ciphertext$c$with key s by $d = D_s(c)$.

VI.Registration

Before moving all items to the shelves, the store needs to register all of them. We give a design of the RFID tags here shown in Fig. 6.

In our 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, anditismoreconvenientfortheservertomanagethem.

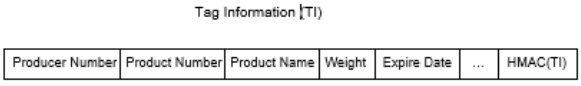

Fig. 6. Tag Design

To prevent a malicious user from rewriting a tag, we create a HMAC appended to the tag for each item. After reading an item, the smart cart needs to first check the HMAC of the item to make sure it has not been modified maliciously. The key $s$used for the HMAC is stored in each smart cart, and the allocation can be done at back-end.

We insist that the tags must be tamper-proof, so that any action on taking off a tag or switching tags between items will lead to a failure. Finally, we utilize the weight scanner on the cart to prevent a dishonest customer from underpaying. If the weight of the items in the cart is greater than they should be, an alarm is triggered. Traditional markets use hidden secure tags such as the Electronic Article Surveillance tags to prevent shoplifting. This idea can also be incorporated into oursystem.

VII.SecurityModel

To make our security model practical, we do not assume the existence of a secure channel. The communications should be resistant to any eavesdropper who actively monitors thetraffic. The security of the system is based on the difficulty of solving the ECDLP, which can not be done in a feasible amount of time.

VIII. Billing Generation OnSmartCarts

As an IoT application, a smart shopping system should involve lightweight cryptographic methods due to limited computational power. We combine symmetric and asymmetric encryption to tackle this issue. When an item is put into a smart cart, the RFID reader on the smart cart should read the tag and then send the tag information to the micro- controller that will then communicate with the server via Zig- Bee to request product information. We adopt ECDSA tosignthe message and Elgamal encryption on Elliptic Curves to encrypt the message. At this point, the smart cart needs to perform the encryption and signing of the message, which are computationally lightweight. To prevent the smart cart from performing the heavy-load, asymmetric decryption work, we let the smart cart randomly generate two symmetric keys $s1$ and $s2$ and send both to the server with its requests. The server then uses $s1$ to encrypt the requested information and creates a message authentication code (MAC) with $s2$. Therefore, upon receiving a message from the server, the smart cart only needs to perform symmetric decryptions and MAC checking.

We propose the following three algorithms to complete the billing generation process. Here we use T to denote thecurrentsystemtime.

In Algorithm 1, the smart cart reads an item, and checks the validation of the HMAC. If the verification passes, the smart cart randomly generates two symmetric keys $s1$ and $s2$: $s1$ will be used for encryption and $s2$ will be used for creating the message authentication code. The smart cart will then sign the tag information together with

its own ID i, a time stamp, and the two session keys $s1$and $s2$, encrypts the message, and sends it to theserver.

Algorithm 2, upon receiving a request from a smart cart, the server decrypts the message and verifies the signature and the time stamp. If the message is valid, the server looks for the requested information $Info(TI)$ for the item in the database, concatenates it with a new time stamp, then encrypts the message using $s1$ obtained from the cart. The server also creates a message authentication code using $s2$ and sends it together with the encrypted message to the smart cart.

In Algorithm 3, upon receiving the response from the server, the smart cart first checks the MAC using $s2$. If MAC is valid, the smart cart decrypts the message using $s1$ and checks if the time stamp is valid. If the verification passes, the smart cart will update the billing information on the LCD display.

IX. Checkout And Verification

Even though the smart cart can generate a billing statement, we insist that a checkout point be equipped with a Point of Sale (PoS) before the store exit. This is to prevent physical attacks on the smart cart's PoS which can be easily moved to areas out of the sights of a store's employees.

To verify that a customer has made a valid purchase for all the items in the smart cart before leaving the store, a RFID reader with a micorcontroller will be installed before the exit door. This RFID reader will read all the items in the smart cart and check with the server if a valid purchase has been made. This can be done by giving all the items two statuses - "for sale" and "sold" - in the server's database, and when an item is paid, the server will be informed immediately to change the item's status from "for sale" to "sold". Therefore, only an honest customer who has paid all the items in the smart cart can pass the verification and the exit door will open for him.

Algorithms for the communication between the RFID reader at the exit door are similar to the one between the smart cart and the server; the only difference here is that, the server isreturning back different information: for smart cart, the server is returning price-related information and for the exit door, the server is returning the status of the items. In short of space, wearenotgivingthealgorithmshere.

We carefully test the reading range of the smart cart in this system. We have found that the metal around the cart is able to block the signals from outside, which is to say, a RFID reader is not able to read the items in a shopping cart unless it is set inside the cart or at the top of the cart. Therefore, the RFID reader on the exit door is suggested to be installed on a high spot in order to read the items in the cart passing by below.

Fig. 7 depicts the checkout point. The user should first pay bill at the PoS. The PoS can either read the billing information from the smart cart via Zig-Bee or a physical cable. After making the payment, the user then walks through the lane to the exit door, where a RFID reader on the top will read all the items in the cart, and verify with the server that everything has been paid for. The exit door will open and let the customer pass if the verification has been passed.

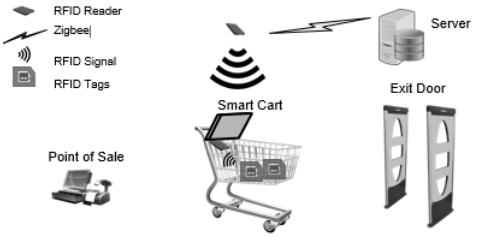

Fig. 7. Checkout Point

X. Security Analysis

We analyze the security of the communication between the smart cart and the server. The communication between the checkout point and the server are the same.

1) **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 iswell-protected.

2) **Integrity***:* The message sent from the smart cart to the server is signed with the smart cart's private key S_s, thus integrity is protected. When the server sends a message back to the smart cart, it creates a 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 iswell-protected.

Algorithm 1 Smart cart sends requests to the server

1: **while** read $TI\ HMAC(TI)$ **do**

2: compute the HMAC using the secret key stored at the smart cart: $HMAC'(TI) = HMAC_s(TI)$.

3: **if** $HMAC'(TI) = HMAC(TI)$ **then**

4: compute $E_{PS}(D_{S\bar{z}}(TI,i,T,s1,s2),TI,i,s1,s2)$,

5: send $E_{PS}(D_{S\bar{z}}(TI,i,T,s1,s2),TI,i,s1,s2)$ totheserver.

6: **else**

7: send analarm.

8: **endif**

9: **endwhile**

Algorithm 2 Server responds to Smart Cart

1:**while**receive$E_{PS}(D_{S\vec{t}}(TI,i,T,s1,s2),TI,i,s1,s2)$**do**

2: decryptthemessage:$(D_{S\vec{t}}(TI,i,T,s1,s2),TI,i,s1,s2) =D_{SS}(E_{PS}(D_{S\vec{t}}(TI,i,T,s1,s2),TI,i,s1,s2))$,

3: Compute$(TI^j,i^j,T^j,s^j_1,s^j_2)=E_{P\vec{t}}(D_{S\vec{t}}(TI,i,T,s1,s2))$,checkif$TI^j=TI,i^j=i$andT^jisvalid.

4: **if** $TI^j= TI$, $i^j= i$and $T^j$is valid, **then**

5: Look for $Info(TI)$ in the serverdatabase.

6: || compute$E_{s1}(Info(TI),T)MAC_{s2}(E_{s1}(Info(TI),T))$andsendsittothesmartcart.

7: **else**

8: discard themessage.

9: **endif**

10: **endwhile**

Algorithm 3 Smart Cart Generates billing information

1: **while** receive $E_{s1}(Info(TI), T)||MAC_{s2}(E_{s1}(Info(TI), T))$ **do**

2: CalculatetheMACusing$s2$:$MAC^j_{s2}(E_{s1}(Info(TI),T))$,andcheckif $MAC_{s2}(E_{s1}(Info(TI), T))$,

3: **if**$MAC^j_{s2}(E_{s1}(Info(TI),T))=MAC_{s2}(E_{s1}(Info(TI),T))$,**then**

4: decryptthemessage:$(Info(TI),T)=D_{s1}(E_{s1}(Info(TI),T)$,

5: **if** T is valid,**then**

6: update the billinginformation.

7: **else**

8: drop themessage.

9: **endif**

10: **else**

11: drop themessage.

12: **endif**

13: **endwhile**

3) **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 notpractical.

4) **One-Time Key***:* Each time a smart cart requests infor- mation from the server, it randomly creates a pair of session keys and sends them to the server. The server uses one key toencryptdataandtheothertocreateaMAC.Thesession keys are generated for each request and are unrelated to the previouskeys.Byadoptingthesessionkeys,thedatasentfromth eservertothesmartcartsiswell-protected.

5) **Tag Security***:* Based on our design, the security of the RFID tags is well-protected. 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 can not be counterfeited by an outside adversary without the secret key. Finally, switching the tags on different items does not work becausepeelingoffthetamper-prooftagswillbreakthem.

Table III:TheComputation Complexities

Computational Overhead	scheme with asymmetric and symmetric operations	scheme with only asymmetric operations
Sever	$R_d+ R_e+ R_s+ C_m$	$2R_d+ 2R_e$
Smart Cart	$tt_s+ R_e+ R_d+ R_s+ 2C_m$	$2R_d+ 2R_e+ C_m$

XI. PerformanceEvaluation

We test the robustness of the system with our prototype, and we find that the RFID reading is accurate and precise. According to our tests, the metal of the cart blocks the signal to a large extent and an item outside the cart can not be read by the reader inside the cart. When a new item is put into the smart cart, it will be automatically read by the reader, which is continually scanning items within its range. After a product is read, its ID will be checked to see if it is a newly added item. If so, its information will be listed on the user interface. On the other hand, when an item is removed from the smart cart, the reader will no longer be able to scan its information. In this case, the smart cart determines that the item has been removedandwillupdatethedisplaycorrespondingly.

We now evaluate the computational and communication overhead of our proposed protocol. We focus only on the communications between the server and the smart cart, as the communication patterns between the checkout point and the server are the same.

A. ComputationalComplexity

We consider the following operations for computational complexity:

- symmetric encryption/decryption:R_s
- asymmetric encryption:R_e
- asymmetric decryption:R_d
- MAC computing:C_m
- symmetric key generation:tt_s

Now we compute the computational complexity for the smart cart and server in one communication.

1) Smart cart: In Algorithm 1, the smart cart initially calculates the HMAC of the item's tag with C_m, and randomly generates two keys within tt_s. Then, it signs and encrypts the message within R_e+ R_d. In Algo- rithm 3, the smart cart decrypts the message from the server using the symmetric key within R_s, and computes the MAC withinC_m.
2) Server: In Algorithm 2, the server decrypts a message within R_d, and checks the signature of a smart cart within R_e. Then, it encrypts the message using the symmetric key $s1$ with R_s, and computes theMACusing the symmetric key $s2$ withC_m.

In our proposed scheme, we combine symmetric and asym- metric encryptions to reduce the computational overhead to a large extent. We compare it with a regular protocol where only asymmetric encryption is used. In such a protocol, the smart cartsignsandencryptsmessagesusingitsownasymmetrickey pairs and the server signs and encrypts the message using the itsownasymmetrickeypairs.Therefore,thesmartcartneeds

Table IV:The Communication Overhead Between Server And A Smart Cart

	Communication Overhead
Algorithm 1	$max\{2n, 320\}$
Algorithm 2	$max\{n + 160, 320\}$
Algorithm 3	0

to first calculate the HMAC of the item's tag with C_m, and signs and encrypts the message within R_e+$R_d$before sending it out. Then, the smart cart needs to decrypt the message from the server using its own private key and then verifies the signature with R_d+ R_e. The server, on the other hand, needs to decrypt the message within $R_d$and checks the signature of the smart cart within R_e. Then, it signs and encrypts the messageusingitsownasymmetrickeypairwithR_d+R_e.

Table III shows the operational complexity for the server andasmartcartintheproposedprotocolandaregularprotocol with only asymmetric encryptions. Computing the MAC and generating the keys are known to be very efficient, and sym- metrickeyoperationsaremuchmoreefficientthanasymmetric key operations [25]. Therefore, the smart cart's computational complexity is mainly determined by R_e(Elgamal encryption on ECC) and R_d(ECDSA). The server, on the other hand, needstodecryptthemessagefromthesmartcarandverifythe signature, thus its computational overhead is also determined by $R_e$andR_d. Note that in our proposed scheme, both the smart cart and the server only needs to perform $R_d$and$R_e$once, which is much more efficient than a scheme with only asymmetric encryptions. Furthermore, while the efficiency is improved, the security is not reduced: the symmetric key pair works as a one-time key and maintains the same level of security.

B. CommunicationComplexity

We choose ECC with 160 bits and MAC with 160 bits, as well. Suppose the size of the data to be sent is n. For simplicity, we do not consider the padding of encryption in ourcalculation.

We consider the communication overhead between the server and the smart cart for one communication: In Algo- rithm 1, the smart cart sends a ciphertext to the server: If n `` 160, the message size is 2n after signing andencryption;

if$n$<160, the message is first signed to be 160 bits, then the signature is concatenated with the message to be

encrypted, yielding 160 + 160 = 320 bits. In Algorithm 2, the server sends a ciphertext and a MAC to the smart cart: If n ‘‘160, themessagesizewillbe$n$+160bits;if$n$<160,themessagesize will be 160+160=320bits. There is no communication in Algorithm 3. Table IV shows the communication overheadbetween the server and the smart cart. The communication overhead between the checkout point and the server is the same, as the communication patterns are identical.

XII. Conclusion AndFutureResearch

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 smartshopping system. We detail the design of a complete system and build a prototype to test its functions. We also design a secure communication protocol and present security analysis and performanceevaluations.

We believe that future stores will be covered with RFID technology and our research is a pioneering one in the de- velopment of a smart shopping system. Our future research will 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 securityproperties.

References

[1] F.Xia, L. T. Yang, L. Wang, and A. Vinel, “Internet of things,” InternationalJournalofCommunicationSystems,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] N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, “Combining cloud and sensors in a smart city environment,” EURASIP journal on WirelessCommunicationsandNetworking,vol.2012,no. 1,p.1,2012.

[4] 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 KnowledgeintheInternet*ofThings(IIKI)2016*,2016.

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

[6] D.M.Dobkin,TherfinRFID:uhfRFIDinpractice.Newnes ,2012.

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

[8] T. Shanmugapriyan, “Smart cart to recognize objects based on user intention,” International Journal of Advanced Research in Computer andCommunicationEngineering,vol.2,no.5,2013.

[9] R. Kumar, K. Gopalakrishna, and K. Ramesha, “Intelligent shopping cart,” International Journal of Engineering Science and Innovative Technology,vol.2,no.4,pp.499–507,2013.

[10] S. Gupta, A. Kaur, A. Garg, A. Verma, A. Bansal, and A. Singh, “ArduinobasedsmartcartInternationalJournalofAdvancedResearch inComputerEngineering&Technology,vol.2,no.12,2013.

[11] Z. Ali and R. Sonkusare, “Rfid based smart shopping and billing,” International Journal of Advanced Research in Computer and Communicationengineering,vol.2,no.12,pp.4696–4699,2013.

[12] P. Chandrasekar and T. Sangeetha, “Smart shopping cart with automatic billing system through rfid and zigbee,” in Information Communication and Embedded Systems (ICICES), 2014 International Conference on. IEEE, 2014, pp.1–4.

[13] M. R. Sawant, K. Krishnan, S. Bhokre, and P. Bhosale, “The rfid based smartshoppingcart,”InternationalJournalofEngineering Researchand GeneralScience,vol.3,no.2,pp.275–280,2015.

[14] 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.

[15] Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-sanitization for preventing sensitive information inference attacks in social networks,” IEEETransactionsonDependableandSecureComputing, 2016.

[16] Z. He, Z. Cai, Q. Han, W. Tong, L. Sun, and Y. Li, “An energy efficient privacy-preserving content sharing scheme in mobile social networks,” Personal and Ubiquitous Computing, vol. 20, no. 5, pp. 833–846,2016.

[17] L. Zhang, Z. Cai, and X. Wang, “Fakemask: A novel privacy preserving approach for smartphones,” IEEE Transactions on Network and Service Management,vol.13,no.2,pp.335–348,2016.

[18] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," ComputerNetworks,vol.102,pp.157–171,2016.

[19] X. Jin, M. Zhang, N. Zhang, and G. Das, "Versatile publishing for privacy preservation," in Proceedings of the 16th ACM SIGKDD inter- national conference on Knowledge discovery and data mining. ACM, 2010, pp.353–362.

[20] C. Hu, R. Li, W. Li, J. Yu, Z. Tian, and R. Bie, "Efficient privacy- preserving schemes for dot-product computation in mobile computing," in Proceedings of the 2st ACM Workshop on Privacy-Aware Mobile Computing. ACM, 2016, pp.51–59.

[21] A. Dasgupta, N. Zhang, G. Das, and S. Chaudhuri, "Privacypreservation of aggregates in hidden databases: why and how?" in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data. ACM, 2009, pp.153–164.

[22] M.Larson,R.Li,C.Hu,W.Li,X.Cheng,andR.Bie,"Abidder-oriented privacy-preserving vcg auction scheme," in International Conference on Wireless Algorithms, Systems, and Applications. Springer, 2015, pp. 284–294.

[23] N. Zhang and W. Zhao, "Privacy-preserving data miningsystems,"

Computer, vol. 40, no. 4, pp. 52–58, 2007.

[24] W.Li,M.Larson,C.Hu,R.Li,X.Cheng,andR.Bie,"Securemulti-unit sealed first-price auction mechanisms," Security and Communication Networks,vol.9,no.16,pp.3833–3843,2016.

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

[26] N. Jansma and B. Arrendondo, "Performance comparison ofellipticcurveandrsadigitalsignatures,"nicj.net/files,2004.

[27] L. Tan and N. Wang, "Future internet: The internet of things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE),vol.5.IEEE,2010,pp.V5–376.

[28] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," Future GenerationComputerSystems,vol.29,no.7,pp.1645–1660,2013.

[29] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and keychallenges," in Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012, pp.257–260.

[30] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "Rfid technology for iot-based personal healthcare in smart spaces," *IEEEInternetofthingsjournal*,vol.1,no.2,pp.144–152,2014.

[31] E.Welbourne,L.Battle,G.Cole,K.Gould,K.Rector,S.Raymer,

M. Balazinska, and G. Borriello, "Building the internet of things using rfid: the rfid ecosystem experience," IEEE Internet Computing, vol. 13, no. 3, pp. 48–55, 2009.

[32] N. Koblitz, "Elliptic curve cryptosystems," Mathematics ofcomputation, vol.48,no.177,pp.203–209,1987.

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

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

[35] R. L. Rivest, M. E. Hellman, J. C. Anderson, and J. W. Lyons, "Responses to nist's proposal," Communications of the ACM, vol. 35, no. 7, pp. 41–54,1992.

[36] Z. Fang, Z. Zhao, X. Cui, D. Geng, L. Du, and C. Pang, "Localization in wireless sensor networks with known coordinate database,"EURASIP Journal on Wireless Communications and Networking, vol. 2010, no. 1, pp. 1–17,2010.

[37] P. Kinney et al., "Zigbee technology: Wireless control that simply works,"inCommunicationsdesignconference,vol.2,2003,pp.1–7.