International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

IoT Applications on Secure Smart System

Shaikh Faizan Hussain, V. V. Yerigeri

Abstract: ***The Internet of Things is altering social lives by associating regular items together. For instance, in a market or stores, all things can be associated with one another, framing a brilliant shopping framework In such system (Internet of Things) IoT framework, a cheap RFID label can be connected to every single item 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, keeping customers from holding up in a long line at checkout point. Alternatively, smart shelving, fitted with RFID readers, can be connected to this smart shopping network and can track stock, perhaps also updating a central server. Extra benefit of this kind of system is that list supervision becomes much easier, as every items can be automatically read by an RFID reader as an alternative of physically look over. To approve the plausibility of such a framework, in this work we distinguish the structure prerequisites of a brilliant shopping framework, fabricate a model framework to test usefulness, and plan a safe correspondence convention to make the framework handy. To the best of our capability, this is the first time that importance is being given to a smart shopping network with safeguards.***

Keywords: Iot, Shopping system, Smart pushcart, Security.

I. INTRODUCTION

Interactions between physical objects became a reality during the Internet of Things (IoT) period. Run-of-the-mill items are connected by computers power and its performance so it's easy to communicate in anywhere in nowadays. This has carried new revolt in manufacturing, environmental as well as financial processes and has sparked problems in wireless communication, data management and decision-making in real-time [1]. In addition, numerous subjects for safety and protection have been developed, and lightweight cryptographic strategies are sought to suitable in through IoT uses.

II. LITERATURE REVIEW

Studying IoT implementations in recent times is a common subject but this type of shopping systems have not been well examined.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Shaikh Faizan Hussain*, Master of Technology in Digital Communication Department, MBES College of Engineering, Ambajogai, India. Email: skfaizanhusain@gmail.com
V. V. Yerigeri, Professor at Digital Communication Department, MBES College of Engineering, Ambajogai, India. Email: vaijanatha_y@rediffmail.com

In recent years several research studies have been conducted on enhancing the shopping experience of customers. Klabjan et al. In 2011 [2] projected following a client in the store and finding clients' inclinations so as to offer customized coupons. Smart shelves and smart carts were additionally talked about in their work. In this System carts can be followed utilizing RFID innovation and smart shelves can screen the status of the things. In 2003, there were different endeavors completed. Shanmuqaprivan et al. projected a structure utilizing RFID and a standardized tag peruser for item distinguishing proof, while utilizing Zig-Bee for correspondence [3]. Kumar et al. spoken to the main bodily execution with Zig-Bee and RFID [4]. Gupta et al. gave the whimsical plan for a smart basket in brilliant shopping framework, and they're among the primary guides to statement the counter robbery in a smart shopping system [5]. Their plan was like a mail container: a chute where things are embedded and checked, at that point released into a shut chamber. The chamber had an entryway on the top which must be opened if the client or client had paid for all things. The plan in a roundabout way made preparations for remote correspondence security dangers by not permitting any remote correspondence - materially wired to a restricted degree of-offer system to pay when the client or customer was finished shopping. Ali et al. proposed a smart cart system with mapping or steering [6]. Their concept included adding smart shelves, which firm when smart carts enter an aisle (using infrared sensors) and delivered product information to carts.

In the last few years there have been more developments in this field [7]–[8], but neither of them contained new ideas. In all the previous prototypes a consumer had to search and scanned the products manually, this is not so easy and suitable. Moreover, In no past work has security issues been investigated. RFID innovation has been generally considered in ongoing not many eons and it is a significant and significant innovation practical in IoT uses. [10] – [11]. Amendola et al. explored the RFID innovation and its utilization for uses on body-centric frameworks [12]. Welbourne et al. built up an RFID ecology with a set of electronics, client level apparatuses and uses [13]. For grocery supplies and goods promoting, most stores are utilizing standardized tags these days for things, however we have motivation to accept that RFID is a general pattern. RFID can accomplish separation perusing, which mentally brings the possessions of IoT and associate every one of the items in a store together.

III. METHODOLOGY

In this system its work on its flow chart as shown in figure. This system has some different component which uses there work to perform properly.

In this type of system there is some restriction and limitation for its software to uses because when there is no limitation is set then there will be chances of some misuse of that network.

This is smart cart because of its ability to scanned the tag by its reader and its geographically area is made by steel because of its design it's impossible to read others cart items accidently and its design make it more convenient and cannot read outside items tag. So it's only read its item within it.

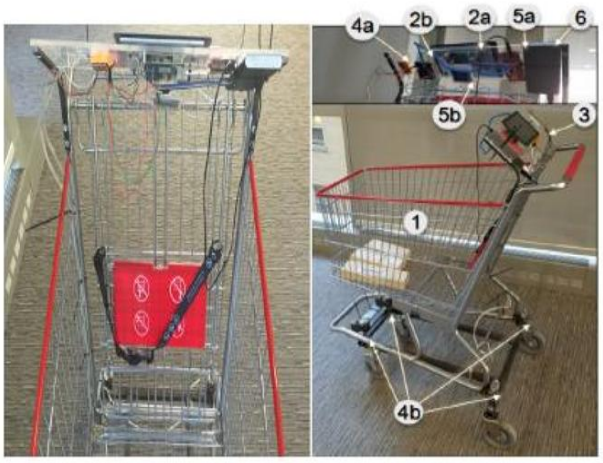

Fig. 1.Smart Cart

Table I. Specification of components

No.	Utility	Mechanisms	Explanation
1	Pushcart	Shopping Cart	Normal Steel Casing
2	RFID Reader	1.Antenna of polarized circularly 5db 2.long range UHF reader	1-Global freq. 840 to 960 MHz , 2-EPC GEN2 , 3-Antenna power 20dBm max
3	Showing Screen	Touchscreen LCD Display Raspberry Pi related	1-Display @ 60fps 2-RGB 800480 3- FT5406 10 point 4-24-bit color
4	Mass Detecting	1- 4xHalf Bridge Load Sensors 2- HX711 ADC	1- Analog-to-Digital Converter 2- Signal Amplifier
5	Micro-processing Unit	1-Arduino Uno 2-Raspberry pi 3	1-Bluetooth 4.1 2-802.11n Wireless LAN 3-1.2GHz 64-bit quad-core ARMv8 CPU
6	Power Supply	12000 mAh Power Bank Universal compact battery	1-Two USB output ports (2.1A and1A) 2-Charge input of 5V/1 A

The server speaks with the smart shelves, smart cart, and checkout focuses. The smart shelves can screen the things on the shelves by perusing the RFID signals from the labels; the smart cart can read and recover data of the things in the carts at last, the checkout focuses can approve the buy finished by a buyer.

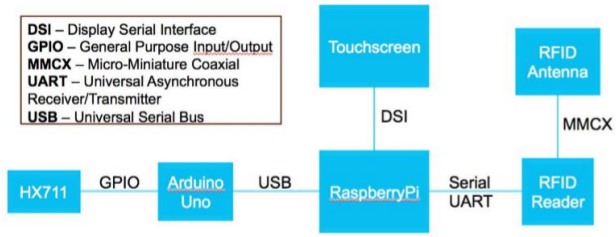

Fig. 2.Work flow of the smart basket or cart

Fig. 3.Structure

As its all iot application, a smart shopping system ought to include lightweight cryptographic strategies because of restricted computational power. There is two issue to handle 1. Symmetric & 2. Asymmetric encryption. When customer is add some product in a smart cart then its read information from its cart reader and sends to server via zigbee request communication for product.

We adopt ECDSA to sign the message and Elgamal encryption on Elliptic curves to encrypt the message. In the cart there should be light weight of the encryption and signing message computationally not to heavy load.

Asymmetric Encryption, in this it generates two keys by its server request i.e. M1 and M2. M1 to encrypt the requested information and create a message authentication code (MAC) with M2.so after receiving message from server smart cart does decryption and check MAC.

Then billing generation process there is algorithm 1: cart reads piece and validate. When verification passes then it automatically generates two keys M1 and M2. M1 used for enc1ryption and M2 used to MAC creation then its reader sign information by its ID and time stamp .then two session key will start M1 and M2 encrypt message and sent to server.

2: After receiving request server decrypt message and verified the signature and time stamp. When message is valid then its server check in its database and give it's with new stamp. And after encrypt messages using M1.it also create M2 (MAC) and send encrypted message to cart.

3: In this last algorithm, when receiving response from server its check MAC by M2. When MAC is valid its decrypt the message using M1 and check time stamp is valid then whole verifying then its update its billing process information on LCD.

A. 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
Step11 else go to Step12
Step11: Server generates the bill and prints the bill
Step12: Stop

IV. RESULT

A. Elliptic Curve Cryptography (ECC)

In 1985 Koblitz [14] and Victor [15] 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 [16].

Let Fp represent the field of integers module p and an elliptic curve E over Fp is defined by the equation: $y^2 = x^3 + ax + b$ (1)

Where a,b $\in$Fp and $4a^3+27b^2 \neq 0$ (mod 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.

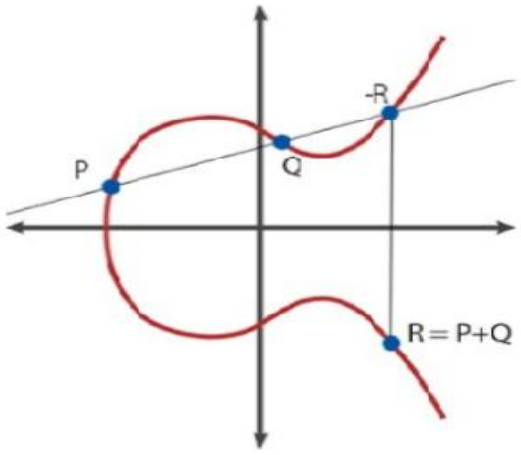

Fig. 4.Group Law arranged an Elliptic Curve

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 [16] 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 II. Security Comparison of Various Algorithm [9]

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

V. ADVANTAGES AND DRAWBACKS

A. Advantages

From this system all problems related to queue, timing, information and etc. in shopping is solved. Because when smart cart is placed and cart which only read RFID tag of that product and easily added its information of product and also its price it's easy to use and handy and also when you remove any item from this it's also discarded or removed that particular product price and information so it's very convenient. It also consume time suppose is there any long queue then you will safely go through that shop by easily paying that bill only in your busy schedule.by this cart shelves it's also store product expiry date and info of price related to product so it's also going easy for inventory management section. By applying this to stores and shops we can smarty add this gadget and take a use of this in our day to day life. And also by customer liking and choices we can also build our business strategies well.

B. Drawbacks

Everything is have a good and bad page also here is same. System is very good within its mechanism but it take microcontroller, RFID tags, Zig-Bee etc. which having also a smart cart .suppose its around 60000 product in a store it will require all products attached to RFID tag and which cost around nearly 1 million which is expensive for this although it's a onetime investment but its maintenance and repairing it's also takes cost more .its expensiveness is major drawback and also its maintaining all tags and checking all information is correct is also an issue for big stores and mall of in this type of system.

VI. 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.

ACKNOWLEDGMENT

First of all I wish to express my gratitude and thank to my project guide Prof. V. V. Yerigeri, for his valuable suggestions from time to time, continuous encouragement, and constant support.

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. 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.*
3. T. Shanmugapriyan, "*Smart cart to recognize objects based on user intention*," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 5, 2013.
4. 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.
5. S. Gupta, A. Kaur, A. Garg, A. Verma, A. Bansal, and A. Singh, "*Arduino based smart cart*," International Journal of Advanced Research in Computer Engineering & Technology, vol. 2, no. 12, 2013.
6. Z. Ali and R. Sonkusare, "*Rfid based smart shopping and billing*," International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 12, pp. 4696–4699, 2013.
7. 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.
8. 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.
9. N. Jansma and B. Arrendondo, "*Performance comparison of elliptic curve and rsa digital signatures*," nicj. net/files, 2004.
10. 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.
11. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "*Future internet: the internet of things architecture, possible applications and key challenges*," in Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE, 2012, pp. 257–260.
12. S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, "*Rfid technology for iot-based personal healthcare in smart spaces*," IEEE Internet of things journal, vol. 1, no. 2, pp. 144–152, 2014.
13. 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.
14. N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.
15. V. S. Miller, "*Use of elliptic curves in cryptography*," in Conference on the Theory and Application of Cryptographic Techniques. Springer, 1985, pp. 417–426.
16. D. Hankerson, A. J. Menezes, and S. Vanstone, Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.

AUTHORS PROFILE

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.