International Journal of Engineering and Techniques - Volume 4 Issue 3, May - June 2018

RESEARCH ARTICLE OPEN ACCESS

IoT Application on Smart and Secure Shopping System using RFID, Zig-Bee and Gossamer Protocol

Purva S. Puranik[1] , Parikshit N. Mahalle[2]

*1(*Department of Computer Engineering, Smt Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India)

2(Department of Computer Engineering, Smt Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune, India)

Abstract:

Anything that can be connected to a network qualifies to become a smart object. Exciting use cases and products can be generated by interconnecting these smart objects with the internet. A secure and smart shopping system is one such use case developed using IoT. In a departmental store all items can be connected with each other. This leads to formation of a smart shopping system. In such an IoT system, an inexpensive UHF RFID tag can be attached to each product. On the other hand, each shopping cart can be equipped with an UHF RFID reader. Along with it, the smart cart will also have a microcontroller, an LCD touchscreen, a Zig-Bee adapter, and a weight sensor. The smart cart is able to proactively read the items put into a cart via the UHF RFID reader. A micro controller is installed on the cart for data processing whereas the LCD touchscreen is for the user interface. Zig-Bee technology can be used for communication between the smart cart and server. Weight scanner installed on the smart cart ensures that no malicious customer can buy products without paying for them. At the checkout point, the customer pays using the generated billing information on the smart cart. To ensure that that all the items in the cart have been paid, RFID reader can be used before the exit door. Using cryptographic methods for communication between the server and smart cart, security of data will be guaranteed, as no outside adversary will be able to gain hold of the data transferred. This makes the system confidential and maintains integrity. In addition to this, in order to protect the RFID system from DoS attacks, Gossamer protocol can be implemented which will ensure an even more secure system. Having such a system gives two benefits. Firstly, it prevents customers from waiting in a long queue at checkout. Secondly, by making the product shelves smart inventory management becomes easy and efficient. Implementation of such a smart shopping system and secure shopping system will ensure enhanced shopping experience.

Keywords – IoT (Internet of Things), Smart Shopping, Secure Shopping, Smart Cart, RFID (Radio Frequency Identification), Gossamer protocol.

I. INTRODUCTION

Today the Internet has become ubiquitous and has seeped into almost every working sector in every corner of the world. It is affecting human lives in marvellous ways. 'The era of Internet of Things' is here. The term Internet of Things (IoT) transpired in 1999.The person behind coining this term was Kevin Ashton, co-founder of MIT's Auto-ID Centre. The network of devices equipped with sensors and computing facilities sense and collect the data from environment and then share that data across the internet where it can be processed and utilized for various interesting purposes. IoT has continued to grow and to evolve due convergence of multiple technologies. The core infrastructure of an IoT framework is formed by sensors and actuators, connectivity, process and people.

Quick and easy payment of bills in supermarkets is one dream which every shopper visualizes of. This article paper reflects the proposal of a smart cart that will be capable of generating a bill from the cart itself. The smart cart uses RFID and Zig-Bee technology for shopping and payment. [1]

RFID (Radio frequency identification) is a form of wireless communication which is used to uniquely identify an object, animal or person. RFID tag and RFID reader are two key components. RFID tag contains a memory element which stores certain information, a microchip along with an antenna. Radio frequency waves are transmitted by the RFID reader,

and whenever the tag comes into vicinity of the reader it is activated. Such an activated tag sends information from its memory to RFID reader in the form of wave. Whereas, Zig-Bee is based on an IEEE 802.15 standard. Zig-Bee devices form a mesh network and transmit data over long distances through such intermediate devices.

Thus, a smart shopping system can be formed, in which, each and every product is equipped with a RFID tag whereas RFID readers are attached to smart carts as well as smart shelves. Such a system will keep the track of all the purchased products and generate a bill based on this information. The customers will be able to see the list of items they have bought themselves on the LCD screen attached to the smart shopping cart, will keep updating the total. Thus, the billing information will be generated pro-actively without any human intervention. The customer has to just pay the billing amount generated on the LCD screen at the point of sales. The smart cart will communicate with the server via Zig-Bee technology and using a micro-controller. As an IoT application, a smart shopping system should involve lightweight cryptographic methods due to limited computational power. We can combine symmetric and symmetric encryption to tackle this issue. Thus, having such a secure and smart shopping system will definitely be beneficial, as it enhances customer's shopping experience as well and helps in efficient inventory management process.

II. MOTIVATION

The existing shopping system model highly relies on use of barcode. Every product kept in a departmental store has a barcode attached to it. A barcode is a visual representation of data that is scanned and interpreted for information. However there are slight disadvantages associated with barcode. Barcodes are always exposed on the outside of the product, due to which they are prone to damage. Barcode scanners need a direct line of sight to the barcode to be able to read. Thus, each product has to be individually scanned. This disadvantage of barcode contributes in making the billing process quite slower in departmental stores. This indeed results in long queues at cash counter which dulls the customer experience of shopping. In existing shopping system, inventory management is done manually. Which products are out of stock and which need to be refilled or replaced is only known when a store assistant looks after it. This results in tiresome jobs. These disadvantages certainly demands for an automated and efficient system.

III. LITERATURE SURVEY

In the year 2013, 'Intelligent smart cart' idea was proposed by Raju Kumar et al.[2] The main aim of this proposed system was to develop an intelligent shopping cart which can be used in shopping stores, where in each product in the store with will equipped with RFID for identification of product. This intelligent shopping cart will also have LCD screen attached to it which will inform customers about product prices, discounts, offers and the total bill. Consistent Wi-Fi connection with the shop's server is extremely essential. The fact that a cart pro-actively generates billing information, frees the staff from repetitive scanning and thus increases operational efficiency of the system.

A paper titled, 'RFID Based Smart Shopping and Billing' proposed by Zeeshan Ali et al talked about designing a smart cart system with navigation. [3]The design proposed included the implementation of smart shelves. When smart carts enter an aisle, product information is delivered to the carts using infrared technology. Proposed system is based on four important technologies: Infrared sensors which are used in an intelligent manner for dynamic location detection and tracking, RFID tags for product identification, Zig-Bee for achieving wireless communication with Server, and integrating system with display for billing and inventory management.

IV. GAP ANALYSIS

Various works has been carried out so far to upgrade the existing shopping system by introducing smart and intelligent carts. However, most of the similar systems implemented fail to provide security. The communications between server and other entities of smart shopping system should be resistant to any eavesdropper who actively monitors the traffic. The data which is transferred from server to other entities in the smart cart can be processed further to obtain information about discounts offered by the store, customer preferences, etc. Hence, we want this information to remain secure so that no other competitor can steal it for one purpose to plan business strategies, personal gains, etc. Thus, such a smart shopping system should involve lightweight cryptographic. Therefore, having such a secure and smart shopping system will definitely be beneficial, as it enhances customers shopping experience as well and helps in efficient inventory management process.

V. SYSTEM ARCHITECTURE

Each and every item the store is equipped with ultra-high frequency passive tags. The proposed smart shopping system consists of a smart cart which is equipped with a microcontroller such as Raspberry Pi which coordinates with RFID reader, Zig-Bee Adapter, LCD Display and weight scanner attached to the cart. Fig 1 depicts the components of a smart cart. The RFID reader reads the information stored on tags attached to the product in the store and transfers it to the server where all the product information is stored via microcontroller. Zig-Bee technology is used for wireless communication between server and smart cart. The LCD screen which is attached to the cart displays the billing information generated by the smart cart. If a malicious user peels off the RFID tags before putting it into the cart then, this weight goes undetected by the weight scanner and thus helps in security.

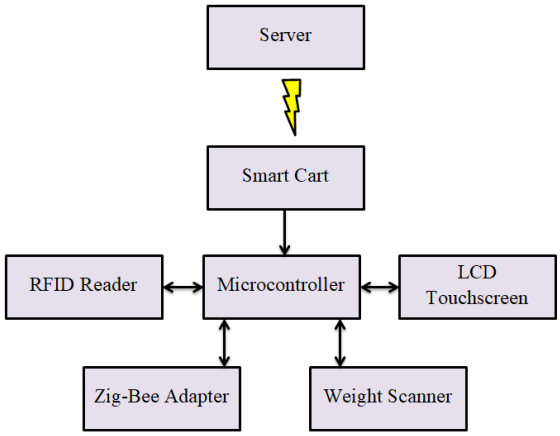

Fig 1: Smart Cart Components

Shelves are also made smart by attaching RFID readers to them. Status of the item, stock information regarding out-of-stock products, customer preferences, refilling of certain items or expiry of products, etc. can be transferred from the smart shelves to the server using Zig-Bee. To ensure that all the items purchased by the customer have been paid, and RFID reader is installed before checkout. So the any underpay will trigger an alert. For this, all the products in the store have either status 'for sale' or 'sold', stored in server database. When payment is done for a product, its status changes to 'sold' in server database. Thus, only an honest customer who has paid for all the items bought can leave the store. Fig 2 shows the system model of the proposed system.

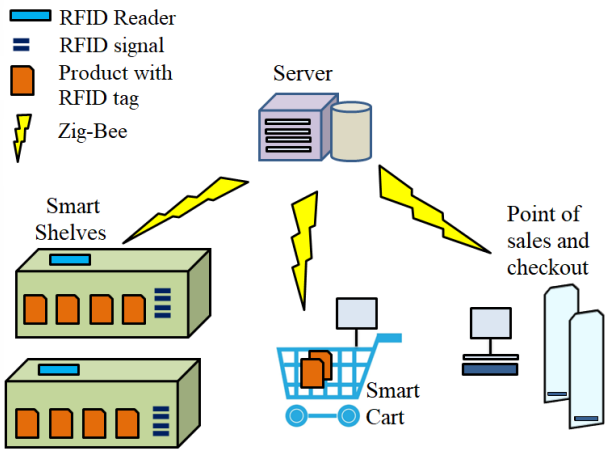

Fig 2: System Model

All the products placed on the shelves are first registered and RFID tags are attached to them. The database at the server end stores the information such as price, location, etc. 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. The encryption and signing of the message is performed by the smart cart further. For this, two symmetric keys s1 and s2 are generated by smart cart and are sent to the server along with its request. S1 is used to encrypt the requested information and s2 for creating a message authentication code (MAC). When the server receives the message it performs symmetric decryption and MAC checking.

Three algorithms are used to complete the billing generation process. [1] Current system time is denoted by T.

a. Algorithm 1: Validation of HMAC present on the tag is performed by the smart cart when it reads the product RFID tag. If the verification passes, the smart cart randomly generates two symmetric keys s1 and s2. S1 is used for encryption and s2 for creating the message authentication code. The smart cart then signs the tag information together with its own ID i, a time stamp, and the two session keys s1and s2, encrypts the message, and sends it to the server.
b. Algorithm 2: When server receives this request from smart cart, it 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.
c. Algorithm 3: After 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.

Major goal which this secure and smart system must accomplish is that appropriate item reading. That means, there may be occasions wherein a customer put an item into a cart and later removes it from the cart. The smart cart should be smart enough to detect this change. That is it should accurately read items put into or removed from the cart. Also, an item put into one cart should not be able to be read by another cart nearby. There might be a chance when a dishonest customer will try to leave the store without making a payment, for this payment verification is must. The confidentiality and integrity of the system are maintained as for every session new session keys are generated which are used by the smart cart and server for communication. The time stamp T provides resistance from replay attacks. Moreover, swapping of the tags cannot be done as they are tamper proof and the HMAC present on the tag is validated before the bill is generated. Hence, this makes the smart shopping system secure.

VI. ADVANTAGES AND DRAWBACKS

A. Advantages

Existence of a smart and secure shopping system using IoT, improvises the entire shopping system. Customer experience is elevated as they no longer have to wait in long queues at the checkout point for their billing information to be generated. The billing procedure is done in the smart cart itself with the help of RFID technology and the customer can easily view the products he/she has bought on the LCD screen equipped with smart cart. Thus, before stepping out of the store only the total billing amount generated on the smart cart needs to be paid, this consequently reduces waiting time. Such a system also reduces the efforts required for inventory management. Smart shelves can easily detect which products are out of stock, while products have expired, which shelf needs to be refilled, etc. Moreover, information such as customer preferences or customer liking for a specific brand related to a certain item can be obtained easily. This information will indeed help for future planning and developing business strategies. By having an efficient security model, confidentiality and integrity of the information in such a system is also ensured. Thus, implementing such a smart and secure shopping model in a store is a smart move.

B. Drawbacks

A smart and secure shopping system mainly relies on RFID technology, Zig-Bee, and micro-controller. For having such a system, each and every product in the store needs to have an RFID tag attached to it. Considering the usage of UHF RFID tag on each item, and assuming that our store has around 50,000 items, the cost of the having products with RFID tags rise well above 1 million which is costly. Adding to this, cost of converting every cart to smart cart, every shelf to smart shelf and building the entire infrastructure is quite high. Though this is a one-time investment, yet the future repairing and maintenance also needs to be taken into account. Thus, from this point of view, implementation of such an efficient system into reality is expensive which is a major drawback as of now is.

VII. ATTACKS AND MITIGATION

The proposed secure and smart shopping system heavily relies on RFID technology. The communication channel between the reader and the tag is insecure, whereas a secure RF communication channel exists between the reader and the backend database. The usage of RFID technology is increasing tremendously, tag numbers are increasing rapidly and tag sizes are shrinking. Indeed, the threats are receptive to similar evolving. Thus, it becomes necessary to design lightweight and effective intrusion detection and prevention mechanisms for RFID systems. The Denial of Service (DoS) attack can impair the communication between legitimate tags and readers. [4] DoS attacks can be broadly classified based on the factors causing them. [5]:-

1. Kill command Attack: RFID tags can be given a password when they are manufactured. However, the tag passwords can be easily cracked using brute force techniques. The tags can be disabled permanently if the attacker issues a kill command along with the password.
2. De-synchronization attack: The authentication capability of a RFID tag is disabled by destroying synchronization between the tag and the RFID reader.
3. Jamming: The communication between tags and readers can be prevented using electromagnetic jamming.
4. Tag Data Modification: DoS can also be launched by modifying the EPC data on RFID tags to a random number that is not recognized by the reader.

Many techniques and protocols have been proposed to prevent DoS attacks on RFID systems. The Gossamer protocol is one such protocol proposed by Peris-Lopez et al to prevent DoS attacks on RFID systems. This protocol belongs to the UMAP (ultra-light mutual authentication protocols) family of protocols. [5] The four classes of RFID tags identified by the EPC system are: Class 1 – Identity tags, Class 2 – Higher functionality tags, Class 3 - Semi-passive tags, and Class 4 - Active tags. The Gossamer protocol has been designed specifically for Class 1 RFID tags, which are passive tags and thereby do not have their own power source, that is, they depend on the RFID reader to be energized. [6] Thus, the Gossamer protocol is an authentication protocol for RFID systems, targeting low cost passive RFIDs.

A legitimate reader makes use of an index pseudonym to retrieve tag information. The tags and readers share sub keys which are part of a single key, then these sub keys are used to build the messages exchanged in the mutual authentication phase. [5]The basis of this protocol are the bitwise logical operations such as AND, OR and XOR. The tags make use of the pseudorandom number generated by the reader for creating messages. Three stages in which the Gossamer are: tag identification phase, mutual authentication phase and updating phase. A static identifier (ID), an index pseudonym (IDS), and two keys (k1, k2) are stored in each tag. The analysis of Gossamer protocol states that it is efficiently in providing protection against DoS attacks and replay attacks also. Such a protocol can thus be implemented in shopping system too, which will make it further more secure.

VIII. CONCLUSION

The proposed secure smart shopping system utilizes RFID technology, Zig-Bee technology as well as the Gossamer protocol which is employed in improvising shopping experiences by making it smart and at the same time incorporating security aspects in the system. By doing so, the departmental stores will also benefit by fast and accurate inventory, improved customer service, etc. Future research for reducing cost of the system and improvising this current system, for example, by reducing the computational overhead at the smart cart side for higher efficiency, and the communication efficiency while preserving security properties will future upgrade this system .I believe that the future stores will be covered with RFID technology and this proposed

smart and secure shopping system will be pioneering one in the development of future stores.

IX. FUTURE SCOPE

The proposed secure and smart shopping system can further be improvised and efforts can be taken to reduce its overall cost. Instead of having smart cart, we can make the point of sales smart. A smart lane can be place before each point of sale (POS).This lane can be made similar to metal detectors used in mall currently, in terms of physical look. RFID reader, computing device and other peripherals which are attached to smart cart can instead by attached to this lane which will make it smarter. Whenever, a customer is done shopping, he/she will pass through this smart lane. The RFID reader attached to on this lane will detect all the items in the cart and communicate with the server via Zig-Bee. Technically, all RFID readers can obtain data from only one tag at a time. If two or more tags are sending signals to the same RFID reader simultaneously, there is no way for the in which the reader can distinguish between them. However, there are special anti-collision algorithms that enable interrogators to 'singulate' on specific tags, which is, a reader can talk to one tag at a time, but in very rapid succession. This interrogating of the RFID tag by the reader is done so fast, that it creates an illusion that many tags are being read at once. This property can be utilized, so that as soon as the customer places the cart in the lane, all the products and scanned within few seconds and as soon the customer walks out of this special lane, the billing information is generated on the LCD screen at the point-of-sale, specific to that customer's cart. Thereafter, the customer has to just pay for the billing amount generated and walk-out of the shop.

The proposed secure and smart shopping system can be upgraded further in several aspects. Customer loyalty cards that are equipped with an RFID tag containing a customer identification number can be introduced which will amplify shopping experience to great extent. The database at the server can use this number for retrieving the customer profile, preselected settings, etc. based on which special offers and discounts can be given to that customer.

The smart carts proposed are equipped with an RFID reader and a display. The customer can see this list of products in cart on the display and is constantly aware of the total value of the content. These smart carts can be further made smarter so that customers can also use the display for requesting: estimated arrival dates of products that are out-of-stock, new product arrivals, discount offer information, additional product information, etc.

The proposition of smart shelves completely modifies the replenishment operations of grocery items in a departmental store. Instead of having employees looking around for empty places on the shelves, the smart shelves can notify when a product need replenishment. In future, the system can be modified in such a way that it also warns when a product is misplaced on the wrong shelf. For example, if a pack of meat has is placed in the normal shelf instead of cold storage, then that can be immediately removed and put back in the meat counter, before it's ruined and unsellable. Thus, automatic replenishment and misplaced product alerts is one feature which future stores can definitely incorporate.

Furthermore, virtual closets, smart mirrors, etc. will revolutionize smart systems. The introduction of IoT in retail sector will be a paradigm shift. It will completely transform the way the system works right now. Shopping as we know it, will not disappear, but will be enhanced tenfold or perhaps even a hundredfold.

REFERENCES

[1] 'IoT applications on Secure Smart Shopping System', Ruinian Li1,et al , IEEE Internet of Things Journal(Volume: 4, Issue: 6, Dec. 2017)

[2] R. Kumar, K. Gopalakrishna, and K. Ramesha, 'Intelligent shopping cart', International Journal of Engineering Science and Innovative Technology, (vol. 2, no. 4, pp. 499507, 2013.)

[3] 'RFID based smart shopping and billing', Z. Ali and R. Sonkusare, International Journal of Advanced Research in Computer and Communication Engineering, (volume: 2, no.12, pp. 46964699, 2013.)

[4] D. Tagra, M. Rahman and S. Sampalli, 'Technique for Preventing DoS Attacks on RFID System's', Proceedings of the 18th IEEE International Conference on Software, Telecommunications and Computer Networks (IEEE SoftCom 2010),(pp. 6-10, Split-Bol, Croatia. September 23-25, 2010.)

[5] A. Juels,'RFID security and privacy: A research survey', IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, Feb. 2006, pp. 381394.

[6] 'Power Analysis of the Gossamer Protocol for Passive RFID Tags', N. Rama and R. Suganya, International Journal of Wireless Networks and Communications, Volume 2, Number 1 (2010), pp. 1--14