Enhancing Security Issues in IoT based Smart Retail using Blowfish Algorithm

Sudhanshu S. Kamble
Department of Electronics
Dr.D.Y.Patil School of Engineering, Charholi (Bk),Via Lohegaon,Pune.

S. S. Sonavane, PhD
Department of Electronics
Director of Dr.D.Y.Patil School of Engineering, Charholi (Bk), Via Lohegaon, Pune.

ABSTRACT
Security is a measure concern while sending and receiving data over internet. In this paper smart trolley system is designed for the shopping mall or complex is a place where people do shopping and buy product and nowadays this is becoming a daily activity. In proposed system, RFID based smart trolley system is implemented. Trolley consists of circuitry with RFID module and the Zigbee module. Each product has given a RFID tag. RFID reader reads product details from the tag and sends it to PC through Zigbee wireless communication. For the payment, data is encrypted using Blowfish encryption algorithm which strengthens the security of the data. Performance of the blowfish algorithm is measured through average encryption time, memory usage and battery consumption.

General Terms
Security, Encryption, Cryptography, IoT

Keywords
Cryptography; Security; Zigbee Module; Blowfish Algorithm; RFID Module.

1. INTRODUCTION
In metro cities, shopping and purchasing at big malls is becoming daily activity and also number of small and large malls are increasing throughout the global due to public demands as there is big rush at these malls on weekends and holidays. When there are special offers and discounts on products crowd becomes huge [1]. Customer purchases products and put them in the trolley. After total purchasing of products one need to go for payment counter. At payment counter using barcode reader cashier prepares bill which is very time consuming process this results in long queue at the payment counter [2].

The increase in computing, networking expansion and threats increased the need for perpetually managed security. Data security helps to keep data privately [10]. Cryptography is the technique converting original data into non readable format which is called as cipher text. Cryptography algorithms are classified into two types symmetric and asymmetric algorithms. In symmetric cryptography single key is used for encryption and decryption. In asymmetric cryptography two keys are used namely private and public key. Data is send in cipher text format over insecure network environment. Cipher is a pair of algorithms which creates the encryption and the reverse decryption of the original data. There are various applications of cryptography including computer passwords, ATM cards, and electronic commerce

[9]. There are various basic algorithms of cryptography used for security purpose such as Data Encryption Standard (DES), Blowfish, Advanced Encryption Standard (AES), MD5, and Triple DES. But out of these Blowfish is very fast and secure algorithm for providing security and managing passwords[9].

This paper is organized as follows: Section II gives the block diagram of the proposed system also flow of system and details of the methodology used. Blowfish algorithm and its process of encryption are discussed in Section III. Software's used for implementation are described in section IV. Section V describes results of proposed system. Finally, conclusion is given in Section VI.

2. PROPOSED WORK

2.1 Block Diagram of Proposed Scheme

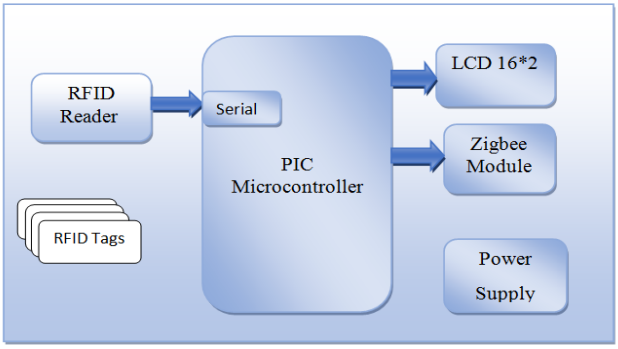

Fig 1:Block Diagram of the trolley unit

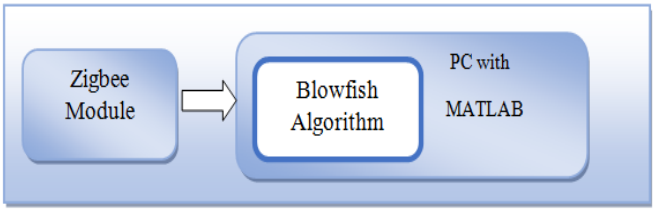

Fig 2: Block Diagram of the receiver side

Proposed System consists of two units such as trolley unit and receiver side unit. Trolley unit consists of PIC microcontroller, RFID Module, Zigbee Transmitter and LCD. The receiver side unit consists of and PC with MATLAB software and Zigbee Receiver with MATLAB software. Suppose all products in the mall are equipped with RFID tag. When customer puts product in the trolley, its code will be detected by the RFID reader[3]. RFID reader requires 5V power supply for its operation for its operation. RFID reader sends this data to PIC microcontroller through serial communication. It is serially interfaced with the microcontroller. Controller matches this code with the code which is stored in the microcontroller. Controller reads product cost and other details and then displays it on LCD. Microcontroller sends this data to PC through wireless Zigbee transmitter [8]. In the receiver side, there is Zigbee receiver it

receives data and sends it to the PC. It receives detail about the product like cost, quantity etc. and total bill. In PC, blowfish algorithm is implemented for making payment of the bill of products. It sends details bank through blowfish encryption algorithm. It makes the payment and receives payment acknowledgment details on the PC.

2.2 Implementation Flow

Step1: Start and initialize the system.
Step2: Put product in the trolley.
Step3: Search for RFID tag on the product.
Step4: Read details of the product from the RFID reader.
Step5: Display details of the product on LCD.
Step6: Send data to PC through Zigbee transmitter.
Step7: Receive data through Zigbee receiver.
Step8: Send received data to PC.
Step9: Make payment trough blowfish algorithm based Payment gateway.
Step10: Receive successful payment details back on the PC.
Step11: Stop the system.

3. BLOWFISH ALGORITHM

3.1 Proposed Data Encryption Model

In this proposed model, data security has been obtained by encrypting and decrypting the data using cryptography. The proposed model uses blowfish encryption algorithm for enhancing the data security while transferring data overpayment gateway.

The proposed method consists of 4 phases in encryption and decryption [10].

Encryption Part:

1. Input Original Data
2. Key Generation
3. Encryption
4. Generate Encrypted Image

Decryption Part:

1. Input Encrypted Data
2. Input key
3. Decryption
4. Get Original Image

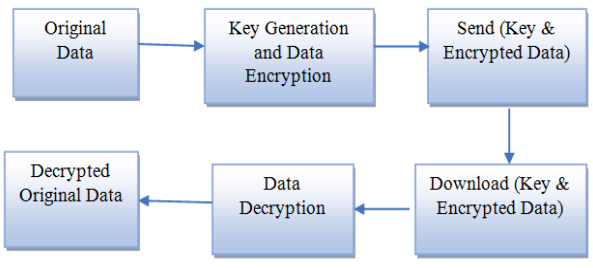

Fig 3: Design of proposed model

Proposed model consists of two modules such as encryption module and decryption module. In encryption module data is encrypted using some encryption algorithm. In this paper blowfish encryption algorithm is used. This encrypted data is transmitted and then decrypted at the receiver end.

3.2 Blowfish Encryption Algorithm

Blowfish is a symmetric encryption algorithm. Symmetric encryption means it uses the same secret key for both encryption and description. Blowfish is a cipher block it divides the message into fixed length blocks during the process of encryption and decryption. Block length is 64 bits and the messages which are not multiple of 8 bytes they are padded. It is based on fiestel network [7].

Blowfish Algorithm consists of two parts:

1. Key-expansion

During key expansion, it converts a key of 448 bits into subkey that will total count into 4168 bytes. Blowfish uses large number of sub keys [5].

2. Data Encryption

In data encryption function is used to iterate 16 items of the network. In each iteration it performs key-dependent permutation and data-dependent substitution.

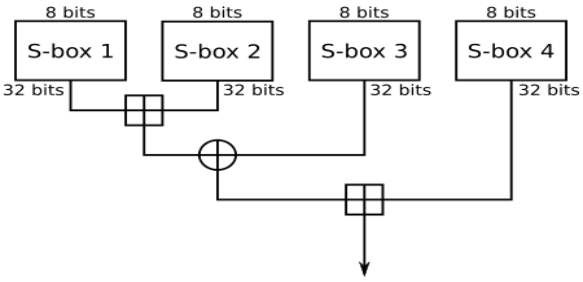

Fig 4: Function F

All the operations in the algorithms are XORs or additions on 32-bit words. Some additional operations needs to be performed which are four indexed array data lookup tables for each iteration [5].

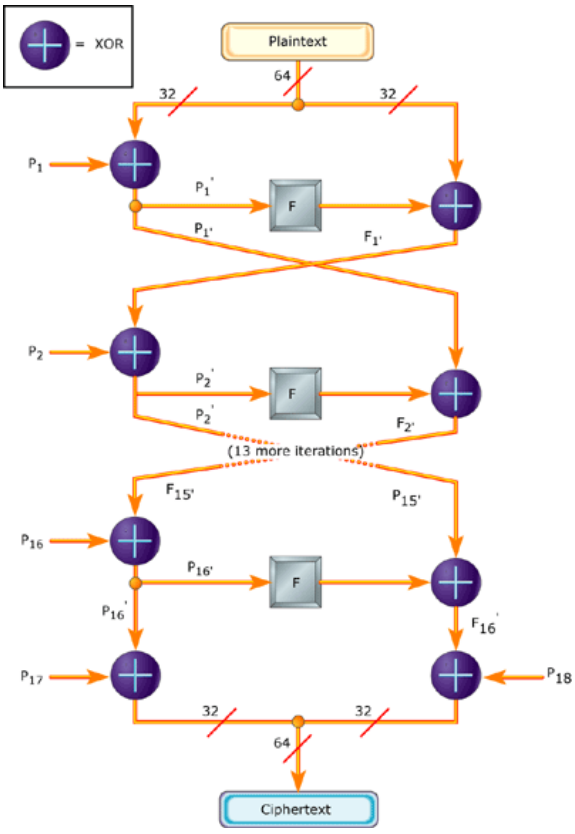

Fig 5: Fiestel Structure of Blowfish Algorithm

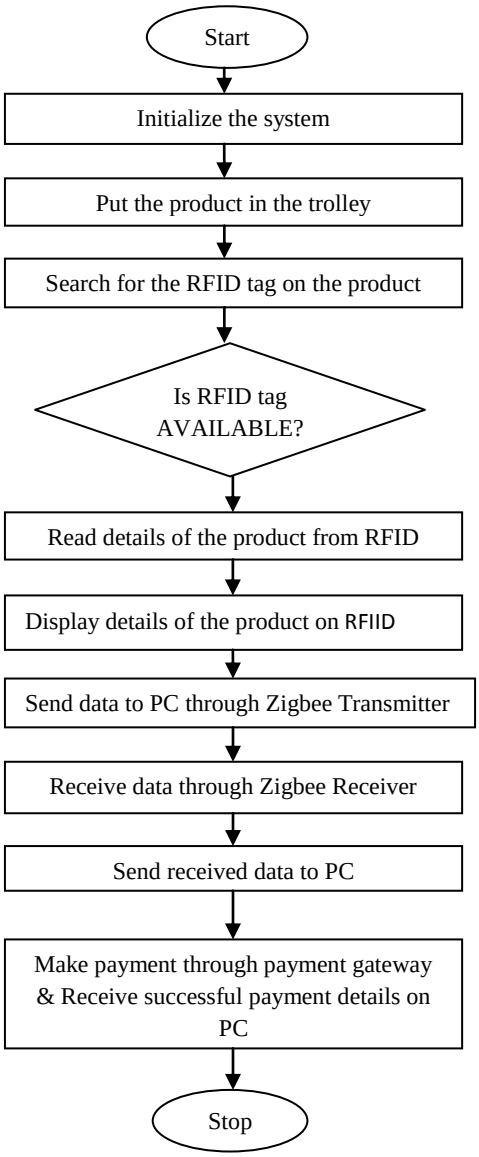

Fig 6: Proposed System Flow

- Key Generation

The p-array consists of 18, 32-bit sub keys:

P1, P2,……., P18.

Four 32-bit S-Boxes consist of 256 entries each:

S1,0, S1,1,……. S1, 255.
S2,0, S2,1,…….. S2, 255.
S3,0, S3,1,…….. S3, 255.
S4,0, S4,1,.....S4,255.

1. Initialize first the P-array with fixed string

2. Initialize the four S-boxes with fixed string.

This string consists of the hexadecimal digits of which are less than (initial 3).

3. XOR first 32 bits of the key with P1, XOR second 32-bits of the key with P2, and so on (possibly XOR up to P14). Repeat this process until whole P-array has been XORed with key bits. (For all short key, there is at least one equivalent longer key.

4. Encrypt the all-zero string using Blowfish algorithm based on the sub keys generated in steps (1) ,(2) and (3).

5. Replace P1 and P2 with the output of step (4).

6. Encrypt the output in the step (4) using the Blowfish algorithm based on modified sub keys.

7. Replace P3 and P4 with the output of step (6).

8. Continue this process, replace all entries of the P array and all four S-boxes with the output of the continuously changing Blowfish algorithm [6].

- Function F

Blowfish is a Feistel network which consists of 16 iterations. The input is 64-bit data element, x. x elements is divided into two 32-bit halves [9]:

xL, xR

For i = 1to 16: xL = XL XOR Pi

xR = F(XL) XOR xR

Swap XL and xR

Swap XL and xR (Undo the last swap.) xR = xR XOR P17

xL = xL XOR P18 Recombine xL and xR

- Operational Modes of Blowfish:

Blowfish is a symmetric block cipher and it can be used in four standard operation modes such as Electronic Codebook Mode (ECB), Cipher Block Chaining Mode, Cipher feedback Mode, Output-feedback Mode (OFB). Performance results of blowfish algorithm with CBC mode is much better than other in terms of protection.

4. IMPLEMENTATION

4.1 Software Used

1. Mikro C

MikroC is a C compiler which supports 5 different microcontroller architectures. It features intuitive IDE, and powerful compiler with advanced SSA optimizations and it has lots of software and hardware libraries [4].

2. MATLAB

This is high performance language its basic data element is an array which does not require any dimensioning. A matrix and vector formulation allows to solve many technical computing problems. It combines programming visualization with computation which provides easy-to-use environment where problems and solutions are expressed in the mathematical form. MATLAB toolboxes are available in various fields including control systems, simulation, signal processing, neural networks, wavelets, fuzzy logic, and many others. Simulink is developed by MathWorks it is a graphical programming environment for simulating, modeling and analyzing multiple domain dynamic systems.

5. RESULTS

Implemented hardware model is shown in figure 7.Then, Results of blowfish algorithms are shown in figure 8 and 9.with waiting for data and with time error shown. Table No.1 shows the different parameters for different encryption algorithms such as key size, Average Encryption time, and Memory usage and battery consumption.

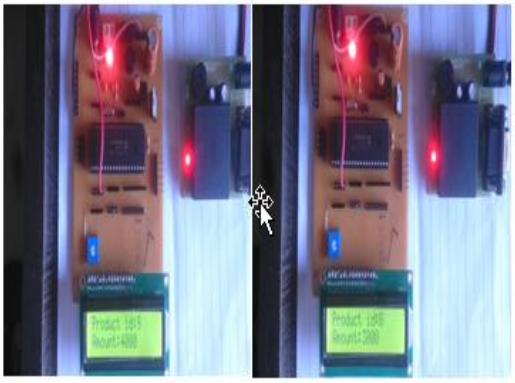

Fig 7:Implemented Hardware Model

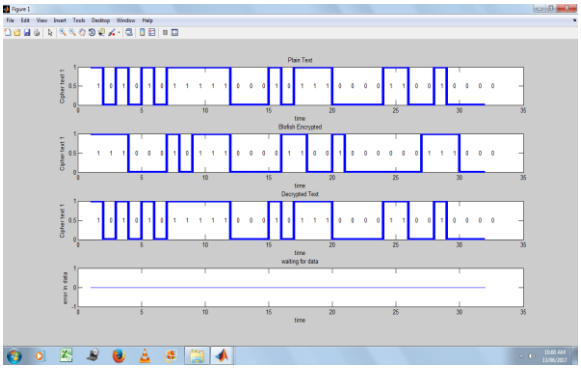

Fig 8: Results of blowfish encryption with waiting for data

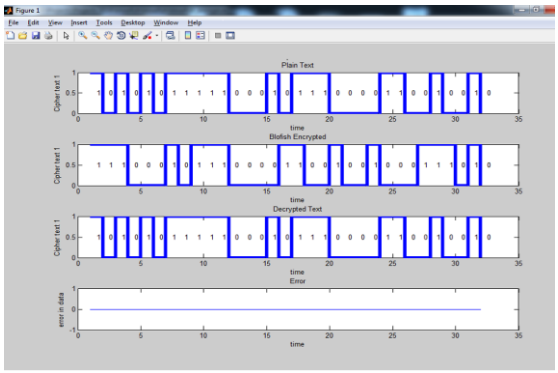

Fig 9: Results of blowfish encryption with time error

Table 1. Parameters for different Encryption Algorithm

Sr No.	Algorithms	Key Size(bits)	Average encryption time(ms)	Memory usage(kbytes)	Battery consumption (%)
1	AES	128	374	32.5	4.2
2	DES	64	389	43.2	4.8
3	RC2	40 - variable	480.7	-	-
4	RC6	128	217	-	-
5	BLOWFISH	64	60.3	25.2	0.5

+

Table 2. Comparison of Various algorithms on the basis of Different Parameter

PARAMETER	DES	3DES	AES	RSA	BLOWFISH
DEVELPOMENT	In early 1970 by IBM and Published in 1977	IBM in 1978	Vincent Rijmen Joan Daeman in 2001	Ron Riverst, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
KEY LENGTH	64 (56 USABLE)	168,112	128,192,256	Key length depenf on no. of bits in the module	Varibe key length i.e 32-448
ROUNDS	16	48	10,12,14	1	16
BLOCK SIZE (Bits)	64	64	18	Variable block size	64
ATTACK FOUND	Exclusive key search, Linear cryptanalysis, Differential Analysis	Related Key attack	Key recovery attack, Size channel attack	Brute force attack, timing attack	No attact is found to be succesfull against blowfish
LEVEL OF SEURITY	Adequate security	Adequate security	Excellent security	Good level of security	Highly secure security
ENCRYPTION SPEED	Very slow	Very slow	Faster	Average	Very fast

6. CONCLUSION

In the proposed system, blowfish algorithm for enhancing the security of the system is implemented for transmitting payment data over payment gateway. Payment data is collected from the server where data is received through Zigbee wireless communication. In this paper RFID based smart trolley system is implemented. It simplifies the billing process and helps customers as it avoids longer waiting in the queue. It continuously displays different parameters of the project such as product name, product cost. Zigbee module transfers these details to PC through wireless communication. At the PC end payment is done through the payment gateway based on blowfish encryption algorithm. Blowfish algorithm based encryption provides high security for the transmission of the payment related data of products in the smart trolley. Smart trolley system can be integrated with WI-FI systems or even with the internet for future use. It can be used in Global sales monitoring and inventory control in off sites. Trolleys will replace salesmen, hence it will help in reducing final product of goods. As it can give more profit margin.

7. REFERENCES

[1] S. Sai Ganesh, B. Sahithi, S.Akhila, T. Venumadhav, "RFID based Shopping Cart", International Journal of Innovative Research in Engineering & Management (IJIREM)ISSN: 2350-0557, Volume-2, Issue-3, May-2015.

[2] Komal Ambekar, Vinayak Dhole, supriya sharma,Tushar Wadekar ,"SMART SHOPPING TROLLEY USING RFID", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 4 Issue 10, October 2015.

[3] Ms. Rupali Sawant, Kripa Krishnan, Shweta Bhokre, Priyanka Bhosale,"The RFID Based Smart Shopping Cart", International Journal of Engineering Research and General Science, Volume 3, Issue 2, March-April, 2015.

[4] Galande Jayshree, Rutuja Gholap,Preeti Yadav "RFID Based Automatic Billing Trolley", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014.

[5] Veena Parihar, Mr. Aishwary Kulshrestha ,"BLOWFISH ALGORITHM: A DETAILED STUDY", International Journal For Technological Research In Engineering,Volume 3, Issue 9, May-2016.

[6] Akshit Shah, Aagam Shah, Prof. Tanaji Biradar ,"Image Encryption and Decryption using Blowfish Algorithm in MATLAB", International Journal of Electronics, Electrical and Computational System, IJEECSISSN 2348-117XVolume 4, Issue 11,November 2015.

[7] Ms Neha Khatri – Valmik, Prof. V. K Kshirsagar, "Blowfish Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE),e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83.

[8] Janhavi Iyer, Harshad Dhabu , Sudeep K. Mohanty, "Smart Trolley System for Automated Billing using RFID and ZIGBEE", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 10, October 2015.

[9] Savita Devidas Patil,"Passwords Management using Blowfish Algorithm", International Journal of Research Review in Engineering Science and Technology (ISSN 2278- 6643) | Volume-2 Issue-1, March 2013.

[10] K. Kanagalakshm , M. Mekala ,"Enhanced Blowfish Algorithm for Image Encryption and Decryption with Supplementary Key ", International Journal of Computer Applications (0975 – 8887) Volume 146 – No.5, July 2016.