ATM TRANSACTION USING ENCRYPTED LI-FI COMMUNICATION

Yogesh Kumawat[1], Sayar Singh Shekhawat[2]
[1]P.G. Student, [2]Associate Professor
Department of Computer Science Engineering
AIET, Jaipur (Raj.), India

***ABSTRACT*:** Data security is the important concern in the banking sector for secure and esoteric data transaction. In this paper, we use several types of encryption mechanism along with the Li-Fi mechanism. Specifically here we dissert the communication procedure between the user and the ATM machine. In this mechanism, we transfer encrypted data using the Li-Fi Device. For Encryption procedure we proposed an encryption algorithm that is Wheel string manipulation Algorithm provides the security while data transmission between the ATM machine and the Li-Fi Device. And the Li-Fi mechanism increases the data transfer rate between the devices. This paper introducing security solution for the ATM transaction, such as security issues (Biometric identification and card tracking, card cloning) and attacks on ATM card. And the final result of this dissert paper enhanced authentication in ATM transaction that ensures security for data transmission and increased banking user's assuredly in the ATM transaction.

***KEYWORDS*:** ATM Card, PIN, Encryption Technique, Li-Fi.

I. INTRODUCTION

Now-a-days in the banking and financial sector for self-finance ATM plays an important role. With an ATM, a banking user can perform many banking and financial operation such as money withdrawal and money transfer and also uses for some account related information to interact with bank staff. In the present era ATM system transaction can be performed by using the two factor and three factor authentication [1] or biometric techniques [2] as well as used some encryption algorithms [6]. But now-a-days many security concerns in two or three factor authentication. Some problems are card cloning, card stolen, card cracking and PIN issue and physical attacks etc. or issues in biometric techniques fingerprinting [4], retina scanning and facial recognition[3] etc. So we can say that all of these are not provides a valid level security in ATM transaction. To overcome these problems we proposed a Li-Fi based device with using proposed encryption Wheel string Manipulation algorithm.

II. RELATED WORK

In the present era problem is that data security and the secure communication while data transmission. The today's scenario of ATM transaction is performed by using the two and three factor authentication [1]. In two factor authentications used ATM card and their unique PIN and in three factor authentication used biometric [9] as a third factor of authentication. But both two and three factor authentication have issues and problem while transaction. Issues regarding the card are Card cloning, Card trapping, skimming attack, ATM malware, ATM Hacking, Physical attack and magnetic stripe is cracked and code tracking is used to identify the PIN by the intruder. And the problems in biometric in facial recognition image can't be detect on different angle, eye disease and high blood pressure problem in retina scanning and fingerprint can be hack and bad influence when number of users used same fingerprint sensor for scanning fingerprint.

III. SYSTEM ANALYSIS

A. *Proposed System Features:*

Proposed system hardware is Li-Fi device, which is used for the communication proposed in the different area. In the Li-Fi mechanism [17] used LED light to transmit the data. Whereas in other communication mechanism such as Wi-Fi used Radio frequency waves, that are not secure and can be hacked and these radio waves is harmful for the human body. But in the Li-Fi used LED light source, is secure and can't be hack and not harmful for the human body. Data transfer rate of the Li-Fi is faster than to compare other wireless techniques.

B. *Proposed System Function:*

The Proposed system has the following capabilities for the banking and financial users.

- Provides Data security while transmission.

- The transmission rate is high.
- Provides a security level compare to present transaction techniques.

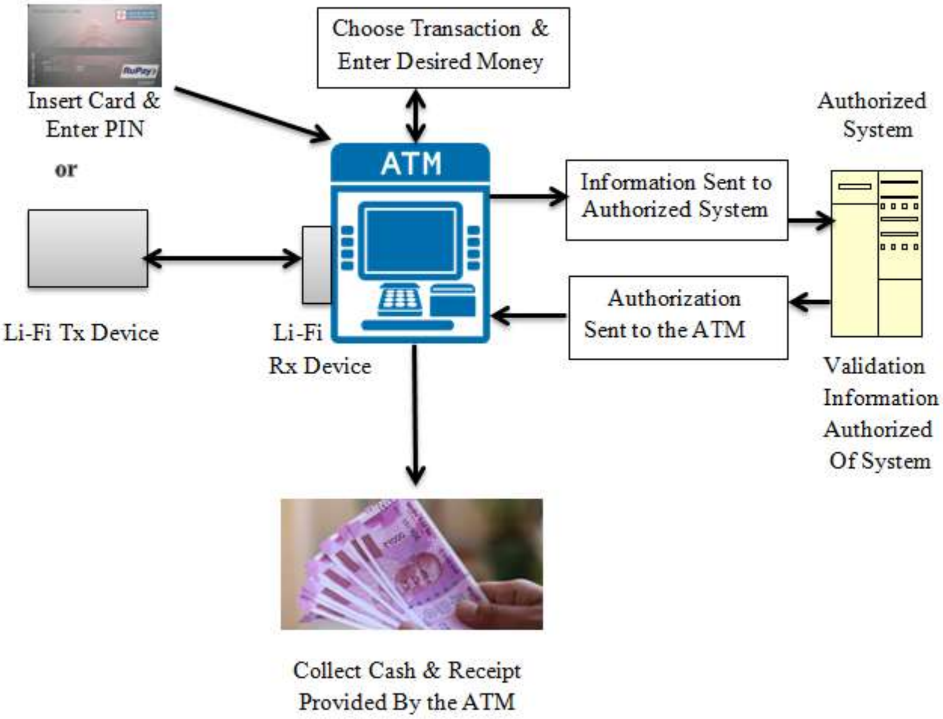


Fig.1: Proposed System Diagram

IV SYSTEM DESIGN IMPLEMENTATION

A. Encryption Method:

Data security is the crucial issue while data transmission. So to provide a security level while data transmission procedure, used encryption method. In the encryption method different encryption algorithm are uses to encrypt the data. In the encryption algorithm ASCII character or string is converting in the cipher text. Then on one cannot detect the original ASCII character or string data.

B. *Li-Fi:*

Li-Fi is bi-directional wireless enabled network technology used to transmit data. The data is transmitted in the form of visible light using the LED light source. The principle of Li-fi is quite easy, when LED is on then it transmit ‘1’ and when LED is OFF it transmit the bit ‘0’.

C. *Software design Implementation:*

a. *VB6:*

To design the proposed system application software used vb6 programming language. Vb6 allows to users to develop GUI application using their powerful tools. Different kinds of tool have the different type functionality. We can create secure and user friendly application in VB6 with ease.

b. *Proteus:*

Proteus ISIS professional combine ease of use with powerful features to help us to design, testing and layout of electronic circuits and microcontrollers design. It is capable for supporting both schematic capture simulation and PCB design. And we can make changes easily in the circuit design by using the schematic rewiring, changing in component value for components and easily add or delete new component according to our requirement in the designing phase.

c. *Serial Port Communication:*

RS232 is communication protocol used for data exchange between the computer and devices. A RS232 serial port is a standard feature of a computer to connect to its peripheral devices. RS232 standard defines the signals connecting between DTE (Data Terminal Equipment) and DCE (Data Communication Equipment or Data Circuit Terminating Equipment) devices. Computer act like as a DTE device and modem as a DCE device.

D. *Hardware Design Implementation:*

Proposed system hardware comprises of Transmitter and Receiver setup.

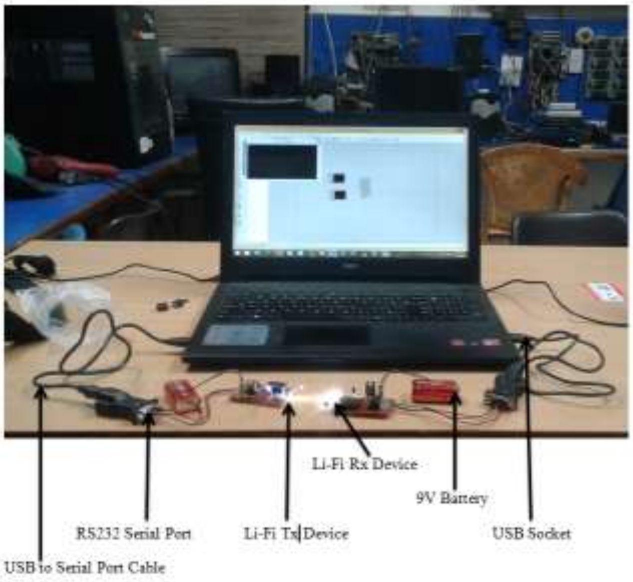


Fig.2: Proposed System Hardware Implementation

a. *Transmitter Part:*

In transmitter part the data is said to be transmitted by transmitting user's data from Li-Fi Device and this data converted to digital signal form of 0's and 1's. Once the data transmitted it reaches receiver side via visible light communication procedure.

b. *Receiver Part:*

The use of receiving part is to receive banking user data that is transmitted successfully from the transmitting side.

V. PROPOSED METHODOLOGY

A. *Proposed Algorithm Implementation:*

In the proposed system when data transmitted using the Li-Fi transfer device as well as encrypt the data using Wheel string manipulation algorithm. When we encrypt data using the encryption algorithms then possibility to identify actual data is less. In Wheel string manipulation algorithm first we encrypt data using the DES algorithm [13] and in second procedure we again encrypt data using the wheel operation that means original data is encrypted twice. DES algorithm is a symmetric encryption algorithm. DES has 64- bit block and 64-bit key length where only 56- bit key length is used rest of the 8- bit is uses for the function as check bits only. In the starting procedure plaintext block was permuted by using the initial permutation. Initial permutation performed in 16 rounds. In this complete procedure used internal keys for all iteration. And the result of the encryption procedure will be permuted using the final permutation that is the reverse of the initial permutation. Once the data encrypt using the DES algorithm then we again encrypt it by using the proposed algorithm wheel string manipulation algorithm. After encrypt used wheel string manipulation algorithm data encrypt twice, that is data security is increases and to decrypt data we use reverse procedure of encryption procedure.

And the algorithm result gets in the following equations:

Wheel String Encryption = Enc $\{f(\, str)\}$ ………. (i)

Where “Str” is indicate the final step of Encryption Procedure
Wheel String Decryption = Dec $\{f(str)\}$ ………. (ii)

And here proposed algorithm explains through the flow chart.

B. *Flow chart:*
a. Encryption Procedure

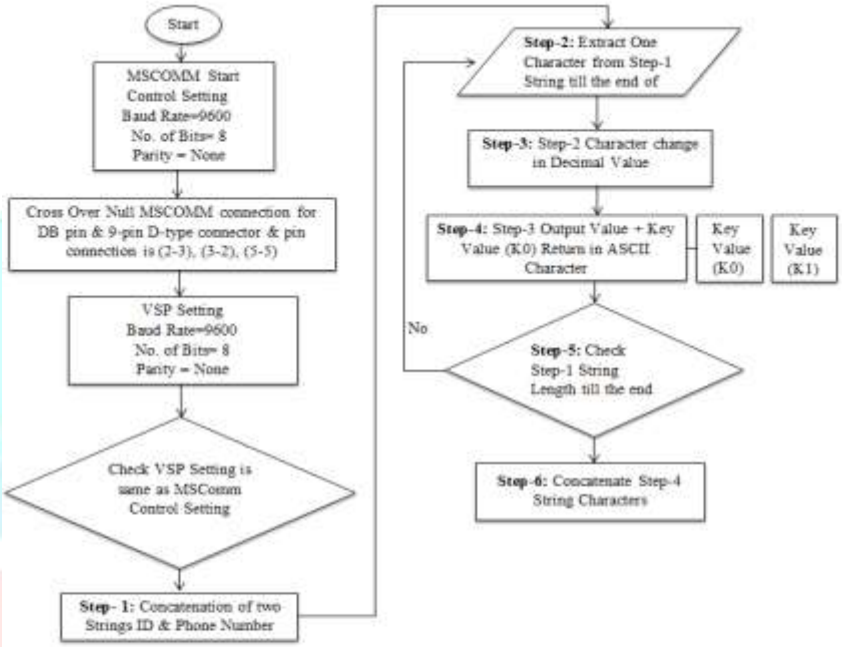

Start
MSCOMM Start Control Setting Baud Rate=9600 No. of Bits= 8 Parity = None
Cross Over Null MSCOMM connection for DB pin & 9-pin D-type connector & pin connection is (2-3), (3-2), (5-5)
VSP Setting Baud Rate=9600 No. of Bits= 8 Parity = None
Check VSP Setting is same as MSComm Control Setting
Step- 1: Concatenation of two Strings ID & Phone Number
Step-2: Extract One Character from Step-1 String till the end of
Step-3: Step-2 Character change in Decimal Value
Step-4: Step-3 Output Value + Key Value (K0) Return in ASCII Character
Key Value (K0)
Key Value (K1)
No
Step-5: Check Step-1 String Length till the end
Step-6: Concatenate Step-4 String Characters

Fig. 3: Encryption procedure Part-1 Flow Chart

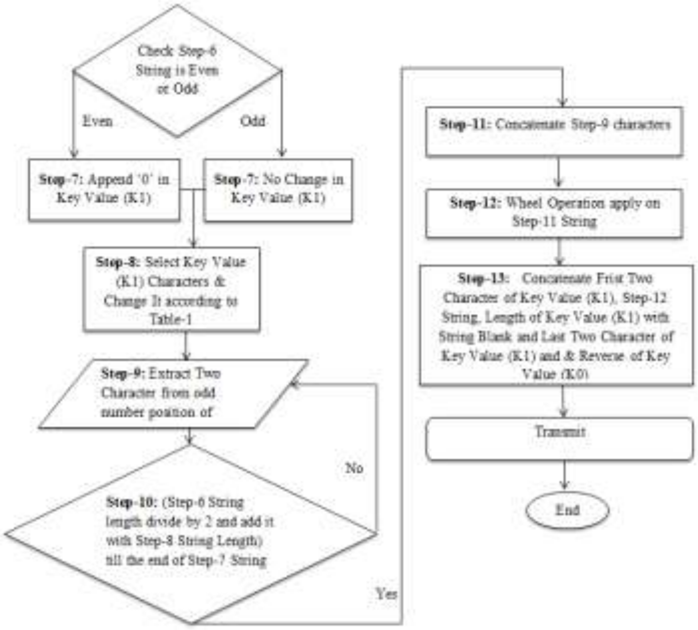

Check Step-6 String is Even or Odd
Even
Odd
Step-7: Append '0' in Key Value (K1)
Step-7: No Change in Key Value (K1)
Step-8: Select Key Value (K1) Characters & Change It according to Table-1
Step-9: Extract Two Character from odd number position of
Step-10: (Step-6 String length divide by 2 and add it with Step-8 String Length) till the end of Step-7 String
No
Yes
Step-11: Concatenate Step-9 characters
Step-12: Wheel Operation apply on Step-11 String
Step-13: Concatenate Frist Two Character of Key Value (K1), Step-12 String, Length of Key Value (K1) with String Blank and Last Two Character of Key Value (K1) and & Reverse of Key Value (K0)
Transmit
End

Fig.4: Encryption procedure Part-2 Flow Chart

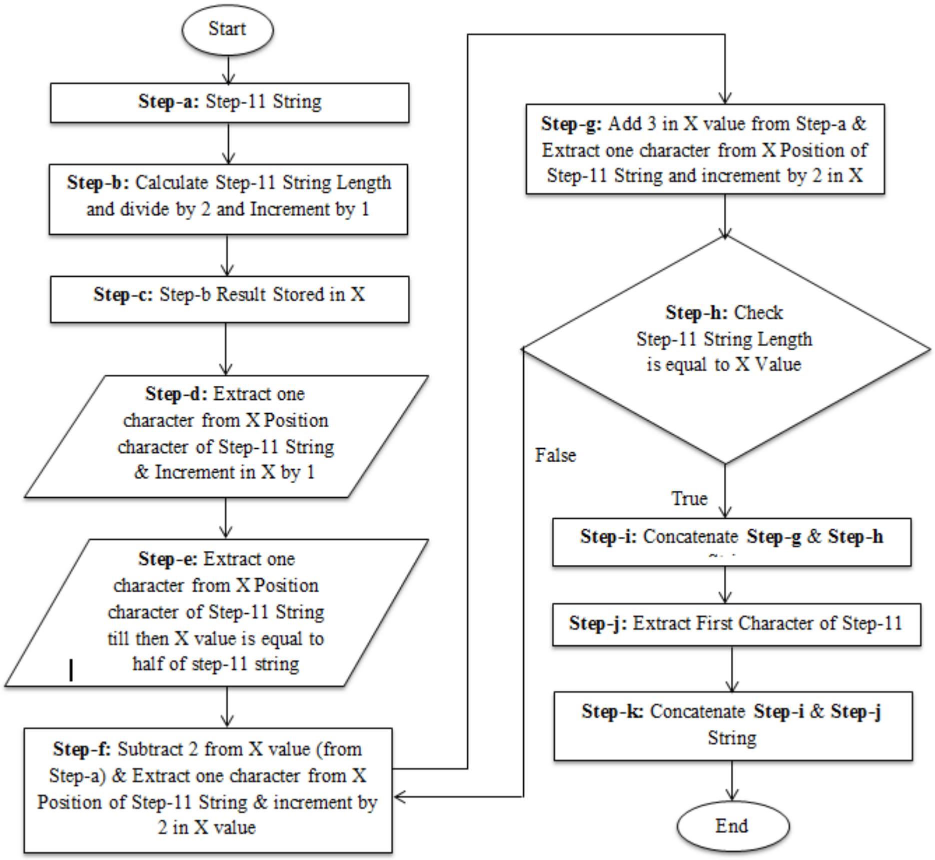

Start
Step-a: Step-11 String
Step-b: Calculate Step-11 String Length and divide by 2 and Increment by 1
Step-c: Step-b Result Stored in X
Step-d: Extract one character from X Position character of Step-11 String & Increment in X by 1
Step-e: Extract one character from X Position character of Step-11 String till then X value is equal to half of step-11 string
Step-f: Subtract 2 from X value (from Step-a) & Extract one character from X Position of Step-11 String & increment by 2 in X value
Step-g: Add 3 in X value from Step-a & Extract one character from X Position of Step-11 String and increment by 2 in X
Step-h: Check Step-11 String Length is equal to X Value
False
True
Step-i: Concatenate Step-g & Step-h
Step-j: Extract First Character of Step-11
Step-k: Concatenate Step-i & Step-j String
End

Fig.5: Encryption procedure Wheel operation Procedure Flow Chart

b. *Decryption Procedure:*

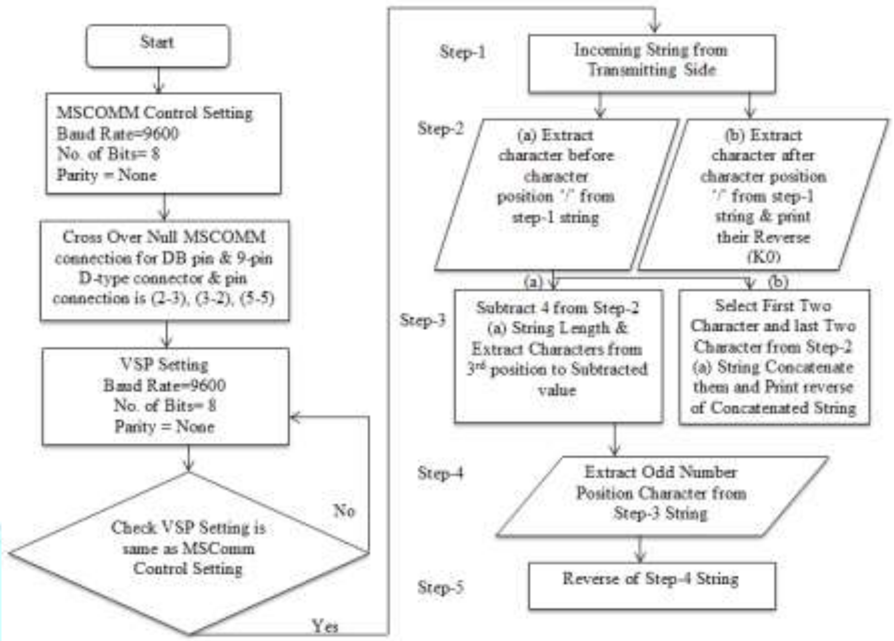

Start
MSCOMM Control Setting
Baud Rate=9600
No. of Bits= 8
Parity = None
Cross Over Null MSCOMM connection for DB pin & 9-pin D-type connector & pin connection is (2-3), (3-2), (5-5)
VSP Setting
Baud Rate=9600
No. of Bits= 8
Parity = None
Check VSP Setting is same as MSComm Control Setting
No
Yes
Step-1
Incoming String from Transmitting Side
Step-2
(a) Extract character before character position '/' from step-1 string
(b) Extract character after character position '/' from step-1 string & print their Reverse (K0)
(a)
(b)
Step-3
Subtract 4 from Step-2 (a) String Length & Extract Characters from 3rd position to Subtracted value
Select First Two Character and last Two Character from Step-2 (a) String Concatenate them and Print reverse of Concatenated String
Step-4
Extract Odd Number Position Character from Step-3 String
Step-5
Reverse of Step-4 String

Fig.6: Decryption procedure Part-1 Flow Chart

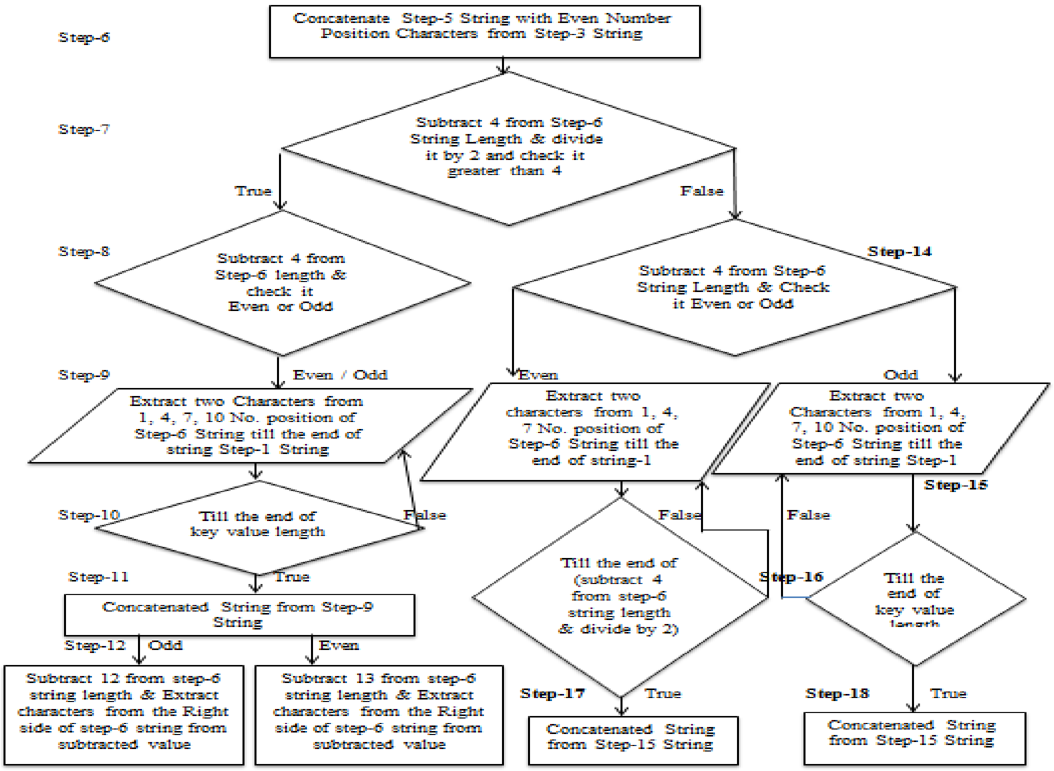

Step-6
Concatenate Step-5 String with Even Number Position Characters from Step-3 String
Step-7
Subtract 4 from Step-6 String Length & divide it by 2 and check it greater than 4
True
False
Step-8
Subtract 4 from Step-6 length & check it Even or Odd
Step-14
Subtract 4 from Step-6 String Length & Check it Even or Odd
Step-9
Even / Odd
Even
Odd
Extract two Characters from 1, 4, 7, 10 No. position of Step-6 String till the end of string Step-1 String
Extract two characters from 1, 4, 7 No. position of Step-6 String till the end of string-1
Extract two Characters from 1, 4, 7, 10 No. position of Step-6 String till the end of string Step-1
Step-15
Step-10
Till the end of key value length
False
True
False
False
Step-11
Concatenated String from Step-9 String
Till the end of (subtract 4 from step-6 string length & divide by 2)
Step-16
Till the end of key value length
Step-12
Odd
Even
Subtract 12 from step-6 string length & Extract characters from the Right side of step-6 string from subtracted value
Subtract 13 from step-6 string length & Extract characters from the Right side of step-6 string from subtracted value
Step-17
True
Concatenated String from Step-15 String
Step-18
True
Concatenated String from Step-15 String

Fig.7: Decryption procedure Part-2 Flow Chart

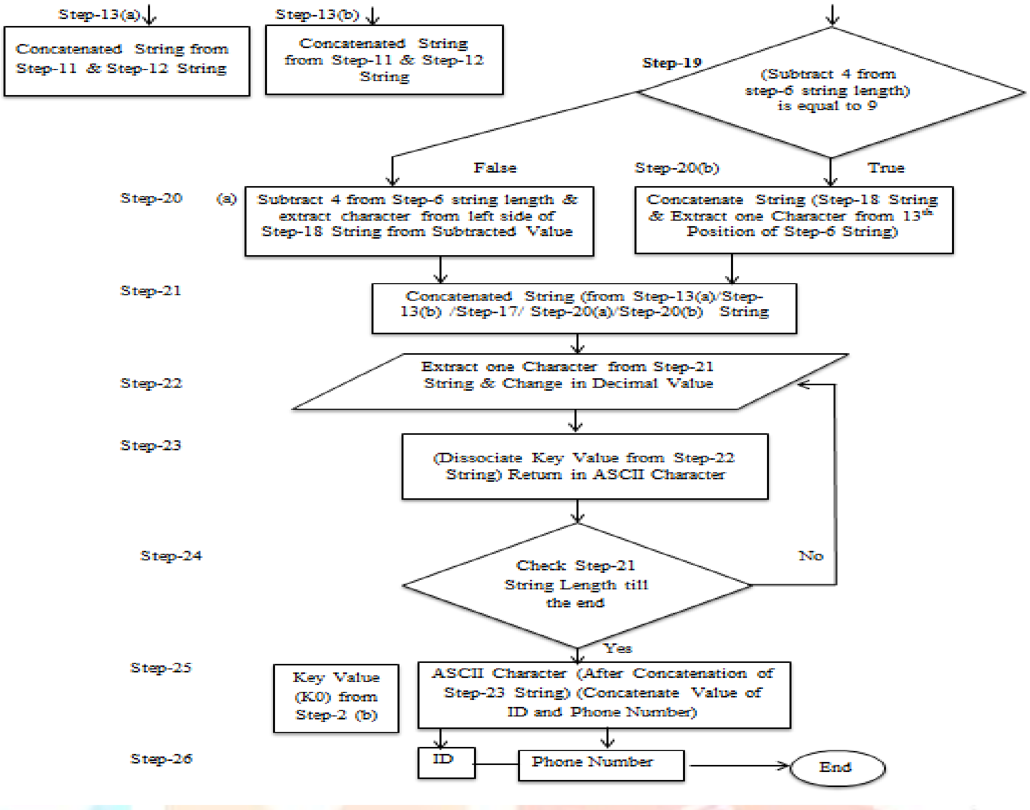
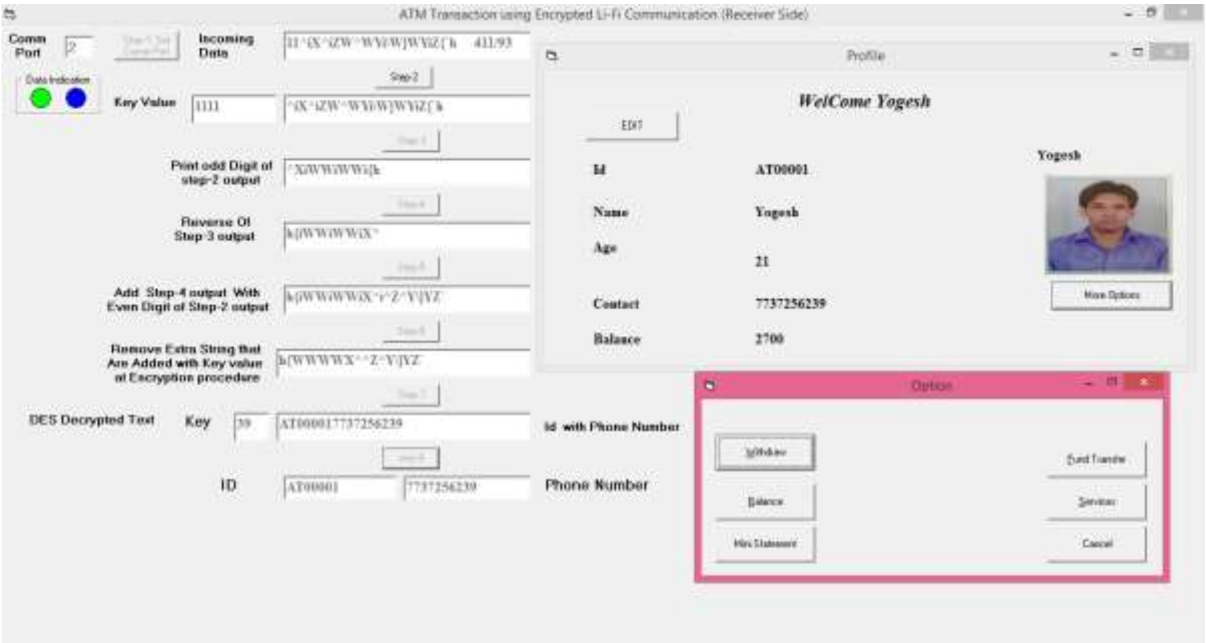

Step-13(a)
Concatenated String from Step-11 & Step-12 String
Step-13(b)
Concatenated String from Step-11 & Step-12 String
Step-19
(Subtract 4 from step-6 string length) is equal to 9
False
Step-20(b)
True
Step-20 (a)
Subtract 4 from Step-6 string length & extract character from left side of Step-18 String from Subtracted Value
Concatenate String (Step-18 String & Extract one Character from 13th Position of Step-6 String)
Step-21
Concatenated String (from Step-13(a)/Step-13(b) /Step-17/ Step-20(a)/Step-20(b) String
Step-22
Extract one Character from Step-21 String & Change in Decimal Value
Step-23
(Dissociate Key Value from Step-22 String) Return in ASCII Character
Step-24
Check Step-21 String Length till the end
No
Yes
Step-25
Key Value (K0) from Step-2 (b)
ASCII Character (After Concatenation of Step-23 String) (Concatenate Value of ID and Phone Number)
Step-26
ID
Phone Number
End

Fig.8: Decryption procedure Part-3 Flow Chart

VI. RESULT

The above figures [2], [3], [4], [5], [6] & [7] show the result of DES and wheel encrypted algorithm. Which is saturated in wheel string manipulation algorithm. The user details send through DES algorithm the result is proceed through wheel algorithm by which data is securely transmitted. This in the next figure [8] data is securely transfer with own created device which shows the successfully login of user if actual data is transmitted.



Comm Port: 2

Incoming Data: 11^iX^iZW^WYiWJWYiZ{`h 411/93

Key Value: 1111 ^iX^iZW^WYiWJWYiZ{`h

Print odd Digit of step-2 output: ^XiWWiWWi{h

Reverse Of Step-3 output: h{iWWiWWiX^

Add Step-4 output With Even Digit of Step-2 output: h{iWWiWWiX^i^Z^Y]YZ

Remove Extra String that Are Added with Key value at Encryption procedure: h{WWWWX^^Z^Y]YZ

DES Decrypted Text Key: 39 AT000017737256239

Id with Phone Number

ID: AT00001 7737256239

Phone Number

WelCome Yogesh

Id	AT00001
Name	Yogesh
Age	21
Contact	7737256239
Balance	2700

Yogesh

Fig.9: user details after successfully login

VII. Conclusion & Future Scope

In the above research experiment we transmitted encrypted data between two devices. With the wide use of internet this work is focused to implement the Li-Fi technology to establish a secure connection of data transmission. In previous research paper study various encryption algorithm and technology used in ATM transaction. But there is various security issues in those paper like Biometric identification and card tracking, card cloning. To resolve these security issue we enhance wheel string manipulation algorithm which is already exist by Jefferson Wheel Cipher and create an own device which is type of a data transfer pin. This string manipulation algorithm is used to securely transfer data through ATM along with device. The main objective of this is to not only increase the security in data transfer but also increase the data transfer rate.

REFERENCES

[1] Jane Ngozi Oruh. 2014. Three-Factor Authentication for Automated Teller Machine System. International Journal of Computer Science and Information technology (CSITS), Vol.-4, No.-6, ISSN: 2249-9555.

[2] Ansiya Mohammed Ali.2015.Biometric Fingerprint ATM for More Secured ATM Transaction. International Journal of Engineering and Technical Research (IJETR), Volume-3, Issue-2, ISSN: 2321-0869.

[3] V.Meena Mphil. 2015. Facial Recognition Technology for use in ATM Transaction. International Journal of Advance Research in Computer Science and Software Engineering", Volume-5, Issue-3, ISSN: 2277 128X.

[4] Krishna Nand Pandey, [2]Md. Masoom, [3]Supriya Kumari, [4]Preeti Dhiman. 2015. ATM Transaction Security Using Fingerprint/OTP. Journal of Emerging Technologies and Innovative Research (JETIR), Volume-2, Issue-3, ISSN-2349-5162.

[5] Alebiosu M. iyabode[1], Yekini N. Nureni2, Adebari F. Adebayo[3], Oloyede A. Olamide[4]. 2015. Card-Less Electronic Automated Teller Machine (EATM) with Biometric Authentication. International Journal of Engineering Trends and Technology (IJETT), Volume-30, Number-2.

[6] CH. Krishna Prasad, G. Srinivasa Rao, Dr. M.V. Siva Prasad. 2014. Data Encryption Methods Used in Secure ATM Transactions. Journal of Computer Science and Mobile Computing", Vol.3 Issue.6, pg. 230- 233.

[7] Nikhita Adidam. 2015. Li-Fi – The Future of Internet. International Journal of Computer Science & Engineering (IJCSET), Vol.-6, No.-01, ISSN: 2229-3345.

[8] [1]Pushpendra Verma, Dr. Jayant Shekhar, [3]Preety, [4]Dr. Amit Asthana. 2015. Light-Fidelity (Li-Fi): Transmission of Data through Light of Future Technology. International Journal of Computer Science and Mobile Computing, Vol.-4, Issue-9, pg. 113-114.

[9] Ankit Kumar Programmer. 2015. A Review Paper on ATM Machine Security with BIOMETRIC OR Aadhaar card and OTP Password. 4th International Conference on System Modelling & Advancement trends (SMART).

[10] Mr. Shobhit Khandare[1], Rebecca Yesuvadian[2], Sagar Bhatia[3], Shreeparna Sarkar[4]. 2016. Indoor Communication through Li-Fi. Interbnational Journal Of Innovative Research in Computer and Communication Engineering, Vol.-4, Issue-3.

[11] Rajesh R Mane[1]. 2015. A Review on Cryptography Algorithm, Attacks and Encryption Tools. International Journal of Innovative Research in Computer and Communication Engineering, Vol.-3, Issue- 9.

[12] Abhijeet S. Kale1, Sunpreet kaur Nanda[2]. 2014. A Review Paper on Design of Highly Secured Automatic Teller Machine System by Using Aadhaar Card and Fingerprint. International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue-1.

[13] Yashwant Kumar[1], Rajat Joshi[2], Tameshwar Mandavi[3], Simran Bharti[4], Miss Roshni Rathour[5]. 2016. Enhancing the Security of data Using DES Algorithm Along with Substitution Technique. International Journal of Engineering and Computer Science, Volume-5, Issue-10, Page No. 18395-18398.

[14] Jay Chapala, Ajay Chaudhary, Roshni Patel. 2017. Li-Fi Technology: Emerging trend of Data Transmission. International Journal of Innovative research in Computer and Communication Engineering, Vol.-5, Issue-3.

[15] Mohammed Abdulmalek Ahmed. 2016. Li-Fi: The Future Bright technology in Wireless communication. International Journal of Advanced Research in Computer Science and Software Engineering, Volume-6, Issue-3.

[16] R.Mahendran1. 2016. Integrated Li-Fi (Light Fidelity) For Smart Communication Through Illumination. International International International Conference on Advanced Communication Control and Computing Technologies.

[17] Mohammed Abdulmalek Ahmed. 2016. Li-Fi: The Future Bright Technology in Wireless Communication . International Journal of Advanced Research in Computer Science and Software Engineering. Volume 6, Issue 3, ISSN: 2277 128X.