ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 2, Issue 2, February 2015

Study of Securing Computer Folders with Bluetooth

Asst. Prof. A.V.Nadargi[1], Apurva Dalmiya[2], Sonali Jadhav[3], Gajendra Singh Solanki[4]

Computer Engg. Dept, SIT, Lonavala, University of Pune[1,2,3,4]

Abstract: We are presenting a system to keep your data prevented against unauthorized access by using symmetric key. In order to keep this symmetric key secret the proposed system encrypts this confidential symmetric key with the public cryptographic function and the key stored into the window's registry. This system also uses the Bluetooth technology as the main technique for communication between elements of the system. The use of Bluetooth device's MAC address which is stored in the registry of our personal computer plays a major role in securing the data. The system focuses on to ensure data confidentiality to the authorized users only.

Keywords: Bluetooth communication, Rijndael algorithm, MAC addresses, Windows Registry.

I. INTRODUCTION

The main objective of this document is to illustrate the requirements of the Security system. This document explains the use of Bluetooth. It also illustrates the algorithm used for Encryption and Decryption.

The purpose of this document is to provide an environment to secure computer folders. This is a document which aims on the aspects of Security system and attempts to develop a proper Security system for it.

This security system uses Bluetooth and MAC address as the Key features of security. The key used here is a private key and it uses block cipher for encryption. The proposed system uses Rijndael algorithm for encryption and decryption.

This system represents client and server model. Here a computer and a phone is used for the working. The application runs on the server side i.e. computer and authentication of authorized device is done on client side i.e. phone. Next sections will describe the proposed system, use of Bluetooth and Rijndael algorithm.

II. LITERATURE SURVEY

File Encryption XP system that encrypts files by Blowfish algorithm. It protects information from being viewed or modified from unauthorized person. It uses 384-bit key, and no encryption passwords are saved within the encrypted files [1].

SafeHouse Pro helps in data privacy. It is unpredictable that your sensitive data will be at risk. The more transportable your data becomes, the more cautious you need to be. And hence SafeHouse is used for file encryption [1].

AES: In AES raising the key size by 64 bits leads to increase in energy usage of about 8% without any data transfer. In case of AES higher key size leads to modification in the battery and time usage [2].

DES: DES is 64 bits key size with 64 bits block size. Many attacks and methods helped in recording the weaknesses of DES, which made it a timid block cipher [3].

III. PROPOSED SYSTEM

In our system there is the client side and the server side.

A. Server Side (Computer)

MAC address of the phone and the key is stored into the registry. Bluetooth device is registered into the system. The system searches for the phone if in range or not, if not in range then selected folders get encrypted. While decryption system finds various devices in range and authenticates the authorized phone device to provide access by checking the MAC address stored into the registry.

B. Client Side (Phone)

An application is installed into the phone that is provided to enter the key to the system while decryption when the system authenticates the phone. This key is fetched by the system with the help of Bluetooth.

C. Bluetooth

Here we are using Bluetooth as the wireless medium for communication between the computer and the phone. As it provides reliable connection and is easily available in all devices it is being used.

The operation of searching discoverable devices is known as inquiry [1]. It provides low cost in terms of cost and power consumption. It provides speed of 1 to 2 mb/sec.

D. MAC Address

Media Access Control (MAC) is a unique identifier assigned to network interfaces for communication. It has six groups of two hexadecimal digits separated by hyphens or colons, in transmission order. Another convention is using three groups of four hexadecimal digits. A host cannot determine from the MAC address of another host whether that host is on same link as the sending host or on network segment bridged to that network segment. Using MAC address of the electronic device movement of every one in a city can be tracked.

DOI 10.17148/IARJSET.2015.2204

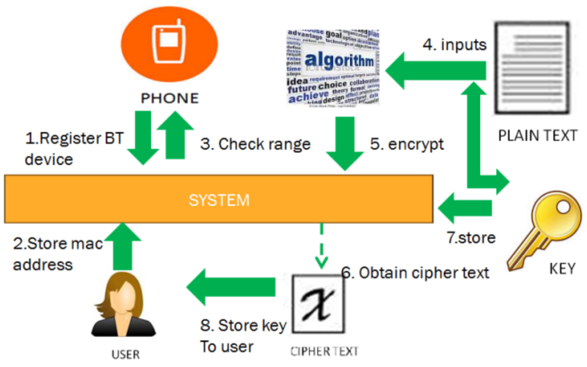

Fig1. Architecture of proposed system

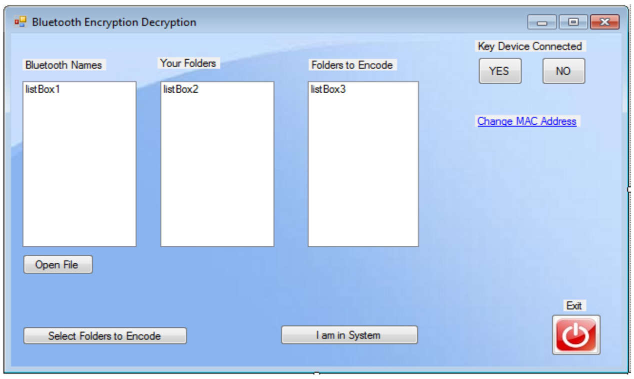

Fig 2. Proposed Work.

IV. PROPOSED ALGORITHM

Rijndael algorithm is the proposed algorithm of our system. It requires two inputs i.e. key and the plain text. It performs number of rounds depending on size of the key. The difference between the AES and Rijndael is that in AES fixed key size is used and in Rijndael key of variable size can be used. Cipher key iterates depending on the following basis.

a. 9 rounds for the key/block size of 128 bits.

b. 11 rounds for the key/block size of 192 bits.

c. 13 rounds for the key/block size of 256 bits.

Each round consists of following four steps.

a. Add Subkey

b. Byte Substitution

c. Shift Row

d. Mixed Column

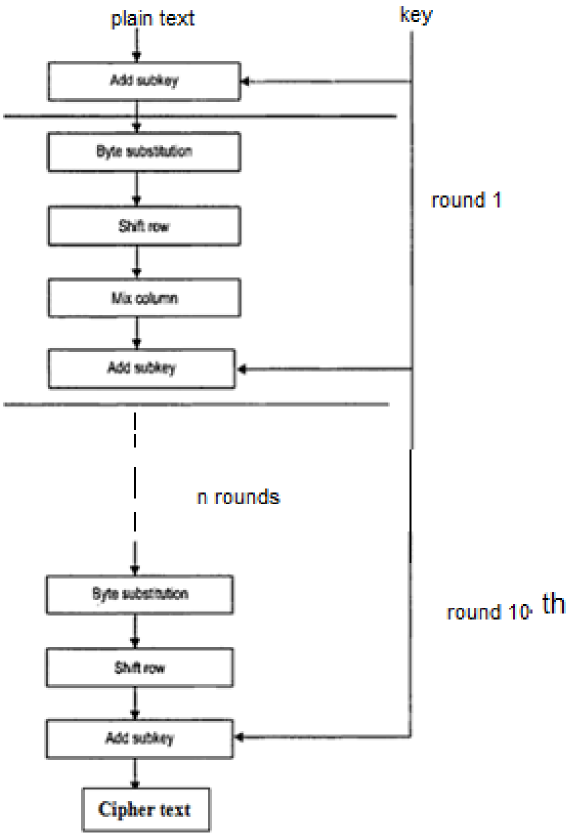

Fig 3. Rijndael algorithm workflow

AES, Rijndael, DES all these algorithms is already defined into .NET. Rijndael algorithm uses Cipher Block Chaining (CBC) mode. In CBC mode an initial vector is used. Rijndael algorithm is private key block cipher algorithm. In CBC mode an initial vector is used which is Exord with plaintext and then the obtained text is Exord with key to obtain cipher text. For another block the obtained cipher text from first block is Exord with plaintext and then key is used for Exoring with obtained text. This process is followed for all blocks.Use Initial Vector (IV) to start process.

$C_i = DES_{K1} (P_i \text{ XOR } C_{i-1})$

$C_{-1} = IV$

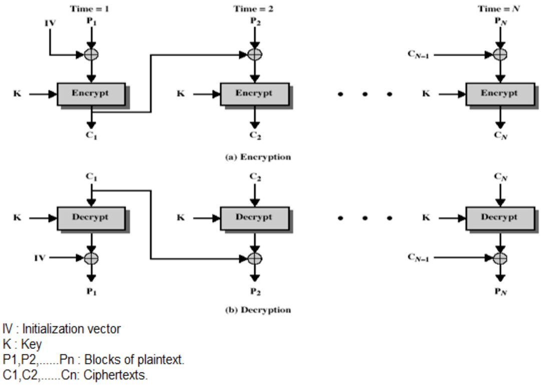

Fig 4. Cipher Block Chaining

DOI 10.17148/IARJSET.2015.2204

V. CONCLUSION

Through this document we could understand that what were the existing algorithms for implementing the encryption and also the advantage of the proposed system. This document helps us to understand the advantage of using Bluetooth into our system. Although there are various other connecting methods but according to the study Bluetooth comes out to be the best method. As the MAC address is unique hence this feature provides more security in our application. This system provides us point to point security without the interference of unauthorized person.

ACKNOWLEDGEMENTS

Our thanks to the experts who have contributed towards development of the proposed system.

REFERENCES

[1] Wankhade S.B., Damani A.G., Desai S.J., Khanapure A.V.,"An Innovative Approach to File Security Using Bluetooth." International Journal of Scientific Engineering and Technology (ISSN: 2277-1581) Volume No.2, Issue No.5.

[2] Bijoy Kumar Mandal,Debnath Bhattacharya,Samir Kumar Bandopadhyay," Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm" 2013 International Conference on Communication Systems and Network Technologies.

[3] M.Umaparvathi1, Dr.Dharmishtan K Varughese," Evaluation of Symmetric Encryption Algorithms for MANETs".

[4] O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi," Performance Analysis Of Data Encryption Algorithms".

[5] Mr. Jay.D.Dalal, Ms. Safiya.S.Dayala,Prof. Nehal Shah,"Optimized AES Algorithm Using Galois Field Multiplication and Parallel Key Scheduling".

[6] Dr. Zahir Zainuddin ,Evanita V Manullang," E-Lerning Concept Design of Rijndael Encryption Process.