An Innovative Approach to File Security Using Bluetooth

Wankhade S.B., Damani A.G., Desai S.J., Khanapure A.V.

Department of Computer Engineering Rajiv Gandhi Institute of Technology, Mumbai, Maharashtra, India.
sunil.wankhade@mctrgit.ac.in, aparnadamani@gmail.com, salodesai@gmail.com,
agraja.khanapure@gmail.com

Abstract* —This paper presents a system based on nontraditional idea that applies symmetric key encryption algorithm to keep your data secure against unauthorized reading and undetected mutilation. The main issue of Reading or tapping data is secrecy and confidentiality. Confidentiality has always played an important role in diplomatic and military matters. In order to keep this symmetric key secret the proposed system encrypts this confidential symmetric key with the public cryptographic function. This system also uses the Bluetooth technology as the main technique to personalize communication between elements of the system and key keeper. 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. File security must be implemented so as to eliminate the problems like unauthorized access, execution of commands illicitly, destructive behavior and confidentiality reaches.The aim of the system is to ensure data integrity and confidentiality to the authorized parties only.

***Keywords*— Wireless Network, Wi-Fi, Bluetooth, IrDA, Security, Rinjdael, Encryption, Decryption**

I. INTRODUCTION

File Security is a feature of your file system which controls which users can access which files, and places limitations on what users can do to files. The file system considers the user's identity, and what kind of action the user is performing, and consults the file's permissions.

Advanced Encryption Standard(AES) is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor Data Encryption Standard(DES), AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

In order to protect the file against unauthorized reading and undetected mutilation, a user encrypts it with a secret cryptographic key of a symmetric cryptosystem. This symmetric key is needed to encrypt or decrypt data with it [1].

The cryptographic keys are used in data encryption to make the file more secure. The same key must be used to decrypt the data. This means that we have to either memorize the key or store it somewhere. Memorizing it isn't practical, so we must store it so that we can recall it when we want to decrypt the data back into its meaningful form, but no one else can[14]. For storage we use windows registry. There are many useful adjustments to the windows configuration or behavior that can be made by simple editing of the registry. Unless you are the administrator, registry cannot be edited.

The three most popular standards that can be used for transferring the keys are IrDA, Bluetooth, and Wi-Fi. Each allows battery-powered devices to communicate wirelessly and each one of them has its own benefits and limitations. After presenting the benefits and limitations of each technology, it is found that Bluetooth is the most appropriate technology for the proposed system as shown in next section.

II. PROBLEM STATEMENT

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. Attacker can access the system to steal or make unauthorized changes in sensitive information, commit fraud, or disrupt operations [2].

Primary source of threats that are encountered are employees or insider attack and malicious hackers or outsider attack. Both can reach the private data and penetrate the security system [3].

The overall aim of the proposed system is protecting any private data from illegal access or from damage and keeping the used keys in the encryption process safe against any pilfering by applying a new method. This method is a three layer encryption with a new key management system approach using windows registry.

III. Previous Related Works

There are many implemented systems that try to solve the problem of stealing and editing a stored private data using different encryption algorithms. File Encryption XP system that can encrypt files of any type using Blowfish algorithm. It protects information against being viewed or modified without authorization [16].

MEO is file encryption software for Mac or Windows that will encrypt or decrypt files of any type. Protect sensitive data against unauthorized viewers with the latest data encryption technologies to keep your documents safe and secure.

User can easily send encrypted emails, or create self-extracting encrypted files so the receiver can open the encrypted files on any Windows or Mac computer without needing to install the encryption software on their machine [16].

File Encryption XP encrypts files and folders using a strong Blowfish algorithm with 384-bit key, and no encryption passwords are saved within the encrypted files. File Encryption XP has a deletion method that will completely remove files after encryption so that the only remaining file is the encrypted version and no unencrypted temporary files ever created.

File Encryption XP has a built-in password generator allows generating new passwords according to the criteria the user specify. Strong passwords are ones containing upper and lower case letters as well as numbers and so they are almost hard to guess. The program adds items into Windows Explorer popup menu to simplify encryption, decryption and wiping tasks [13].

SafeHouse Pro promotes data privacy and help you to protect your confidential files. It is inevitable that sooner or later your sensitive data will be at risk. Maybe your laptop gets stolen. Maybe that memory stick in your pocket ends up at the dry cleaners. The more portable your data becomes, the more careful you need to be. And that is the reason why SafeHouse is used for file encryption [16].

IV. Short Range Wireless Communication Technologies

There are several standards available for transferring keys between the elements of the system wirelessly in a short range. The most three popular technologies are Wi-Fi, Bluetooth and IrDA. The following section presents benefits and limitations of each technology.

A. Wi-fi

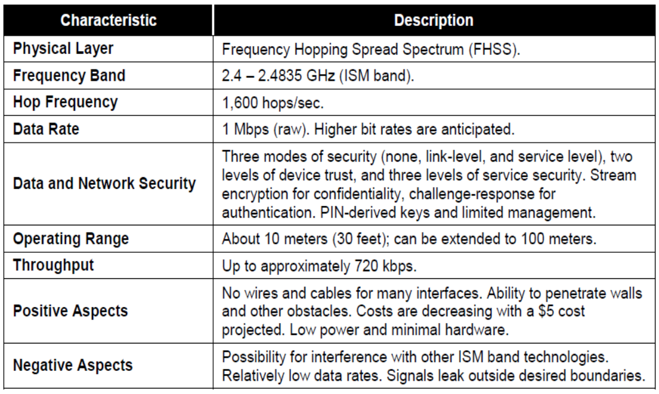
Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term Wi-Fi is short for "*wireless fidelity*," however this is not the case. Wi-Fi is simply a trademarked term meaning IEEE 802.11x. Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters .

B. IrDA

As infrared data communications, based on standards from the Infrared Data Association (IrDA), become widely available on personal computers and peripherals, a timely opportunity exists for effective and inexpensive short range wireless communications on embedded systems and devices of all types. The IrDA standards were developed rapidly (compared to most standards organizations), and information on the IrDA protocols has not yet reached every corner of the embedded systems universe. The Infrared Data Association (IrDA) is an industry-based group of over 150 companies that have developed communication standards especially suited for low cost,short range, cross-platform, point-to-point communications at a wide range of speeds.

C. Bluetooth Technology

Bluetooth is a Radio Frequency (RF) specification for short-range, point-to-point and point-to-multi-point voice and data transfer. Bluetooth will enable users to connect to a wide range of computing and telecommunications devices without the need for proprietary cables that often fall short in terms of ease-of-use. The technology represents an opportunity for the industry to deliver wireless solutions that are ubiquitous across a broad range of devices. The strength and direction of the underlying Bluetooth standard will ensure that all solutions meet stringent expectations for ease-of-use and interoperability [4].



Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 – 2.4835 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1 Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level, and service level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge-response for authentication. PIN-derived keys and limited management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 720 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technologies. Relatively low data rates. Signals leak outside desired boundaries.

Table 1 Characteristics of Bluetooth

Bluetooth network topologies are established on a temporary and random basis. A distinguishing feature of Bluetooth networks is the master-slave relationship maintained between the network devices. Up to eight Bluetooth devices may be networked together in a master-slave relationship, called a "piconet." In a piconet, as shown in fig1, one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network's hopping scheme).

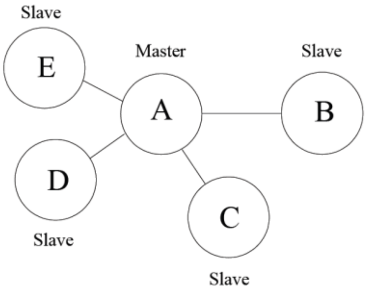


Fig 1. Piconet

Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device may perform as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. This series of piconets, often referred to as scatter-nets, allows several devices to be internetworked over an extended distance. Scatternet diagram can be seen in fig 2. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward or away from the master device in the network, the topology and therefore the relationships of the devices in the immediate network change [5].

Due to the ad-hoc nature of Bluetooth networks, remote Bluetooth devices will move in and out of range frequently. Bluetooth devices must therefore have the ability to discover nearby Bluetooth devices. When a new Bluetooth device is discovered, a service discovery may be initiated in order to determine which services the device is offering.

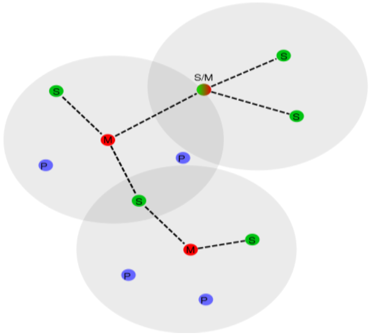


Fig 2. Scatternet

The Bluetooth Specification refers to the device discovery operation as inquiry. During the inquiry process the inquiring Bluetooth device will receive the Bluetooth address and clock from nearby discoverable devices. The inquiring device then has identified the other devices by their Bluetooth address and is also able to synchronize the frequency hopping with discovered devices, using their Bluetooth address and clock. Discoverable devices make use of an Inquiry Access Code (IAC). Two IACs exist, the General Inquiry Access Code (GIAC) and the Limited Inquiry Access Code (LIAC). IAC is used to specify whether to search for all class device or a specific class of device. GIAC scans for all class device and LIAC scans for limited time period. It limits the no. of inquiry responses. The GIAC is used when a device is general discoverable, meaning it will be discoverable for a undefined period of time. The LIAC is used when a device will be discoverable for only a limited period of time. [6].

Security Services

The three basic security services defined by the Bluetooth specifications are the following:

- Authentication: A goal of Bluetooth is the identity verification of communicating devices. This security service addresses the question "Do I know with whom I'm communicating?" This service provides an abort mechanism if a device cannot authenticate properly [7].

- Confidentiality: Confidentiality, or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by eavesdropping (passive attack). This service, in general, addresses the question "Are only authorized devices allowed to view my data?" [7].

- Authorization: A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question “Has this device been authorized to use this service?” [7].

The table 2 summarizes the difference between all the three above mention wireless technologies

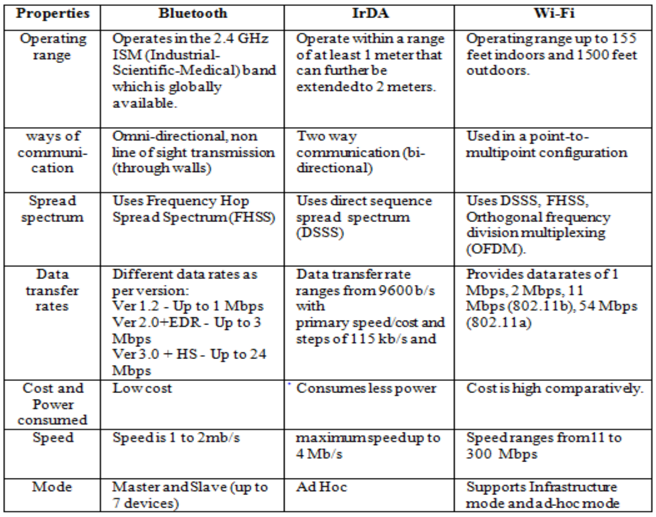
V.RIJNDAEL ALGORITHM

Rijndael algorithm is successor to what is currently used the data encryption standard which has proved to be crackable, given enough computing resources. Rijndael uses a variable number of rounds which is the number of cycles through which the cipher iterates, depending on key/block sizes, as follows:

a) 9 rounds if the key/block size is 128 bits
b) 11 rounds if the key/block size is 192 bits
c) 13 rounds if the key/block size is 256 bits

Rijndael is a substitution linear transformation cipher. It does not require a Feistel network. It uses a triple discreet invertible uniform transformations (layers).Specifically these are: linear mix transform, non-linear transform and key addition transform. Even before the first round, a simple key addition layer is performed, which adds to security.

The transformations form a state when started but before completion of entire process. Rijndael operates on a two dimensional array of bytes called the state that contains 4 rows and Nc columns, where Nc is the input sequence length divided by 32.Similarly cipher key is an array with 4 rows, but the key length divided by 32 to give the number of columns. the blocks can be interpreted as one dimensional arrays of 4 byte vectors.



Properties	Bluetooth	IrDA	Wi-Fi
Operating range	Operates in the 2.4 GHz ISM (Industrial-Scientific-Medical) band which is globally available.	Operate within a range of at least 1 meter that can further be extendedto 2 meters.	Operating range up to 155 feet indoors and 1500 feet outdoors.
ways of communi-cation	Omni-directional, non line of sight transmission (through walls)	Two way communication (bi-directional)	Used in a point-to-multipoint configuration
Spread spectrum	Uses Frequency Hop Spread Spectrum (FHSS)	Uses direct sequence spread spectrum (DSSS)	Uses DSSS, FHSS, Orthogonal frequency division multiplexing (OFDM).
Data transfer rates	Different data rates as per version: Ver 1.2 - Up to 1 Mbps Ver 2.0+EDR - Up to 3 Mbps Ver 3.0 + HS - Up to 24 Mbps	Data transfer rate ranges from 9600 b/s with primary speed/cost and steps of 115 kb/s and	Provides data rates of 1 Mbps, 2 Mbps, 11 Mbps (802.11b), 54 Mbps (802.11a)
Cost and Power consumed	Low cost	Consumes less power	Cost is high comparatively.
Speed	Speed is 1 to 2mb/s	maximum speedup to 4 Mb/s	Speed ranges from11 to 300 Mbps
Mode	Master and Slave (up to 7 devices)	Ad Hoc	Supports Infrastructure mode and ad-hoc mode

Table 2 Difference between Bluetooth, IrDA, WI-Fi

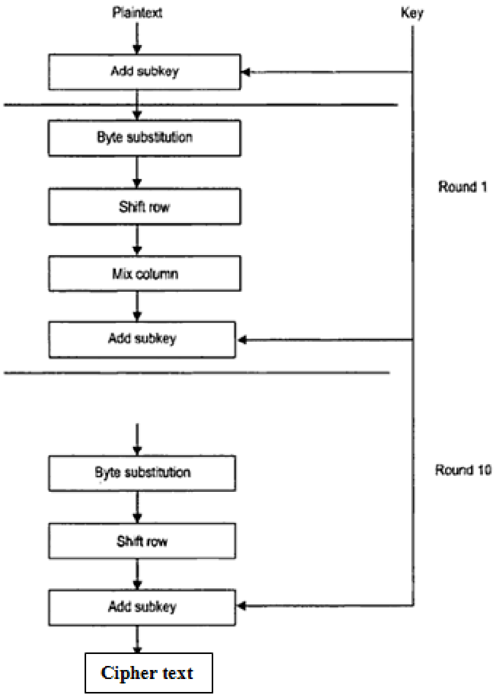


Fig 3. Encryption Process of Rijndael Algorithm

The exact transformations as shown in fig 3 occur as follows: Each round consist of 4 steps:

- Add subkey: A portion of a key unique to this round is XOR with the round result. This operation provides confusion and incorporates the key.
- Byte substitution: It uses S-block structure similar to DES, substituting each byte of a 128-bit block.
- Shift row: It is simple permutation operation. For 128 and 192 bit block sizes, row n is shifted left circular (n-1) bytes while for 256-bit blocks, row 2 is shifted 1 byte and rows 3 and 4 are shifted 3 and 4 bytes respectively.
- Mix columns: The four bytes of every column are mixed in a linear fashion. This step involves shifting left and XOR with the round result. These provide both confusion and diffusion.[8]

An iteration of the above steps is called a round. The amount of rounds of the algorithm depends on the key size.

Key size	Block size	Rounds
(bytes)	(bytes)	
16	16	10
24	16	12
32	16	14

The only exception being that in the last round the mix column step is not performed, to make the algorithm reversible during decryption. Overall the structure of Rijndael displays a high degree of modular design, which should make modification to counter any attack developed in the future much simpler than with past algorithm designs [9].

VI. PROPOSED SYSTEM

The main idea of the system depends on file encryption- plaintext transformation- using encryption algorithm to make it meaningless data that cannot be read without decrypting the data back into its meaningful form. The system target is to keep a file unreadable to anyone except those possessing special knowledge, usually referred to as a key. Keys are saved with authenticated parties to be kept on their personal smart devices [1].

The proposed system needs two inputs the plain text to be encrypted and a friendly name of the Bluetooth device that will cover encryption process as shown in the workflow of the system in figure 5. Firstly the system gets the first key from a first authenticated party in the system and plain text. Then the system generates one random key using RNG and encrypts the plain text to get final cipher text. It starts when the authenticated user enters friendly Key1; the system uses this entered key to generate two random keys RK2 and RK3 using RNG. A random number generator (RNG) is a computational device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. appear random.

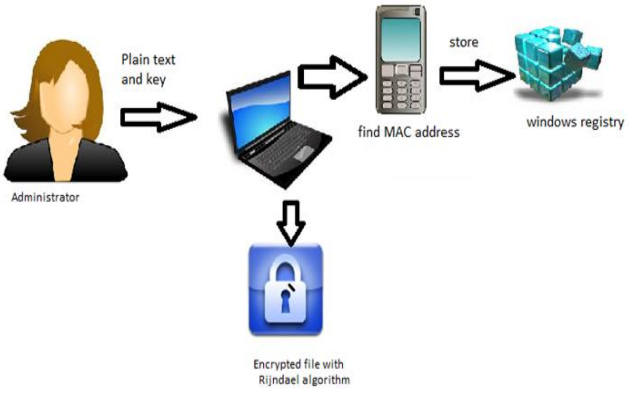


Fig 4 Encryption Process

The proposed system as seen in fig 4 encrypts the plain text for the first time using the entered K1 to generate a cipher text called CTx1 and destroy the plain text. Then the system encrypts CTx1 using RK2 to generate the second cipher text called CTx2 and destroy CTx1. The flowchart of encryption process is shown below.

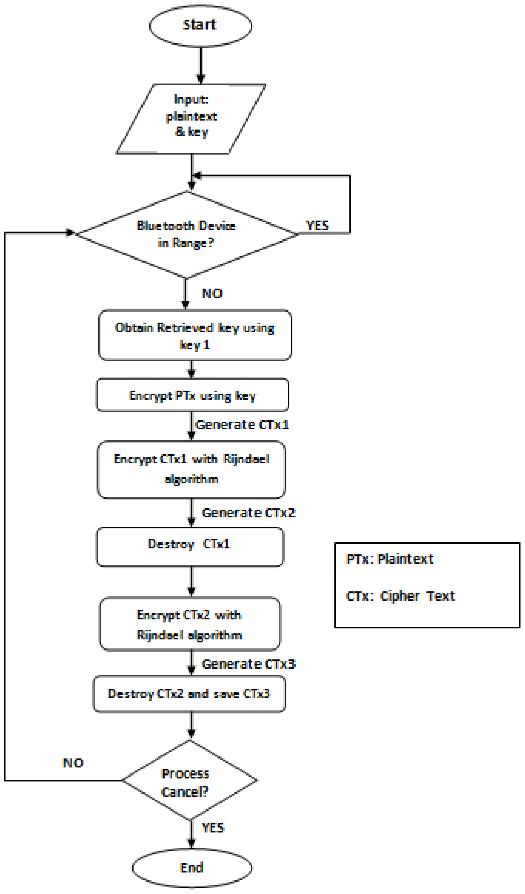


Fig 5 Flowchart of Encryption Process

The final phase in the encryption process is encrypting CTx2 using RK3 to generate the final cipher text called CTx3 and destroy CTx2 which means destroy all intermediate cipher text that are generated through the encryption process and keep only the final cipher text that is called CTx3 which is encrypted by three different keys.

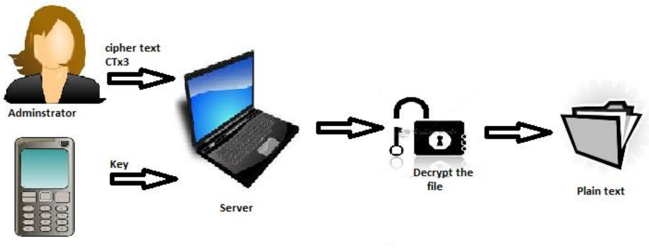


Fig 6. Decryption Process

Finally after completing the encryption process the system guarantee safeness of the keys in storage phases, the system uses Rijndael algorithm to encrypt the keys before distributing it via a Bluetooth connection. After encrypting the used keys are stored in the Windows registry so that it can be used again in future. Then decryption process, as depicted in fig 6, is carried out.

To decrypt the file that contains the cipher text again into its meaningful form. The system needs the MAC address to match with the authenticated party as shown in the flowchart below.

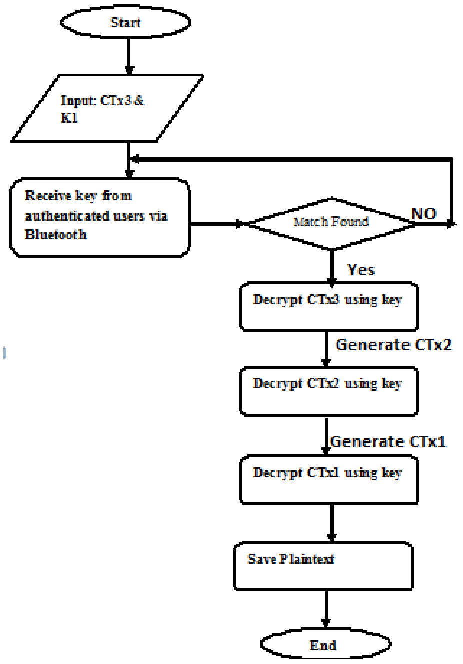
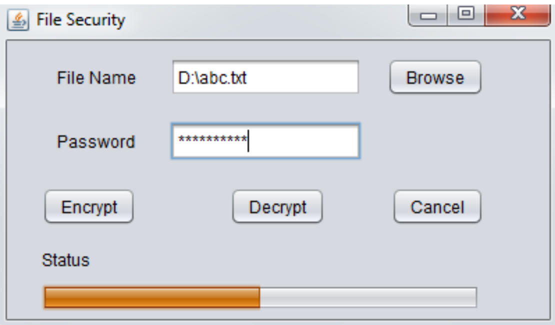


Fig 7 Flowchart of Decryption Process

However, the attacker would have to break the encryption to get the key that protects the megabytes of information. The most common ways is that an encryption application manages keys for the user and depends on an access password to control use of the key. It is rare to use keys in raw form [13].

VII. IMPLEMENTED SYSTEM

This section briefly presents the practical implementation of the proposed system. In the encryption phase, firstly the administrator enters the friendly name of the Bluetooth device and browses the specified file to be encrypted. The selected file may be data, image, media or other file formats.



File Name D:\abc.txt

Password **********

Fig 8. Implemented System

Before the encryption process the system generates the other two random keys and uses them with the entered key in the encryption process by applying Rijndael symmetric algorithm. The two generated keys are stored in the Windows Registry. The MAC Address is unique for each Bluetooth device, thus the system is secure. The result of this operation is a file that contains a cipher text.

The previous steps guarantee the safety of both the file and the keys against unauthorized reading and undetected mutilation.To decrypt the file the system applies the same sequence of the encryption process but in a reverse order using the three key.

VIII. EVALUATION AND DISCUSSION

The proposed system applies a decentralized security system by using the unique MAC Address which guarantees that the decryption did not occur until the Bluetooth device is connected to the system. Inconsequence if the insider or outsider attack can get the encrypted data cannot get the MAC Address and the keys which are stored in the Windows Registry which cannot be accessed unless the user is the administrator

The used keys in the encryption process are generated internally in the system and no one have authority to get their contents which is called a “blind technology” that guarantees the keys safeness against keylogger attack. It is a tool designed to record –log– every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data.

After the encryption process of the private data completes the encrypting keys are encrypted with cryptography algorithm stored in the Registry.

The proposed system prevents any insider or outsider attacks in the private data by encrypting the specified data with a Rijndael block cipher algorithm and prevents any access without having the used keys. The system deletes the initial plaintext and intermediate cipher texts that are generated through the encryption process and keep only the final cipher text.

Bluetooth is selected as a short range technique that is used to transmit the used keys to the authorized parties. Bluetooth has built-in authentication and encryption systems. The authentication between two devices covers only the knowledge of a common secret key called PIN and the knowledge of the device addresses. Encryption is a separate process that starts after authentication is successfully finished.

REFERENCES

1. *André Postma, Willem de Boer, Arne Helme, Gerard Smit, "Distributed Encryption and Decryption Algorithms", University of Twente, Department of Computer Science - Netherland, June 2000.*

2. *Demyo Inc., "What is a vulnerability assessment?", Miami, Florida, USA, July 2011.*

3. *Laura J. Kleen, "Malicious Hackers: A Framework For Analysis And Case Study Thesis", March 2001.*

4. *Smart Handheld Group, Hewlett-Packard Company, "Bluetooth Technology Overview", April 2003.*

5. *Tom Karygiannis & Les Owens, "Wireless network security 802.11, Bluetooth and handheld devices", National institute of Standards and Technology Administration U.S Department of Commerce, November 2002.*

6. *André N. Klingsheim, "J2ME Bluetooth Programming", Department of Informatics University of Bergen, June2004.*

7. *Nikos Mavrogiannopoulos, "On Bluetooth. Security", December 2005*

8. *V.K. Pachghare, "Cryptography and Information Security", PHI Learning Private Limited, New Delhi, 2009.*

9. *Srinivisan Nagaraj, Kishore Bhamidipati, G Apparao, "An Approach to Security Using Rijndael Algorithm", International Journal of Computer Applications Volume 8– No.5, October 2010.*

10. *Lance Bryant, "Caesar Ciphers: An Introduction to Cryptography", Purdue University, Portugal, 2007*

11. *William A. Arbaugh, Narendar Shankar and Y.C.Justin Wan, "Your 802.11 Wireless Network has No Clothes", University of Maryland, March 2001.*

12. *IEEE 802.11, "LAN/MAN Wireless LANS IEEE-SA Standards Association",* http://standards.ieee.org/getieee802/802.11.html

13. *Ozlem Sonmez, "Symmetric Key Management, Key Derivation and Key Wrap", Bochum , Germany, February 2009*

14. *Mostafa-Sami M. Mostafa1, Rowayda A. Sadek2, Noha Hamdy Abd ElKader3," Enhancement Of Data Security Using Bluetooth Technology" Faculty of Computers and Information, Helwan University Cairo, Egypt*

15. *http://www.cp-lab.com/filecrypt/index.html*

16. *http://www.nchsoftware.com/encrypt/index.html*