# Securing Computer Folders Using Wi-Fi And Rijndael Encryption

**Kowsalya.S[1], Ananthy.S[2], Sakthi Deepika.J[3] , Pavithran. K[4]**
[1]Assistant Professor, Dept of Computer Science and Application
[2, 3, 4]Dept of Computer Science and Application
[1, 2, 3, 4] Sri Krishna Arts and Science College, Coimbatore, India

***Abstract-*** *Securing the computer files and folders has been a core issue in the system. Passwords were then introduced to solve this issue but which it lends a host of disadvantages. In this disadvantage of the passwords and solutions to tackle them were clearly defined. Folders are secured via Mobile by using WIFI Technology and a Two Factor Authentication [T-FA] system utilizing WIFI Technology as a factor coupled with the powerful Rijndael Encryption Algorithm was proposed. WIFI is the most commonly used technology for Multipoint connection. Unlike the existing Bluetooth technology it supports with a long range of communication.Rijndael algorithm is an Advanced Encryption standard, believed to be the most effective encryption and decryption cryptographic algorithm of new generation symmetric block cipher. It supports key sizes of 128,192 and 256 bits.Also it has number of rounds depending on key/block sizes,like 10 rounds if the key/block size is 128 bits,12 rounds if the key/block size is 192bits and 14 rounds if the key/block size is 256bits.Rijndael algorithm is a substitution linear transformation cipher,it does not requires feistal network.the computational complexity of* $2^{126.1}$ *for 128 bits,* $2^{189.9}$ *for 192 bits and* $2^{254.3}$ *for 256bits is difficult to crack the key. Coupling the widespread accessibility of WIFI Technology and powerful encryption of Rijndael algorithm, along with a Two Factor Authentication System [T-FA] can be created which will efface the disadvantages of passwords but also creates an user friendly security system.*

***Keywords***- Bluetooth, Wi-Fi, Rijndael, protection, computer, folders, two, factor, authentication, security

## I. INTRODUCTION

In present day, the increasing reliance on computer system has led to the dependence on confidential security measures. Password has become one of the most ubiquitous modern-day security tools and is very commonly used for authentication. These passwords are string of characters used for authentication or user access. Unfortunately, user set password that can be easily memorized, in turn increase threats. Biometrics requires the assumption of unrealistic preconditions for performance gain. Access control system requires time trusted and reliable personal recognition.

To overcome the problem faced by these processes individually, the combination of two or more security processes are implemented. Two-factor authentication has improved security in authentication system. Sensitive files can be provided double protection using Two Factor Authentication. Protecting data has been our primary concern for the computer users all over the world. Windows authentication policies provide securities to a limited extent. However, these policies do not ensure guarantee of personal and organizational security. Windows authentication policies can be broken down easily and cracked easily by the hackers. Hence it does not ensure a full proof security to the users.

Windows does not provide any other secure mechanism other than this. About 30% of the user's password are easy to guess and appear in the hacker's dictionary. Using difficult user password can also create more problems of remembering them.

People generally choose password related to themselves. So other people close to a user can guess the passwords. To ensure security the additional security layer must provide us automated services when we are not in the proximity of the laptop/computer device. The objective of this project is to secure the computer files by using WIFI Technology in mobile, User must enter the password in mobile so that the files are secured via system mobile and files are accessed via mobile or system

## II. EXISTING SYSTEMS

This work is mainly based on the discussions and proposals given in the IEEE papers. In existing securing computer folder technique to Bluetooth technology for securing the folders and files. The Bluetooth technology contains a short range of communication, since it does not contain a high bandwidth. Bluetooth devices are those run on battery power and have a range of about up to 30 feet. This range limitation is meant to avoid the quick reduction of the battery. Since Bluetooth signal will penetrate through walls, however more the objects in between the devices, then lesser the range that devices have.

*2.1 Password security in windows*

The windows password features are interlinked with windows user accounts. Those users having administrator privileges can able to create, modify and delete accounts. For judging the strength of passwords, password policy came into existence. This has been an important issue in the windows system. Key loggers or keystroke logging malwares are effectively protected by the help of password managers. Since, these managers cannot fight man-in-the-middle attacks. The major benefit of passwords is that are portable. These are very much useful in securing web and cloud-based accounts.

Passwords face lots of flaws which are responsible to authorization in web and user interfaces. The bookmarks stored in the web browsers that hold JavaScript to stretch the browser functionality. Even though biometrics and security tokens are alternatives for passwords, they have increase the risk of theft, privacy threat and are increase in infrastructural costs.

Elizabeth Stobert explained in her paper about the password life cycle with the help of following diagram:

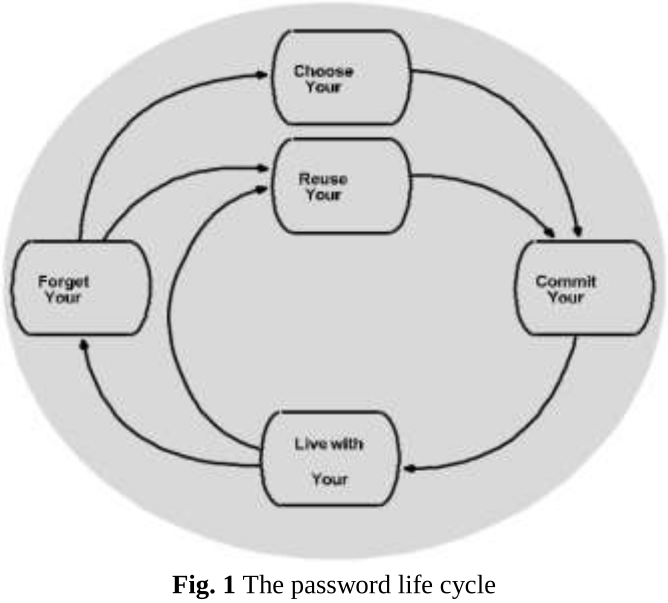

**Fig. 1** The password life cycle

Usually length of passwords plays a vital role in determining the strength. Since mainly depends on the length of passwords. Usually, brute force attack fails in case of long passwords. Those passwords containing alphanumeric characters are another way of strong passwords. Disclosing password should be avoided to prevent social engineering attacks.

*2.2 Vulnerabilities*

There are many reasons for which password are considered as a weak medium of protection. Hence password is user-dependent in network security. Users do not take security procedures for password as serious issue. This tends to vulnerability in passwords. Common problems faced by passwords are follows:

- Note down of difficult passwords somewhere
- Periodically changing of passwords
- Use of dictionary words as passwords
- Using default passwords. For example: password

## III. SOLUTIONS TO PASSWORD VULNERABILITIES

Vulnerability is a threat in the system which can be victim by the intruder to attack the system. This threat can be present in implementation, design or maintenance of system. We can block these threats if we establish a control over vulnerability. Various modes of vulnerabilities are existing in the password protection system. Creating a strong password and generating a high extremity on the frequency of guesses to cracking. Strong policies can also be implementing using Single Sign-On. The load on user can shrinks with the help of strong passwords. Misuse of unattended desktops can be secured with the help of screen locks and time-out. Various problems that are faced by passwords have different solutions. In order to overcome this, two factor authentications is used. This provides a best solution to all the problems facing by passwords.

## IV. TWO FACTOR AUTHENTICATION

The introduction of Two Factor Authentication can be done to increase the Authentication Systems. The overall access to system is not defined by a single factor like password, but combination of multiple factors. To strengthening the security of access control systems, two factor authentication (T-FA) comes in a very handy mainly because it focuses on combinations of both the factors. Christian Rathgeb had defined by his research “Those factors include passwords, representing that ‘something you know’, or physical tokens, such as smart-cards, representing that ‘something you have’. Also, biometric traits are applied, representing ‘something you are’”. (Christian Rathgeb *et a l,* 2010). Popular examples are ATM, Biometrics, etc.

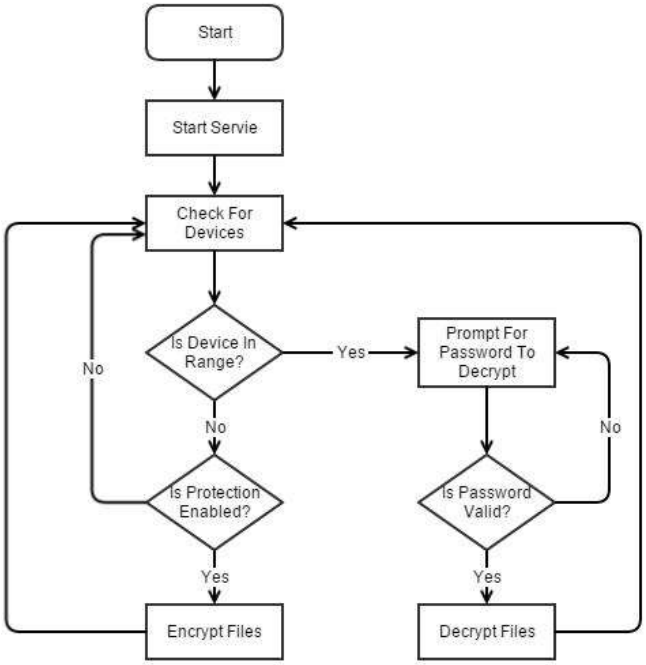

**Fig. 2** Windows Service-Float chart

## V. WI-FI IN TWO FACTOR AUTHENTICATION

Wi-Fi is technology in radio wireless local area networking of devices based on the IEEE 802.11 standards. Wi-Fi is a trademark of Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified products that successfully complete testing of interoperability.

Devices that uses Wi-Fi technologies include desktops, laptops, smartphones, tablets, smart TVs, digital audio players, cars and modern printers. Wi-Fi compatible devices can connect to the Internet through a WLAN and a wireless access point. Those access points have a range of about 30 meters indoors and have a greater range outdoors. Hotspot coverage can be as small as a single room with walls can block radio waves, or as large as many square kilometres achieved by multiple overlapping access points.
Device that sending information wirelessly to another device, both connected to the local network, to print a document. Various versions of Wi-Fi exist, with a different range, radio bands and speeds. Wi-Fi commonly uses the 2.4 gigahertz (12 cm) UHF and 5.8 gigahertz SHF ISM radio bands; these bands can subdivided into various channels. Each channel can be time-shared by various networks.

These wavelengths are work best for line of sight. Most common materials can absorb or reflect them, which may further restrict range, but can tend to help and minimise interference between different networks in an crowded environments. At close range, most versions of Wi-Fi, running be on suitable hardware, can achieve speeds of over 1 Gb/s.
Anyone within range on a wireless network interface controller can attempt to access the network; so Wi-Fi is more vulnerable to attack (called eavesdropping) than that of wired networks. Wi-Fi Protected Access (WPA) is a technology created to protect information transferred across Wi-Fi networks and includes solutions for personal and enterprise networks. Security features of WPA can included stronger protections and some new security practices as the security landscape has changed over time.

## VI. RIJNDAEL ENCRYPTION

Rijndael Cipher is an Advanced Encryption Standard (AES) that is based on design principle grounded as substitution permutation network and is a quick in both software and hardware. Avoiding Fiestal network in the AES is an important characteristic. AES is a variant of Rijndael has fixed block size of 128 bits and a key size of 128, 192 or 256 bits. Here key size specifies the total number of rounds for converting plaintext to cipher text. They are,

10 rounds for 128 bit keys
12 rounds for 192 bit keys
14 rounds for 256 bit keys

There are 4 processes in each round namely,

Sub Bytes Transformation
Shift Rows Transformation
Mix Column Transformation
Add Round Key (Zahir Zainuddin *et al*, 2013)

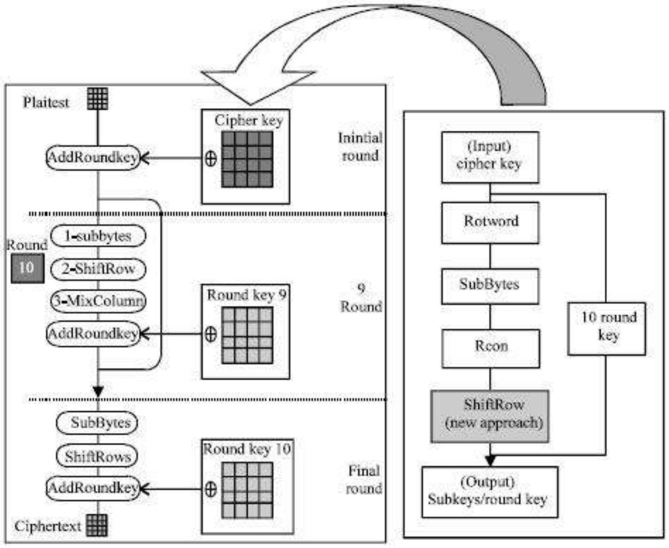

**Fig. 3** Steps in Rijndael Encryption

### *6.1 Advantages*

Rijndael Algorithm is widely considered as one of the best algorithms for encryption. Efficient implementation of the algorithm is due to the characteristics of its design which made easy to understand. Joan Daemen in his paper defines that "It also facilitates understanding the mechanisms that give the algorithm its high resistance against differential cryptanalysis and linear cryptanalysis, to most important general methods of cryptanalysis in symmetric cryptography". (Joan Daemen & Vincent Rijmen *et al,* 2010).

## VII. PROPOSED SYSTEM

This project is proposed with WIFI technology. WIFI is one of the greatest connective technologies. Its range is up to 100m. The greatest part is what Wi-Fi technology has a global standard. WIFI allows users to stay connected all of the time. In this approach the investment on wireless network hardware is reasonable, especially in comparison to wired cables that are difficult to install and manage.

WIFI is easy to expand and can take on additional users with existing equipment, unlike wired cables which require additional wiring and installation. This project also contains file transformation concept (i.e.) from system to mobile. The objective of this project is to provide the necessary security for computer folders and files by using rijndael encryption algorithm. The folders are secured, and files are transfer to mobile phone by using WIFI technology.

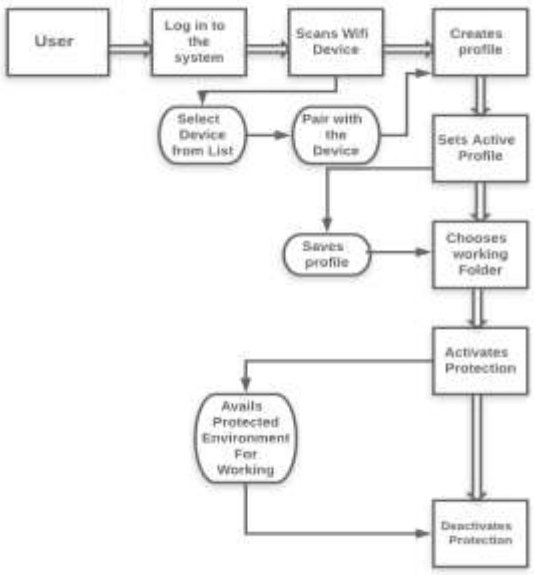

**Fig. 4** system design

## VIII. CONCLUSION

Securing computer folders and files by using Rijndael Encryption algorithm widely supported in existing WIFI Technology. Java and android connectivity has been implemented. Two Factor Authentications (T-FA) for more security was provided. Finally, and folders have been secured and files have been transferred to mobile phone. Main advantage of this paper is, there is no need of internet connectivity. This approach mainly helps to secure the sensitive files and folders so that user can access their files more securely.

## REFERENCES

[1] Mrs Aruna Gawde, Sanchit Jaina, Mohsin Masanib, Sahil Deliwalaa, Securing Computer Device Using Bluetooth Technology and Onr Time Password, International Journey of Engineering and Computer Science ISSN:2319-7242 Volume 4 Issues 4 April 2015, Page No.11426-11429

[2] Daniel Fowles, Implementation and analysis of the Rijndael encryption algorithm in different programming languages, April 2008.

[3] Nikita Saple, Dhanraj Poojar, Ankita Lesarka and Alka Srivastava Securing Computer Folders using Bluetooth and Rijndael Encryption, International Journel of Current Engineering and Technology, E-ISSN 2277 – 4106, 16 Feb 2015,20 Feb 2015, Vol.5,No.1.

[4] Prof. V.P.Patil, Onkar Hajare,Shekhar Palkhe, Burhanuddin Rangwala, Wi-Fi Based Notification System, The International Journel Of Engineering And Science, Vol.3, Pages 08-12-2014.

[5] Sumant Ku Mohapatra, Ramya Ranjan Choudhury, Pravanjan Das, THE FUTURE DIRECTIONS IN EVOLVING WIFI-TECHNOLOGY APPLICATIONS AND SERVICES, International Journel of Next-Generaton Networks (IJNGN) Vol.6, No.3, September 2014.