Enhancing File Security by Rijndael Algorithm Using Combination of Other New Generation Security Algorithms

Anshu Dixit[#1], Ashish Kumar Jain[*2]

[#1]M.TECH Student, IT Department, BUIT, Bhopal (M.P.), India

*2 Asst.Prof. Head Dept. of MCA, IT Department, BUIT, Bhopal (M.P.), India

***Abstract*— The one of the famous algorithm is Advanced Encryption Standard (AES) that is used Rijndael Algorithm. The cipher standard algorithms selected, by a Rijndael algorithm because of its high performance of security. In this paper used for file security three different kinds of algorithms i.e. RIJNDAEL, Initialization vector (IV), SHA512 Hashing algorithm these three popular algorithms are used for file encryption and decryption approach. The first is the Rijndael algorithm used for file encryption/decryption it is using a key and Initialization vector (IV), the second Initialization vector algorithm is for encrypting the first portion of data to be encrypted and the third one is SHA512 Hashing algorithm takes a string and transforms it into a fixed size the same or 512 bits of data string. The encryption and decryption operation used to increase the strength of security and high performance provides for file security**

***Keywords*— RIJNDAEL, Initialization vector (IV), SHA512 Hashing Algorithm, Enhance, Encryption, Decryption, Security.**

I. INTRODUCTION

The U.S. National Institute of Standards and Technology (NIST) established the specification for encryption of electronic data is an Advanced Encryption Standard (AES) established by Rijndael is a family of ciphers with different key and block sizes. The algorithm described by the AES is a symmetric key algorithm; the same key is used for both encrypting and decrypting the data. A variant of AES is Rijndael which has 128 bits of fixed block size, and a 128, 192, or 256 bits of key size. By the Rijndael specification per size is specified with a block and key sizes that may be any multiple of 32 bits, both with a maximum of 256 and a minimum of 128bits.

For stronger security the Advanced Encryption Standard (AES, Rijndael) algorithms used to key for file encryption with change extension. Both of these ciphers are regarded as being very secure.

To protect the file against unauthorized reading and undetected mutilation, with a secret cryptographic key of a symmetric cryptosystem by authenticated user encrypted it. The symmetric key is needed to encrypt or decrypt data with confidentially. The cryptographic keys are used in data encryption to make the file more secure. To decrypt the data the same key must be used. The key either memorize 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 in previous form. For storage used the window registry, unless the administrator, the registry cannot be edited or deleted.

For the achieve encryption and decryption approach use for file security three different kinds of algorithms i.e. RIJNDAEL, Initialization vector (IV), SHA512 Hashing algorithm. Each one of them has its own benefits and limitations. The secure hashing technique is used in a string and transforms it into a fixed size (512 bits) of "encrypted data" and the same string will always "hash" into the same 512 bits of data. This algorithm is proposed file security shown in the next section.

II. PROBLEM STATEMENTS

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

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 by applying a new method. This method is a file encryption with a symmetric key management system that approach using window registry.

III. Previous Related Works

There are many systems try to solve the problem for access the private data to increase the security by adding a second key to the algorithm and keep the performance close to traditional algorithm, and some results which have been extracted, The execution time of encryption and decryption operations in both enhanced and traditional algorithms are close from each other, if the execution time of generating key has been excluded from this calculation. If a large number of open sessions by the sender and receiver use, the differences between execution times of generating key/keys will be larger. Rijndael algorithm has been enhanced by adding second key as it has been explained above and the implementation shows that if any bit changed within key, the half of cipher file will be changed that is called "On bit test" which is the simplest way to test the algorithm strength. The unfortunately other tests are much expensive and need more hardware and special environment to do them and get clear results. [2]

The most effective attack method is Square attack at present. It needs to improve the Rijndael algorithm. This work was proposed an improvement blueprint which imports prefix code, because the square attack method depends on invariable of encryption system to attack. So it can make encryption system changes with different plaintext inputted, and therefore increases security and make the algorithm have resistant ability against Square attack radically. Analysis shows that the proposed blueprint can improve its algorithm effectiveness under the precondition that it will not influence algorithm efficiency. [1]

Digital signatures are used to achieve some of the properties for hand signatures, e.g. (Validity and Verifiability). The bandwidth of subliminal channel is defined as how many bits of covert message can be transmitted through such a channel in one session of protocol run. It measures the capacity of the subliminal channel in conveying hidden information. They do not propose a method for the extension of the authentication system to image and extend digital signatures. [3]

IV. APPROACHES Used For Enhanced File Security

There are several standard algorithms available to encrypt and decrypt files. The most three popular algorithms are Initialization vector, SHA512 and Rijndael. The following section presents the benefits and limitations of file security.

A. INITIALIZATION VECTOR

Initialization vector (IV) is an arbitrary number that can be used as along with a secret key for data encryption. The use of IV is prevented to repetition in data encryption, making it more difficult for the hacker using dictionary attack to find patterns and break a cipher. If there are repeated sequences in encrypted data, an attacker assumes that the corresponding sequences in the message were also identical. Initialization vector prevents the corresponding duplicate character sequences in the cipher-text.

The ideal IV is a random number that is made known to the destination computer to facilitate decryption of the data when it received. The IV can be agreed in advance, transmitted independently or included as the part of the session setup prior to exchange of the message data. The length of the IV depends on the method of encryption. The IV length is comparable to the length of the encryption key or block of the cipher in use. It is used to encrypt the first portion of the data to be encrypted in file security.

B. SHA512 Hashing

To calculate a SHA hash with 512 Bits from sensitive data like passwords, a file is to create a SHA-512 checksum. They additionally provide a shared key to strengthen for the security of the hash. A hash function is an algorithm that transforms hashes an arbitrary set of data, such as a text file, into a single fixed length value the hash. The computed hash value may be used to verify the integrity of copies of the original data without providing any means to derive said original data.

SHA-512 is novel hash functions computed with 64-bit words used for secure password hashing. Its use in different shift amounts and additive constants, but its differing only in the number of round structures is virtually identical.

C. RIJNDAEL Algorithm

Rijndael allows for both key and block sizes to be chosen independently from the set of {128, 160, 192, 224, 256} bits. It managed is an implementation; it will allow selecting different block sizes (although both block and key sizes). The Rijndael algorithm is a new generation symmetric block cipher that supports key sizes in bits, with data handled in blocks however; excess of AES design criteria, and the block sizes can mirror those of the keys. A Rijndael use is a variable number of cycles through which cipher rounds, depending on key/block sizes, as follows:

9 rounds if the key/block size is 128 bits.
11 rounds if the key/block size is 192 bits.
13 rounds if the key/block size is 256 bits.

Rijndael is a substitution linear transformation cipher that is not requiring a Feistel network. It uses triple discreet invertible uniform transformations, and uses the following: key addition transforms, linear mix transform, non-linear transforms. Even the first round before, a simple key addition layer is performed, which is added to security, used for encryption/decryption for file security. This approach is to use a 256 bit key and a 128 bit IV.

It's used iterated block cipher, the encryption or decryption is a block of data is accomplished by the iteration (a round) of a specific transformation (use a round function). It accepts one-dimensional 8-bit byte arrays that create data blocks. The data is input and then mapped onto state bytes.

The iterated block cipher, use the different transformations operate in sequence on intermediate cipher results. Key Size and Block Size are a prime feature of Rijndael is able to operate on varying sizes of keys and data blocks. It provides flexibility in that both the key size and the block size 256 bits. The sub and schedule key by the Rijndael key schedule, sub keys are derived from the cipher key. The cipher key is expanded, to create an expanded key and the sub key is created by deriving a "round key" by round key. To the required round key length is equal to the data block length multiplied by the number of rounds plus 1. The round keys are taken from the expanded key.

To managed security system, from the cipher key the expanded key is always derived. The method ensures that the expanded key is never directly specified, which Rijndael up to several cryptanalytic attacks against its key generation methods. To recall the security of the system depends entirely on the secrecy of the key, the design of the algorithm itself is public and contains no secrecy.

Enciphering with the Rijndael cipher is an interactive block cipher. It is consists of a sequence of transformations is to encipher or decipher the data. Rijndael work with encryption and decryption begin and end with a step mix sub-keys with data block. The extra step is done with protection against cryptanalysis. [4]

V. Proposed Work

The proposed system depends on the file encryption 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 that referred to as a key. Keys are saved only with authenticated user or administrator. [5]

In the proposed system file security needs input file to be encrypted and a system that will cover the encryption process as shown in the workflow of the system in fig 1. Firstly the system gets select file and enter key from an authenticated user, and the system wants to re-enter the key, then the system generates byte code when it's successfully encrypted, file with change ".encrypt" extension. It starts when the authenticated user enters string or password. The key is generating a sequence of numbers of bytes that uses alphabetic, numeric or symbols that lack any pattern.

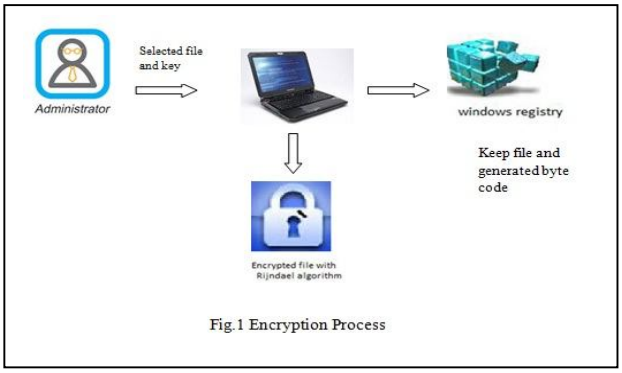

Fig.1 Encryption Process

The file security on the proposed system shown in fig. 1 encrypts the file for the entered key to generate byte code and encrypted with ".encrypt" extension. Then the file encryption used the initialization vector and SHA512 hashing key. The

flowchart of the encryption process is shown in below in fig. 3

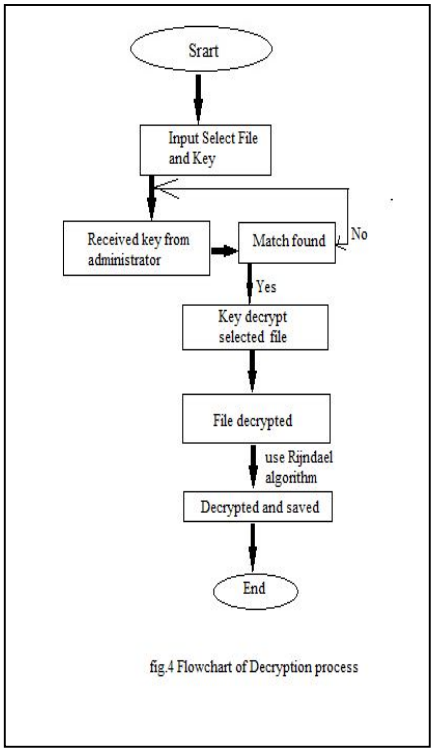

fig.4 Flowchart of Decryption process

The final phase in the encryption, process encrypting the file with the Rijndael encryption and the file encrypt with generating the final byte code through the encryption process and keep only the final file with change extension which is encrypted by three different keys.

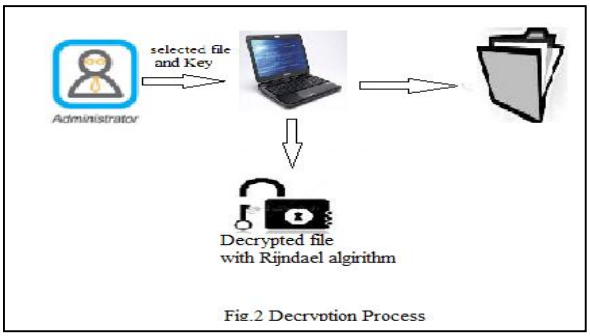

Fig.2 Decryption Process

Finally after completing the encryption process the system file guarantee safeness of the keys in storage phases is, the system uses with a Rijndael symmetric algorithm to encrypt the keys. After encrypting the used keys are stored in the Windows registry by the authenticated user so that it can be used again in future. Then decryption process, as shown in fig 2

To decrypt the file that contains the data again into its meaningful form. The key to access the file in its original form, the system needs to encrypt same key to decrypt the file with its old extension [6], which is to match with the key and use it's only by authenticated user that's shown in fig. 4

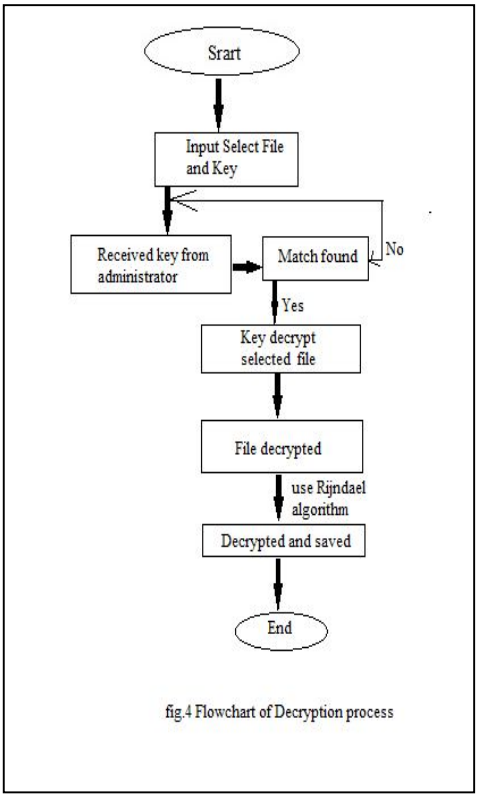

fig.4 Flowchart of Decryption process

VI. Implementation of System

This section briefly processes the practical implementation of a file in the system. In the encryption phases, firstly the administrator or authenticated user selects the file, and browses the specified file to be encrypted. The selected file may be data, media, image or other file formats are accepted.

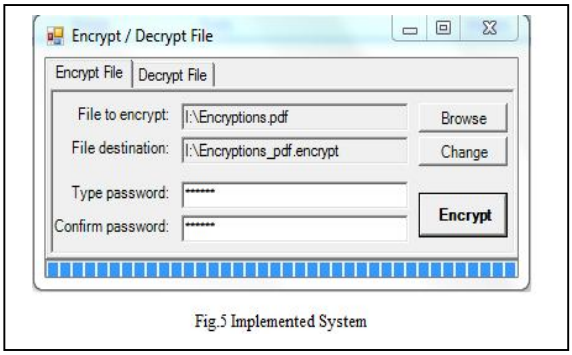

Fig.5 Implemented System

Before the encryption process the system needed two random keys and uses them to enter key in encryption process and applying the Rijndael symmetric algorithm. The keys are stored in the window registry. Then the file is secure on the system .the result of this operation is a file that contains the data. The encryption process is completed successfully generated byte code, key is that calculated total bytes processed that's show process is completed. Shown in fig.6

Fig.6 Encryption completed

The previous steps guarantee the safety of both the keys and file 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 different key to obtain original file formats.

VII. Evaluation And Discussion

The proposed system used for file security system by using the unique key for encryption which is guaranteed that decryption did not occur until it's not completely generated byte code by the Rijndael symmetric algorithm. That key which is stored in the Windows Registry which cannot be accessed unless the user is the administrator.

The used keys in the encryption process that 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 is safe against key-logger attack. 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 the other private data.

After the encryption process of private data file completes the encrypting keys are encrypted through the byte code 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 symmetric algorithm and prevents any access without having the used keys. The system deletes the initial data file and intermediate data that are generated through the encryption process and keep only the final data.

The authentication between user and system that covers only the knowledge of a common secret key called password or string and the knowledge of the device addresses, encryption is a separate process that starts after authentication is successfully finished.

REFERENCES

[1] Zhiqiang Xie1,2, Pengfei Gao1, Yujing He1, and Jing Yang2, "Study on Improved Rijndael Encryption Algorithm Based on Prefix Code," Journal of Springer, Springer-Verlag Berlin Heidelberg 2012.

[2] Ibtihal Mohamed Abdullateef Fadul1 and Tariq Mohamed Hassan Ahmed2, "Enhanced Security of Rijndael Algorithm using Two Secret Keys" International Journal of Security and Its Applications, Vol. 7, No. 4, July, 2013.

[3] Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi,"Secure Digital Signature Schemes Based on Hash Functions," International Journal of Innovative Technology and Exploring Engineering, 2(4). Pp 321-325 ISSN 2278-3075, 2013.

[4] Srinivisan Nagaraj, Kishore Bhamidipati, G Apparao, "An Approach to Security Using Rijndael Algorithm", International Journal of Computer Applications, Volume 8– No.5, pp: 365-403, 2010.

[5] Andre Postma, Willem de Boer, Arne Helme, Gerard Smit,"Distributed Encryption and Decryption Algorithms", University of Twente, Department of Computer Science - Netherland, pp : 417-423 2000.

[6] Ozlem Sonmez, "Symmetric Key Management, Key Derivation and Key Wrap", Bochum, Germany, in Ruhr-University at Bochum 2009.

[7] Jaspreet kaur, Er. Kanwal preet Singh,"Comparative Study of Speech Encryption Algorithms Using Mobile Applications", International Journal of Computer Trenda and Technology ,pp:2346-2350 2013

[8] G. Sivagama Sundari , C. Srimathi, P.Sakthivel,"A New Approach towards identification of spam, spoofing using Domain Keys" , The Journal of Engineering, Science and Technology Management, pp:61-64 (JEST-M, ISSN 2277-5161 Vol. 2, Issue 1, 2013