Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, December 2021: 5510-5514

Securing Files Using Hybrid Cryptography

Dr. V. Padmavathi, M. Jayanth Kumar, M. Saikiran Reddy
Department of Computer Science and Engineering, Anurag Group of Institutions, Hyderabad, Telangana

ABSTRACT

Data Security in terms of file encryption is very crucial, every file nowadays is important as it contains either personal information or industrial data. Hybrid encryption is achieved through data transfer using a combination method of symmetric and asymmetric encryption algorithms. Users can safely send files through hybrid encryption. Asymmetric encryption slows down the encryption process when used alone so symmetric encryption is used for file encryption, advantages of both forms of encryption are utilized. The result is another layer of security with no extra burden to system performance. The idea of hybrid encryption is very simple. Instead of using just AES only to encrypt the file, we use AES to encrypt the file. Then to maintain the secrecy of the key, we encrypt the key using RSA. This discussed paper is a completely different approach which is used for securely storing files. This proposed scheme will also make sure the newly proposed model to have confidentiality and integrity mechanisms.

KEYWORDS: Cryptography, Encoding, Decoding, Security.

I. INTRODUCTION

Data stored in files can be accessed or retrieved on the users request without direct access to the server computer [12]. This Security problem can be solved using several different ways, cryptography and steganography are the most commonly used techniques. But sometimes a single algorithm alone cannot provide security that is required. Hybrid encryption is achieved through data transfer using a combination method of symmetric and asymmetric encryption algorithms. Files are the basic and important units of a system. Data is usually stored and shared in form of files. This makes file security as a subset of data security that requires secure use of files [2] whereas File security, protects files such as personal information of users and other business files. But this security can still fail if professionals attempt to break through the security barricades. Our paper aims to secure the files to different level which makes this data being leaked into the wrong hands even more difficult.

II. LITERATURE SURVEY

A literature review is a survey across sources for a particular topic. It is complete overview of existing knowledge. It helps us on familiarizing topic.

The paper represents on how files are stored securely on a cloud platform with the help of encryption. Also, it also depicts the problems arising because of using only a single algorithm to encrypt the file and how ineffective it will be on the cloud [4].This paper splits shows file encrypted using AES. The key information about which file uses which algorithm is sent to the receiver using RSA modern approach to file system integrity.

The main focus of the paper is on the integrity of files and restoring the files if integrity is violated. The proposed system uses a pattern of each protected file to determine its modification [3][5]. The method used for pattern generation is cryptographic hash functions. The system also stores the files that need to be protected and also stores their hash codes. Checking integrity of files is simple, new hash generated can be compared to one in database. If the file gives correct hash, then access is granted else the admin gets alert and if a saved copy is available of the same file, then the file is restored.

The paper focuses on the implementationon secure store and shares the data in a group using cloud technology for storage [1]. The method discussed in the paper encryption techniques related to group signatures. The advantage of this method is that storing file is possible without data owners showing their identity to others in the cloud. Public key exchange known as (PKA) uses a two-key system, consisting of the public and the private keys, where messages are encrypted with one key and decrypted with another.

A cryptography algorithm needs a key along with a file or message of any format to form the encrypted ciphertext [3] [6]. The level of security of ciphertext depends on the strength of the cryptographic algorithm and the privacy of the cryptographic key used. Thus, the first security has been given. Another data hiding technique called steganography can be used for more security. The cryptography is used to provide security to information in networks that are not secured and which can only be accessed by the actual receiver.

This paper describes on how a cryptography key can be shared with other users to whom access to informationis needed. It also points the problem where a single key is used to encrypt all data and using different keys for files. The solution described in the paper tries to address both the problems using key aggregation. Key aggregation means encrypting different data files with different keys but a single aggregated key is used to decrypt them. The encryption algorithm used is AES [10].

In our proposed system there are two main entities: sender and receiver who got access from sender. The owner will upload the file that is required to be stored at a remote location or needs to be shared with other users [8].The owner gives access to other users by sharing the required metadata to decrypt the file using an asymmetric cryptosystem.

III. ALGORITHMS

Advanced Encryption Standard (AES) AES is an iterative cyphernot Feistel cipher as in DES. It is based on the substitution and permutation done in an order. It forms a series of operations, some of these operations involve replacing input by some outputs known as substitutions and some operations involve bits to be shuffled known as permutations. AES implements its operations on bytes rather than bits. Hence, AES uses the 16 bytes instead of 128 bits of a plaintext block. These 16 bytes are placed in four columns and four rows as a matrix.

The number of rounds in AES is variable and rounds depend on the length of the key used whereas it’s fixed in DES. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and

14 rounds for 256-bit keys as mentioned it varies depending on key size. Each of these rounds uses a different round key, which is calculated from the previousmain AES key using a key generation procedure.

Encryption:

AES considers each block as a 16-byte (4-byte x 4 bytes = 128) grid in a column major arrangement.

Each round comprises of 4 steps:

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

Decryption:

Rounds of AES can be easily undone as these rounds have an opposite to it which when performed negate the changes done in encryption stage. Each 128 block will go through the 10,12 or 14 rounds depending on the key size similar to encryption but order of operations will differ.

The stages of each round in decryption are as follows:

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

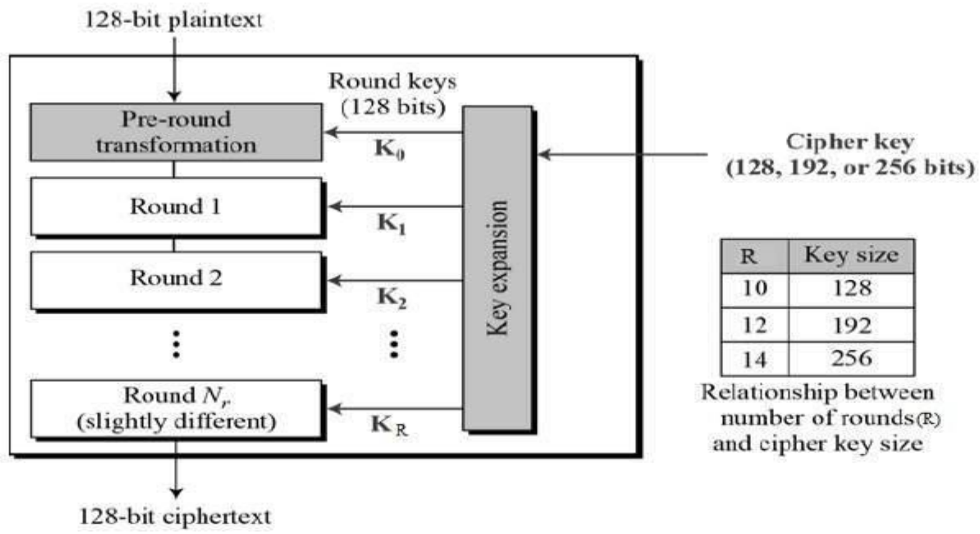

Fig. 1. Working of AES Algorithm

RSA (Rivest, Shamir, Adleman) algorithm is an asymmetric cryptography algorithm. Asymmetric cryptographymeansusing two different keys where one is used for encryption and one for decryption i.e., Public Key and Private Key. As the name describes, the Public Key is usually given to everyone and the Private key is kept safe.

The point of RSA is based on the fact that it is very difficult to factorize aextremely big integer. The public key is created using two numbers where one number ismultiplication of two very large prime numbers. And private key is also created from the same two prime numbers. If factorization of the large number happens, the private key is likely compromised. Therefore, encryption in RSA completelydepends on the key size and if we double or triple the key size, the encryption strength increases exponentially according to key size. RSA keys are usually 1024 or 2048 bits long, but research shows that 1024-bit keys will be broken in near future. But till now it was impossible tobreak 1024-bit key also.

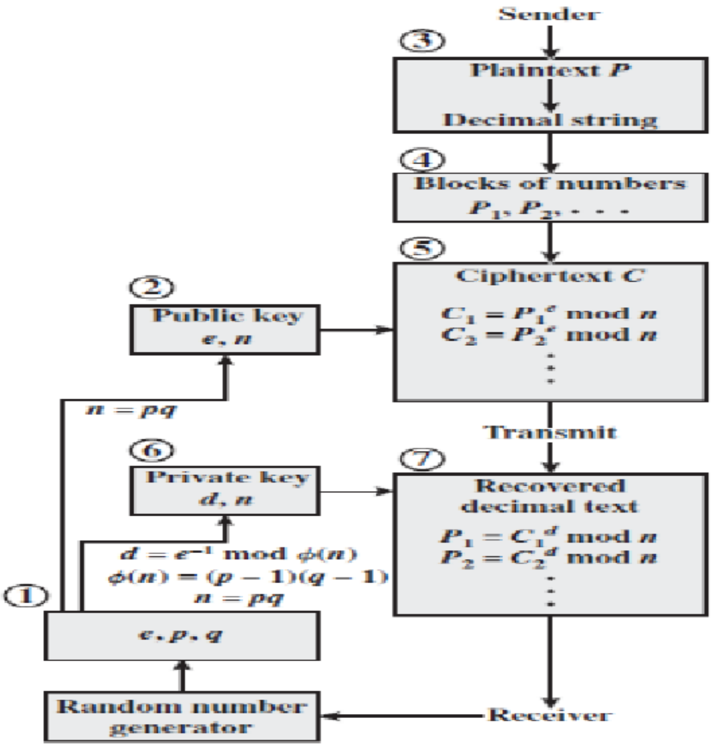

Fig. 2. Working of RSA algorithm

IV. RESULTS AND DISCUSSION

The stored file is completely secured, as the file is being encrypted by using symmetric key cryptography and asymmetric key cryptography techniques. The system formed by hybrid encryption is very secure and robust compared to simple encryption. Data of the users is secured avoiding unauthorized access from the outsiders. Data security is very crucial and is a priority. This system can be implemented in the banking and corporate sectors to securely transfer confidential data.

V. CONCLUSION

Based on the survey it was identified that secure file storage and sharing would not only require confidentiality but also authentication and integrity. To overcome the drawbacks of simple encryption, hybrid encryption is proposed which tries to provide an enhanced solution for securely storing the files.

REFERENCES

[1] Maitri, P. V., & Verma, A. (2016). Secure file storage in cloud computing using a hybrid cryptography algorithm. 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 1635–1638. https://doi.org/10.1109/wispnet.2016.7566416

[2] Shaikh, S., & Vora, D. (2016). Secure cloud auditing over encrypted data. 2016 International Conference on Communication and Electronics Systems (ICCES). doi:10.1109/cesys.2016.7889842

[3] Gajendra, B. P., Singh, V. K., & Sujeet, M. (2016). Achieving cloud security using third party auditor, MD5, and identity-based encryption. 2016 International Conference on Computing, Communication, and Automation (ICCCA), 1304– 1309. https://doi.org/10.1109/ccaa.2016.7813920.

[4] Bhandari, A., Gupta, A., & Das, D. (2016). Secure algorithm for cloud computing and its applications. 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), 188–192. https://doi.org/10.1109/confluence.2016.7508111.

[5] Taha, A. A., Elminaam, D. S. A., N Hosny, K. M. (2018). An Improved Security schema For Mobile Cloud Computing using Hybrid cryptographic algorithms. Far East Journal of Electronics and Communications, 18(4), 521546.https://doi.org/10.17654/ec018040521.

[6] Kranthi Kumar K, Devi T,(2018). Secured Data Transmission in Cloud Using Hybrid Cryptography. International Journal of Pure and Applied Mathematics, 119(16), 3257-3262.

[7] Shimbre, N., & Deshpande, P. (2015). Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm. 2015 International Conference on Computing Communication Control and Automation. doi:10.1109/iccubea.2015.16.

[8] Ronak Karani ,Tejas Chaudhari , Anindita Bhajan , Madhu Nashipudi Math 2020). SecureFile Storage Using Hybrid Cryptography.2020 International Journalofinnovative Research In Technology, 6(9).37.

[9] Shakeeba S. Khan, Prof. R. R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms”, 2015.

[10] Anjali Patil, Nimisha Patel, Dr. Hiren Patel “Secure data sharing using cryptography in cloud environment”, 2016.

[11] Palanisamy, V., & Mary, J. (n.d.). Hybrid Cryptography by the Implementation of RSA and AES. Retrieved November 26, 2021, from https://www.journalcra.com/sites/default/files/issue-pdf/546.pdf.

[12] Lin Zou, Ming Ni,Yiting Huang. Hybrid Encryption Algorithm Based on AES and RSA in File Encryption Retrieved February 2020, from https://www.researchgate.net/publication/339491993_Hybrid_Encryption_Algorithm_Based_on_AES_and_RSA_in_File_Encryption.