ISSN No:-2456-2165

Secure File Storage Using Hybrid Cryptography

Aditya SadanandGhadi
Research student, Department of Information Technology
B. K. Birla College of Arts, Science, and Commerce (Autonomous)
Kalyan, India

Abstract:- Nowadays the growing use of mobile devices and advancement in networking technology is leading us to secure file storage over the network. Cryptography is the most popular technology used for all types of data security. This discussed paper is a broad survey of the different approach which is used for securely storing files, and sharing it over the network. This proposed scheme will also ensure the whole model to have confidentiality, integrity, and availability mechanisms to be implemented in it.

Keywords:- *Cryptography, Confidentiality, Integrity, Availability, Storage, and Security.*

I. INTRODUCTION

The aim of the project is to create an encrypted and secured file storage system to transfer files within users in a remote location. This system will require an input that is successfully encrypted using any of the algorithm techniques and store them anywhere. The uploaded file can be downloaded by other users, but to read the data present in it, they have to decrypt the file using the decryption algorithm and the information provided about the file within the users by the owner. The system uses public-key cryptographic techniques like RSA and Symmetric key cryptography like AES. Hashing techniques like static hashing and dynamic hashing are used for performing integrity. Due to the encryption of data, confidentiality is also achieved in the process. The project is also open to new challenges and future changes to other advanced technologies in keeping the data secured.

II. OBJECTIVES

The proposed paper meets the required security needs and implementation of the data center of the cloud server. The paper uses some symmetric key cryptography techniques in addition to stenography techniques. The idea of splitting and merging adds on to meet the principle of data security. This hybrid approach when implemented in a cloud server makes the remote server more secure and thus, helps the cloud providers to do their work more securely. For data security and privacy protection problems, the fundamental challenge of separation of sensitive data and access control is fulfilled. The Cryptography technique converts original data into ciphertext. The cryptography technique is divided into symmetric-key cryptography and public-key cryptography. So only an authorized person can access data from the cloud server. Ciphertext data is visible for all people. But for that again the decryption technique has to be used to translate it back into the original text.

III. LITERATURE SURVEY

A literature review is nothing but an objective, aim, or summary of whatever research has done relevant to a certain topic. The following published articles have been referred to create a base for my project. Following are some papers been referred to:-

Secure file storage in the cloud using Hybrid Cryptography;

[1] Author - Punam V. Maitri, Aruna Verma, Year – 2016
Description – The paper focuses on how files are securely stored on a cloud platform. Also, it discusses the problem of using only a single algorithm to encrypt the file and how ineffective it will be on the cloud. This paper splits the file into blocks and each block is encrypted using AES, blowfish, RC6algorithm. The key information about which file uses which algorithm is sent to the receiver using steganography modern approach to file system integrity checking [2]

Author – M. Malarvizhi, J. Angela JennifaSujana, T. Revathi, Year – 2014
Description - 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. The method used for pattern generation is cryptographic hash functions. The system also uses a database that stores the files that need to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. If the file is successfully tested positively then access is granted otherwise the administrator gets alerted and if it is saved copy is available of the same file then the file is restored.

New approach to user authentication using digital signature [3]

Author - Jerzy Kaczmarek, MichałWróbel, Year -2008
Description – This paper describes an approach to the integrity of files and restoring the files if any problem is arising in the future. This proposed course uses a pattern of each protected file to determine its modification. Methods used for pattern generation are cryptographic hash functions. This system uses a database that stores the names of all files

that are to be protected and their hash codes. To check the integrity of the file the hash code of the file is produced and checked with one in the database. After the file is verified then only access is granted else the administrator is been alerted about the problems and a saved copy of the same file is restored safely. Secure file sharing using cryptographic techniques in the cloud [4]

Author - RashiDhagat, Purvi Joshi, Year– 2016 Description – The paper focuses on providing the facility to securely store and share the data in a group using cloud technology for storage. The method discussed in the paper uses group signature and encryption techniques. The advantage of this proposed method is that data owners can store the file without showing their true identity to others in the cloud. Public key exchange known as (PKA) [5]

Author - Bilal Habib, Bertrand Cambou, DuaneBooher, Christopher Philabaum, Year – 2017
Description – This paper provides a new method to implement the public key infrastructure. The PKI has the disadvantage that the mathematical relation between public and private between the public and the private key is maintained. Paper proposes a new PKI scheme with addressable elements (PKA). The approach proposed removes the mathematical relation between public and private keys using addressable cryptographic tables. Secure data sharing in cloud storage using key aggregation cryptography [6]

Author - Tulip Dutta, Amarjyoti Pathak, Year – 2016
Description – This paper discusses how a secret key can be shared with other users to whom access needs to be given. It discusses the problem with using a single key to encrypt all data and using different keys for different files. The solution described in the paper tries to address both the problem using key aggregation. In key aggregation, different data files are encrypted with different keys and then for decryption, a single aggregated key is used. The encryption algorithm used is AES and the system is being implemented in java using the key store data structure. Achieving cloud security using third party auditor, MD5, and identity- based encryption [7]

Author -Bhale Pradeep Kumar Gajendra, Vinay Kumar Singh, More Sujeet, Year – 2016
Description – This paper overcomes the security tradeoff and improves the performance of data transmission and increases security. Also, MD5 hashes are no longer considered cryptography secure. An approach to hybrid cryptography on cloud environment [8]

Author -Mr. Rohit Barvekar, Mr. ShrajalBehere, Mr. Yash Pounikar, Ms. Anushka Gulhane, Year -2018
Description - The proposed security mechanisms will prevent confidential data from being misused making the system more reliable. High speed: The proposed method will make encryption and decryption with proper keys much faster than usual. Security in Cloud Computing using Cryptographic Algorithms [9]

Author - Shakeeba S. Khan, Prof. R. R. Tuteja, Year – 2015
Description -The proposed algorithm is a Multilevel Encryption and Decryption algorithm. Only the authorized user can access the data. Even if some intruder gets the data, he must have to decrypt the data at each level which is a very difficult task without a valid key. It is time-consuming as multiple encryption and decryption take place. Secure data sharing using cryptography in a cloud environment [10]

Author - Anjali Patil, Nimisha Patel, Dr. Hiren Patel, Year – 2016
Description - In this paper, The system satisfies confidentiality, integrity, and authentication. Provides access control. The confidentiality of data is dependent on a trusted crypt server.

Data Security Issues are the main issue in the existing system. Due to the multi-tenant characteristics of the cloud, the previous security mechanisms are no longer suitable for data in the cloud. Some of the problem areas following:

[1] Due to the high scalability, service, and location transparency function of the cloud computing model, all kinds of servers and data of the cloud platform have no fixed infrastructure and security boundaries. In the event of a security breach, it is difficult to isolate a particular resource that has a threat or has been compromised.
[2] According to service models of Cloud computing, cloud services may be owned by many providers. As there is a conflict of interest, it is difficult to deploy a whole security measure.
[3] Due to the openness of the cloud and sharing virtualized resources by multitenant, user data may be accessed by other unauthorized users. The word cryptography means changing the message data into a scrambled code that can be retrieved back n the open network. The cryptography technique secures the sensitive information in unsecured transmission networks and which can be read by the intended recipient.

A cryptography algorithm needs a key along with a message of any format to form the ciphertext. 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. Further security can be improved using yet another Data hiding technique, Steganography.

In this proposed system AES, DES, algorithms are used to provide block-wise security to data for the user file security. Key information security is implemented by using the LSB steganography technique. The purpose of Key information is to decide the link between the available algorithm and key file encryption. By using this technique the file is fragmented into three parts and each part uses a unique algorithm technique. Multithreading is used to encrypt every part of the file simultaneously for improving the performance.

LSB technique is used to insert Data encryption Keys into the cover image. The valid user receives an email with Stego-Image of the key. The reverse process of encryption is applied for file decryption purposes. Symmetric key cryptography algorithms are AES, DES. These algorithms accomplished high-level security but taking more time for data encode and decode. Steganography hides the secret data existence into an envelope.

In this technique existence of data is not visible to users. The only valid receiver knows about the data's existence. Secret data of user hide into an image file. After adding text into the image file it looks like a normal image file. DES algorithm is probably used for text-encode and decode.

Three bit LSB technique used for image steganography. We can hide a huge amount of images using the LSB steganography technique. AES is a symmetric-key cryptography algorithm. It supports three types of keys. The 128-bit key requires 10 rounds, the 192-bit key requires 12 rounds and the 256-bit key requires 14 rounds. The advantage of the modified AES algorithm provides better performance in terms of delay.

The size of DES the key is 128 bit. In this algorithm, many formats are executed randomly so the user cannot even guess the steps of the algorithm. Provide high throughput is the advantage of cryptography algorithms.

Improved DES algorithm uses a 112-bit key size for data encode and decode. The key generation process is done using the random key generation technique. It provides security to data. The disadvantage of this algorithm is the essential maximum time for converting data into ciphertext because it operates on a single byte at a time.

IV. METHODOLOGY

The research process aims to detect cloud storage security using hybrid cryptography. In this scheme, there is the use of symmetric key cryptography and stenography techniques. This paper's content is highly focused on the security of files in the cloud. The data of the above algorithm is collected from google or another platform of a research paper. The above techniques and algorithms are a suitable method for protecting files from social platforms and the cloud.

V. MODELING AND ANALYSIS

The system overview is presented in this Section. Existing System Architecture

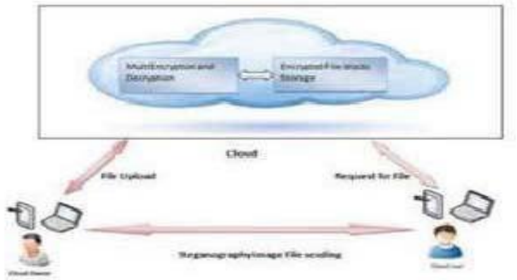

Figure 1 Existing system architecture[1]

The high-level architecture of the current secure file storage system is represented in Figure 1. The current system uses symmetric key cryptography and steganography techniques. Symmetric key algorithms like AES, blowfish, RC6 algorithms are used to provide block-wise security to data in the files. Each file is split into 8 blocks and every block is encrypted using a different algorithm. Using LSB steganography keys are inserted into cover images and then cover images are shared with the user via email. The existing system only focuses on confidentiality and does not consider integrity and authentication. Proposed System Architecture –

The main disadvantage of the current system is it does not consider integrity and authentication. Also, it uses stenography to share secret keys between users. To overcome these drawbacks we propose a system that provides integrity and authentication along with confidentiality. Also, our system uses asymmetric key cryptography rather than stenography to share secret keys among users. We plan to use asymmetric key cryptography over stenography as it would be better to use asymmetric key cryptography as our system is using a digital signature.

In our proposed system there are two main entities: an owner of the file and another with whom the owner has shared access. The owner will upload the file that is required to be stored at a remote location or needs to be shared with other users. The owner gives access to other users by sharing the required metadata to decrypt the file using an asymmetric cryptosystem.

A user with shared access can download the file from a remote storage and view the contents of the file.

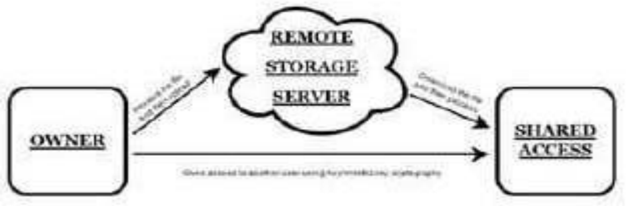

Figure 2 High level system

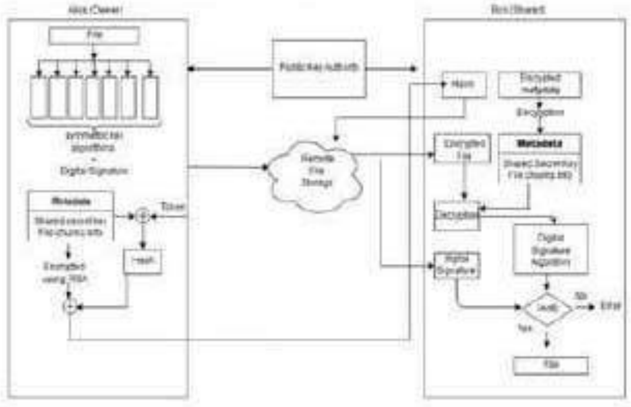

Figure 3 Purposed system architecture

In our proposed system there are four blocks each having different functionality.

- The file is divided into chunks and then every chunk is encrypted using the AES algorithm and a digital signature for the file is generated. A metadata file is created consisting of secret keys and information about file chunks.
- On the server, files are stored and a table is maintained to map hash codes with file names.
- A different server is maintained as a trusted center for the distribution of the public key.
- Lastly, there is a block for downloading the file. The file downloaded is decrypted then it's digital signature is verified before showing the file to the user.

VI. RESULTS AND DISCUSSION

The stored file is completely secured, as the file is being encrypted by using symmetric key cryptography and stenography techniques. The system is very secure and robust. Data of the users issecured on a cloud server which helps in avoiding unauthorized access from the outside world.. Data security is a major priority. This system can be implemented in the banking and corporate sectors to securely transfer confidential data.

VII. 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 these drawbacks a architecture is proposed which tries to provide a complete solution for securely storing the files.

ACKNOWLEDGEMENT

Special gratitude is conveyed to our prof. Swapna Augustine Nikale, Department of information technology of B. k. Birla College of Arts, Science & Commerce (Autonomous) Kalyan.

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., &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), 521–546. 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 ,TejasChoudhari , Anindita Bhajan , Madhu Nashipudimath 2020). Secure File Storage Using Hybrid Cryptography.2020 INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN TECHNOLOGY, 6(9).

[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 cloudenvironment”, 2016

[11]. Fortine Mata, Michael Kimwele, George Okeyo, “Enhanced Secure Data Storage in Cloud Computing Using Hybrid Cryptographic Techniques (AES and Blowfish