Securing File Storage on Cloud using Hybrid Cryptography

Cryptography Mini Project

Mohamed Ali Mohamed

Mostafa Mahmoud Mostafa

Ahmed Mostafa Morad

Mohamed Hani Abou El-Ela

Supervisor: Dr. Sahar Abd El-Rahman

Department of Computer Systems Engineering

Faculty of Engineering - Shoubra

Benha University

2021/2022

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

Abstract

Cloud computing is used in many areas like industry and military for storing huge amounts of data. We may face some security threats like Man-in-the-Middle (MITM) attacks and security breaches. To overcome these threats, we encrypt the traffic between the client and cloud server and do not store the decryption key on the cloud. Using a single algorithm in the encryption process is not sufficient for high level security of data in cloud computing. Therefore, we introduce a security solution using hybrid cryptography algorithms and steganography to achieve data integrity, security, confidentiality. We use public key cryptosystem (PKC) for key exchange processes between the user and the cloud server and symmetric cryptosystem for file encryption and decryption. Finally, the decryption key has to be saved securely, so steganography is used to hide the key and then send the carrier file that contains the decryption key to the receiver through email. For the decryption process the reverse process of encryption is applied.

***Keywords*—** Security, Cryptography, Stegnography, Hybrid Cryptography, Cloud

Chapter 1

Introduction

1.1 Report Objective

In this report we provide a solution for the problem of security breaches and attacks that may occur during uploading and storing data on the cloud. This solution combines both symmetric and asymmetric cryptography and steganography to achieve data integrity, security, confidentiality.

1.2 Background

Nowadays most people are very interested in sending and receiving data through internet and mobile data storage devices. Although this data usually contains personal information, a great number of them do not encrypt their data therefore the chances of data lose, or hacking are very high. The importance of Information security has become in continuous growth in all aspects of life. As long as technology continues to control various operations in our day-to-day life, this increases the need for information security. When the medium of information transmission is susceptible to interception, we use cryptography to provide a layer of security through translating messages into a form that cannot be understood by an unauthorized user or third party. An efficient solution for storing data in a secure form, is cloud storage where data is stored a on Internet-connected servers instead of local hard drives. These servers are managed by data centers to keep the data safe and secure to access. Cloud-based internet security is efficient solution for storing data. While data moves between your local device and the cloud provider, encryption in transit is used to protect your data if the communication are interpreted by a malicious actor. This protection is achieved through encrypting the data before transmission using symmetric cryptosystem and using public key cryptosystem (PKC) for key exchange processes between the user and the cloud.

1.3 Litrature Review

1.3.1 Cloud Computing

The cloud" refers to servers which are accessed over the Internet, and the software programs and databases that run on those servers. Cloud servers are placed in data centers all over the world. Through cloud, customers and companies do not have to manipulate physical servers themselves or run software applications on their own machines. Users can access the same files and applications from almost any device through the cloud because the computing and storage occur on servers in a data center, instead of local devices of the users. Switching to cloud computing gits rid of some IT costs and overhead for businesses. for example, businesses no longer need to update and maintain their own servers because the

cloud vendor, with who they are subscribed, will do that. Small businesses that may not have been able to afford their own internal infrastructure can now deploy their infrastructure on the cloud with low cost. Another benefit of the cloud for companies is that it makes it easier for them to operate internationally, because employees and customers can access the same files and applications from any location.

1.3.2 Cryptography

Cryptography or Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography [1]. Modern cryptography involves the study of mathematical techniques for securing digital information, systems, and distributed computations against adversarial attacks [6].

- **Symmetric-key cryptography:** refers to the methods in which both the sender and receiver use the same key for encryption and decryption. Symmetric key ciphers are implemented as either block ciphers or stream ciphers [1]. In a block cipher, the plaintext is divided into fixed-sized chunks called blocks. A block is specified to be a bit string (i.e., a string of 0's and 1's) of some fixed length (e.g., 64 or 128 bits). A block cipher will encrypt (or decrypt) one block at a time. The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are examples of block cipher algorithms. In contrast, a stream cipher first uses the key to construct a keystream, which is a bit string that has exactly the same length as the plaintext (the plaintext is a bitstring of arbitrary length). The encryption operation constructs the ciphertext as the exclusive-or of the plaintext and the key stream. Decryption is accomplished by computing the exclusive-or of the ciphertext and the key stream [7]. There are many symmetric-key algorithms such as. RC4 is an example of stream cipher algorithms.
- **Asymmetric-key cryptography:** which is called public-key cryptography refers to the methods in which the sender and receiver use two different but mathematically related keys for encryption and decryption. These two keys are called public key, which is used for encryption, and private key, which is used for decryption. A Public key is known for everyone, whereas a private key is known only for the recipient of the encrypted message. Asymmetric-key cryptography is a modern cryptography technique that is more secure and robust than symmetric cryptography, but it is slower than symmetric cryptography requires high consumption of resources and used to encrypt small amount of data [3]. There are many asymmetric-key algorithms such as Diffie–Hellman, RSA, elliptic curve and ElGamal encryption
- **Hybrid cryptography:** is to combine symmetric and asymmetric cryptography together to benefit from the strengths of each cryptosystem. Hybrid cryptography (almost) achieves the efficiency because it uses the slow asymmetric cryptosystem to encrypt the short secret key and the symmetric cryptosystem to encrypt the longer plaintext [7].

1.3.3 Stegnography

Steganography is the practice of concealing a message within another message or a physical object [2]. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. The content to be concealed through steganography is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream [8]. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program, or protocol. The ideal form for steganographic transmission is media files because they have a large size. For example, a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone

who is not specifically looking for it is unlikely to notice the change [2].
Steganography comes in five types, text steganography, audio steganography, video steganography, image steganography and network steganography [5]. Hiding data within an image is called image steganography. It depends on two images, the first is called the cover image in which we hide the data, and the other is called the stego image, it is the image that is obtained after steganography. To embed a message in an image you need to alter the values of some pixels which are chosen by an encryption algorithm. To extract the message, the recipient of the stego image must be aware of the same algorithm to know the which pixel he must select to extract the message [4].

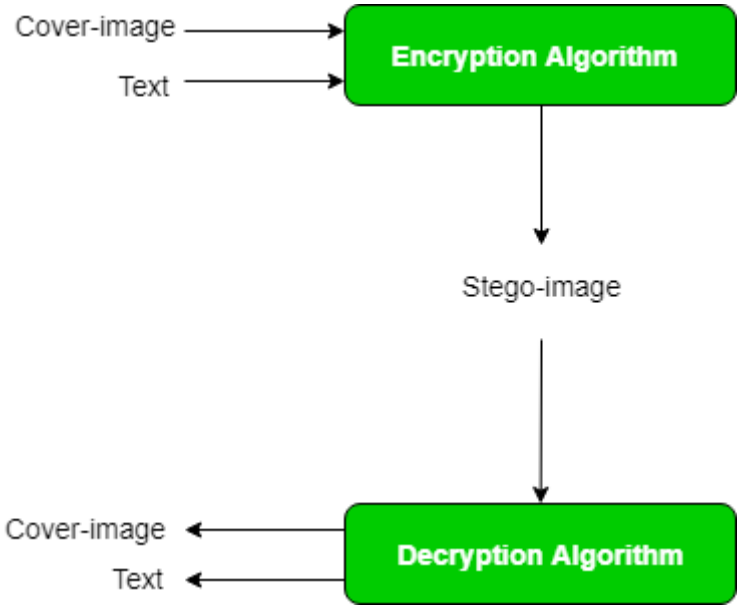

Figure 1.1: Stegnography [4].

1.4 Project Scope

We will implement a hybrid cryptography solution using symmetric and asymmetric cryptography algorisms that allow the users to upload and download their files from cloud in an encrypted form for backing up purposes and storing the data securely. Finally, we will use steganography to send the decryption key to the user in a hidden form.

1.5 Project Objectives

- Using cloud storage for storing data in a secure form
- Achieve the secrecy of data during sending to the cloud using hybrid cryptography algorithms
- Analyze the implementation of hybrid cryptography and its relation to securing file storage on the cloud storage
- Send the decryption key to the user in in a hidden form

1.6 Proposed Solution

We propose a solution to achieve the secrecy of the data during uploading to and downloading from the cloud then saving the decryption key secure through steganography.

Bibliography

[1] Cryptography. https://en.wikipedia.org/wiki/Cryptography. Accessed: March 2022.

[2] Stegnography. https://en.wikipedia.org/wiki/Steganography. Accessed: March 2022.

[3] Symmetric vs. asymmetric encryption. https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. Accessed: March 2022.

[4] Image stegnography. https://www.geeksforgeeks.org/image-steganography-in-cryptography/, 2021. Accessed: March 2022.

[5] Stegnography. https://www.simplilearn.com/what-is-steganography-article, 2022. Accessed: March 2022.

[6] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2020.

[7] James S Kraft and Lawrence C Washington. *An introduction to number theory with cryptography*. Chapman and Hall/CRC, 2018.

[8] Casey Clark Margie Semilof. Stegnography. https://www.techtarget.com/searchsecurity/definition/steganography. Accessed: March 2022.