Epitome Journals
International Journal of Multidisciplinary Research
ISSN : 2395-6968 | Impact Factor = 0.565

Crypto-Steganography :
An Information Security Tool for a Cloud Environment

Mrs. Aparna G. Korde
Department of Computer Science
AKI's Poona College of Arts, Science & Commerce
Camp, Pune-1 (India)
Email ID : apkorde@gmail.com

Abstract :

With the rapid development of cloud technologies, more and more multimedia data (text, video, image, sound) are generated and transmitted in the medical, education, commercial, military and other private sectors, public communications, which may include some sensitive information, which should be secure. The communication media through which we send data does not provide data security, so other methods of securing data are required. Therefore, security and privacy has become an important thing. Over the last few years, several security algorithms have been proposed, applied and tested in the literature with their strengths and weaknesses. This paper states the technique that exists for information hiding and how these can be combined to provide another level of security.

Keywords : *Security, Steganography, Crypto-Steganography, Intruders, Sensitive Information*

Research Paper :

Introduction :

Information hiding has been since long time. In past, people used hidden pictures or invisible ink to convey secret information. Any attacks on information hiding means, violated the confidentiality and integrity of the message passed. Providing intended access and avoiding unintended access is a very challenging task.

The two important aspects of security that deal with transmitting information or data over some medium like cloud are steganography and cryptography. Steganography deals with hiding the presence of a message and cryptography deals with hiding the contents of a message. Both of them are used to ensure security. However, none of them can simply fulfill the basic requirements of security. So a new method based on the combination of both cryptography and steganography known as Crypto-Steganography, which overcomes each other's weaknesses and makes difficult for the intruders to attack or steal sensitive information is being proposed.

Cloud Computing:

CC is a pay-per-use model for enabling available, convenient, on demand network access to a shared pool of configurable computing resources like networks, servers, storage, applications, services etc., that can be rapidly provisioned and released with minimal management effort or service provider interaction. Key characteristics of cloud computing includes: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [4]. Cloud computing is available over the internet to share data, applications and hardware. Cloud computing provides unlimited infrastructure to store data and execute the applications. The customers do not need to own the infrastructure. One of the main problems with cloud-based computing services, is that the uncertainty about the level of information security offered by these services. In the clouds, data is sent to and processed in the environment that is not under the user or data owner control. Therefore, it could potentially be compromised either by clouds insiders or by other users sharing the same resource. Policies and security requirements must be bound to the data. To enforce these policies, the corresponding security mechanisms should be in place [2].

Basics of Cryptography:

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. A process called ‘Encryption’ mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage. The main goal of cryptography is keeping data secure form unauthorized attackers. The reverse of encryption is called ‘Decryption’, which recovers the original data. Since cryptography first known usage in ancient Egypt, it has passed through different stages and was affected by any major event that affected the way people handled information.

The original data that to be transmitted or stored is called plaintext, the one that can be readable and understandable either by a person or by a computer. Whereas the converted data so-called cipher text, which is unreadable, neither human nor machine can properly process it until it is decrypted. A system or product that provides encryption and decryption is called cryptosystem. Cryptosystem uses an encryption algorithms which determines how simple or complex the encryption process will be, the necessary software component, and the key (usually a long string of bits), which works with the algorithm to encrypt and decrypt the data. Kerchhoff theory gave the encryption algorithm are supposed to be known to the opponents. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. The security level of an encryption algorithm is measured by the size of its key space and its secrecy. The larger size of the key space is, the more time the attacker needs to do the exhaustive search of the key space, and thus the higher the security level is. The strength of the encryption algorithm relies on the secrecy of the key, length of the key, the initialization vector, and how they all work together. Depending on the algorithm and length of the key, the strength of encryption can be considered.

There are two encryption/decryption key types : In some of encryption technologies when two end points need to communicate with one another via encryption, they must use the same algorithm, and in the most of the time the same key, and in other encryption technologies, they must use different but related keys for encryption and decryption purposes. Cryptography algorithms are either symmetric algorithms, which use symmetric keys (also called secret keys), or asymmetric algorithms, which use asymmetric keys (also called public and private keys).

Algorithm works as follows:

Sender	Receiver
1. Start	1. Start
2. Enter secrete message	2. Get the cipher text
3. Enter encryption key	3. Enter decryption key
4. Save cipher text and send.	4. Save secrete message
5. Stop.	5. Stop.

Basics of Steganography:

Steganography is a Greek word, which means concealed writing. The word *stegano* means covered and *graphia* means writing. Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. However, today's most of the people transmit the data in the form of text, images, video and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as cover sources to hide the data.[3]

Some terms used in steganography are:

1. Secrete message: The data to be hidden or to be extracted.
2. Cover Image: The medium in which information is to be hidden. It may be an audio, video, image or a text file.
3. Stego-key: It's a secret value, which helps in encoding or extraction of data, without which data cannot be encoded and extracted.
4. Stego-image: A medium within which information is hidden.

Sender	Receiver
1. Start	1. Start
2. Enter secrete message	2. Getstego-image
3. Select cover-image	3. Enter stego-key
4 Enter stego-key	4. If key is matched?
5. Save stego-image	5. Yes, decrypt the message.
6. Hide secrete message and send no, go to step	
7. Stop.	6. Save the secrete message.
	7. Stop.

Crypto- Steganography:

Steganography can protect data by hiding it in a cover object but using it alone may not guarantee total protection. Thus, the use of encryption in steganography can lead to 'security in depth'.

Steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium. The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes" [3]. It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information streams, determine whether they have hidden messages encoded into them or not, and if possible, recover the hidden information. The cryptanalysis is the process of encrypted messages can sometimes be called as code breaking, although modern cryptography techniques are virtually unbreakable[6].

Based on the findings in the existing papers studied, a new algorithm is being proposed that can ensure all of the security principles i.e. robustness, confidentiality, authentication, integrity and non-repudiation and that would also satisfy the requirements of steganography i.e. capacity, undetectability and robustness. The algorithm, which will be implemented in a proposed system at a later stage of this research work, consists of four layers. Various steps involved in the algorithm are as follows:[7]

Sender	Receiver
1. Start.	1. Start.
2. Enter username and password to login.	2. Login by username and password.
3. Enter secrete message.	3. Get the stego-image.
4. Get digitally signed secrete message by cloud provider.	4. Enter the stego-key. 5. If key matched?
5. Apply encryption alg. On this digitally signed message and form an encrypted message	6. Yes, get cipher-text. 7. Apply the decryption alg.

and get the secrete message.

6. Select an image to embed the encrypted message into this image using any steganography alg. to produce stego-image.
7. Send the stego-image and send.
8. Stop.

8. Stop.

Each step is used to achieve one security principle like step-2 implements authorization, step-4 implements authentication, integrity and non-repudiation, step-5 implements confidentiality and partial security, step-6 implements robustness. Each step defined is unperceivable for an attacker.

Future work :

Nowadays, the communication is the prime necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. Cloud is a fantastic enabler when it comes to resource centralization and allows remote resources to come together under one environment and data becomes correspondingly “denser”. The proposed algorithm can be implemented in a security system as a future research work that would probably excel in comparison to the existing algorithms. The system would be tested based on various test cases and the results would be compared with those of existing algorithm. Achieving an efficiency, flexibility and security is a challenge of researchers.

Conclusion :

In this paper, a very comprehensive review of the conventional approaches and techniques used in the security of transmitted data over the cloud has been given. The survey has been carried out related to both steganography and cryptography that ensures security but lacks in some way or the other as far as their individual capabilities related to coverage of all the security principles are concerned. So, in order to overcome the lack of coverage of all the principles of security in those algorithms, a new algorithm has been proposed that would satisfy all the basic principles of security. This study will be helpful for the security challenges that the people face in the usage and implementation of cloud computing.

References :

1. International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 5– Mar 2014 ISSN: 2231-2803 http://www.ijcttjournal.org Page260 Importance and Techniques of Information Hiding : A Review Richa Gupta1 , Sunny Gupta2 , Anuradha Singhal3 13(Department of Computer Science, University of Delhi, India) 2 (University of Delhi, India)
2. European Scientific Journal August 2014 edition vol.10, No.24 ISSN: 1857 – 7881 e - ISSN 1857- 7431 'DEVELOPING SECURED INTEROPERABLE CLOUD COMPUTING SERVICES Al'-Khanjari, Z. Alani, A.
3. International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume – 3, Issue – 5) May 2014'Steganography Techniques– A Review Paper' Jasleen Kour Deepankar Verma.
4. http://www.epitomejournals.com, Vol. 2, Issue 2, February 2016, ISSN: 2395-6968, Epitome Journal, A Solution to Cloud Security: Image Steganography, Aparna G. Korde
5. International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010, 1793-8201An Overview of Video Encryption Techniques M. Abomhara, Omar Zakaria, Othman O. Khalifa
6. International Journal of Engineering Trends and Technology- Volume3Issue3- 2012 ISSN: 2231-5381 'Image Security Using Steganography And Cryptographic Techniques' R.Nivedhitha1, Dr.T.Meyyappan.
7. *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014* 149 | Page www.ijacsa.thesai.org A Crypto-Steganography: A Survey Md. Khalid Imam Rahmani1

Kamiya Arora, Naina Pal.