HIERARCHY BASED SECURED FILE SHARING

Akshaya Ganesan Iyer,Harshali Poojary,Nupur Sonve,Sneha Annappanavar

Student,student,student,student,Assistant Professor

Department of Computer Engineering

Vidyalankar Institute of Technology,Mumbai,India

Abstract: As technology is advancing exponentially, anyone is able to access confidential data if it is not secured properly. To protect the data which the administrator does not want to share or needs the data to be confidential we use AES encryption method where the user requires a public key to decrypt the encrypted data. Hence enhancing the security of Hierarchical based access control model. The admin would be able to upload/delete files from the application, declare the visibility of the file and also change the password if needed. There are two hierarchy in case of the visibility. One is partially visible, which the admin is willing to share with multiple users. Each of such user will be given a partial access (i.e. only selected files would be visible) provided they have the password for it. The admin will have a separate password which will provide him with full access to files and enable him to perform the functions mentioned above.

IndexTerms**: Encryption, File security, Visibility, Key, Password, AES.**

I. Introduction

An access control is a mechanism in which a system grants or revokes the right to access some data or to perform some action. Information must be made secure from internal as well as from external security threats. A large portion of threats comes from the organization internally. An access control is a security parameter enforced against internal security threats. The concept of Hierarchy based access control is the level which can demonstrate the access control policy for a particular organization, institution or enterprise. Permissions are created when actions are applied to objects and then these permissions are assigned to these levels. Hierarchy based access control has various features like tight security, robust access control facility and it provides ease of management for the administrator as well.

Development of information technology brings us convenience and efficiency together with new challenges on information security. Only by ensuring the security of information transmission, can people make better use of information services.

File encryption, as a basic means of protection, is forced on the outside the system memory to the computer data, especially on the theft of data and destructive activities. When file encrypted, even if the key documents leaked or lost, they can hardly be deciphered, thus greatly increased the security of key documents. On the other hand, file encryption can be set to each user (or user group) by the user's own key encryption, even when sharing the computer, other people cannot decrypt properly and get the access to plaintext because they do not know the key, thus ensured the security of personal documents. In addition, through encryption, backup file has become a ciphertext so that it can reduce losses caused by heft or loss of backup media. There are many secure file system has been achieved both at home and abroad, but generally lack of security key management functions, or exist security vulnerability of the key management. In the way, it reduces the system security.

Cryptography is the term for information security by rearranging information in an unreadable manner. Cryptography is mainly derived from two Greek words: kryptos meaning “hidden secret” and graphein meaning “writing”. The technique to convert a message into an unreadable or random form is called encryption. The technique to convert a random text (encrypted text) back to its original form is known as decryption. The files are encrypted into ciphertext with a cryptographic algorithm, which will, in turn, be decrypted into usable plaintext. A single key is used for encryption and decryption in any symmetric cryptography algorithm e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES).In the asymmetric algorithm, different keys are used to encrypt and decrypt the data. AES is widely used in electronic e-commerce protocols.

II. Literature Survey

2.1 Risks in File Sharing Technology

2.1.1 Chances of Installing Malicious code

When file sharing applications are used, it is difficult to verify that the source of the files is a genuine one. Attackers often use such applications to transmit malicious code. By doing so, they may also bring along viruses, Trojan horses, spywares or worms into the files. Downloading such files may infect your device.

2.1.2 Personal or sensitive information exposure

In such activities (File sharing) you may be giving other users access to personal information. This might happen as certain directories are given access to or because you share information to what you believe to be a trusted person or organization. Unauthorized sensitive corporate information, financial or medical data, or other personal information. It's difficult to know how many people have accessed the information once it has been exposed. The risk of identity theft significantly goes up with such availability of information.

2.1.3 Susceptibility to attack

A few of these applications may ask to open certain ports on your firewall to transmit the files. However, doing so might give attackers access to your computer or enable them to attack your device by taking advantage of any vulnerabilities that may exist.

2.1.4 Denial of service

Downloading files without an overlook might cause a significant amount of network traffic. This may bring down the availability of specific programs on your device or may limit your access to the internet.

2.1.5 Prosecution

Files shared through such applications may include copyrighted material, pirated software, or pornography. Even if unknowingly downloaded, you might have to face fines or other legal action.

2.2 Current steps advised to be taken to minimize the risk

2.2.1 Maintain and use anti-virus software

Anti-virus software protects and recognizes your device against most known viruses. However, new viruses are written by attackers continually, so keeping your anti-virus software current is important.

2.2.2 Firewall

Some types of infection can be prevented by firewalls. This is done by blocking malicious traffic before it can enters your device. A firewall is present in some operating systems. We need to make sure that it is enabled.

III. Advanced Encryption Standard (AES)

One of the widely adopted Centro symmetric secret writing algorithmic program seemingly to be encountered today is the Advanced Encryption Standard (AES).It is found to be at least six times quicker than triple DES.A replacement for DES was required as its key size was too little. With computing power increasing, the risk of exhaustive key search attack went up. Triple DES was designed to beat this disadvantage however it had been found slow.

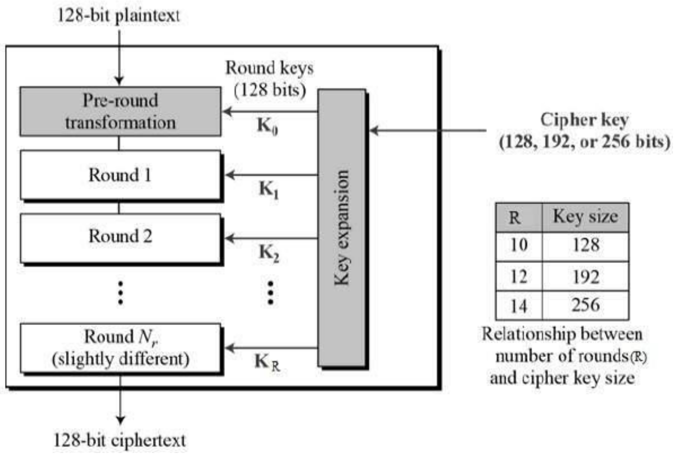
The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

3.1 Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It contains of a series of joined operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).The computations of AES takes place in bytes rather than the well anticipated bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes. These sixteen bytes are organized in four columns and 4 rows for process as a matrix. The length of the key determines the number of rounds in AES. This remains variable unlike DES.AES uses ten rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of those spherical uses a distinct 128-bit round key that is calculated from the initial AES key.

3.2 AES Structure



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

3.3 AES Analysis

Considering the recent times in cryptography, AES is supported and widely adopted in both software and hardware. Till now, there has been no practical cryptanalytic attacks against AES that has been observed. It also provides a built-in flexibility of key length. This brings in the aspect of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, AES security is assured only if it is implemented correctly and the key is managed well.

IV. Proposed Methodology

The goal is to find a method for secured sharing of files. To achieve this, the admin chooses which user will access which file. By doing so, users only get access to the files which admin knows are safe to share with the user. This thus eliminates the chances of unwanted file access as well as files from unknown resources.

4.1 Login/Registration of user or admin

As one installs this application, the application asks for the IP address of the server. This is done to establish a connection between devices and the server. The first step is to register. The user has to create an account on the application using details such as name, email address, phone number, password he would want to use while logging in etc. These details are stored in the database. The next time he opens the application he can directly login and open the files he has access to.

4.2 Uploading files for admin and selection of access

After logging in to the application, the admin can upload files he would like to share. After uploading the file, he can select users who would get access to that file and also set a password for accessing the file. This password is then converted into SHA and stored.

4.3 Encryption of file

Once the admin uploads the file to the application, the file is encrypted using AES algorithm. This is done by putting the file in a string, converting it into bytes and then applying the algorithm for encryption of the file.

4.4 Emailing the password to users who have access to that file

The file has been encrypted and stored. Now we need some kind of communication for letting the allowed users know the password to decrypt the file. This is done via email. The password the admin has set is sent to the user as an email. Using this, he can access the file.

4.5 Matching of password and decrypting the file

The user now access the file using the key, which is in the form of password he received. When the user selects the file from the list of files the admin has uploaded, the application asks him for the password. Then the password the user entered is matched with that of the password the admin created for that file. If the password matches, the file is decrypted and the user can now view the file. If the password entered is wrong, the user will be given only one more chance to enter the password (i.e. two tries). If the password entered is not valid after two tries, the user will be able to view the file in an encrypted form only.

V. Conclusion

This paper proposes a unique method for ensuring known access to files. It also talks about the various threat involved with files that comes from unknown resources. Here, the method to process and encrypt the file is detailed and information about how the file can be accessed by allowed users is also mentioned.

VI. Future Scope

In future, we can try to add more features to this application. In the current application, only the admin can upload files and select users who can access it. In the future, we can also allow users to upload files and select which fellow users will have an access to the same. However, the admin will have an overlook of files being uploaded. We can also track malicious activity by any of the user and stop providing him any access.

VII. Acknowledgement

For publishing, we required the guidance and help of many. We are very grateful for the support they have provided throughout. We would like to thank Dr. Arun Chavan, Head of the Department, Computer Engineering Department at Vidyalankar Institute of Technology for his useful suggestions. We would also like to express our gratitude towards Prof. Sneha Annappanavar for the valuable aid and guiding us through the process.

References

[1] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf, Jules Ehoussou, “Research on a normal file encryption and decryption”, International Conference on Computer and Management, 2011.

[2] Gang Hu, “Study of File Encryption and Decryption System using Security Key”, 2nd International Conference on Computer Engineering and Technology, 17 June 2010

[3] Wenhui Wang, Jing Han, Meina Song, Xiaohui Wang, “The Design of a Trust and Role Based Access Control Model in Cloud Computing” 6th International Conference on Pervasive Computing and Applications, 2011.

[4] Dhananjay M. Dumbere, Nitin J. Janwe, “Video Encryption Using AES Algorithm”, 2nd International Conference on Current Trends in Engineering and Technology(ICCTET), 2014.