Automated Encryption Technique to Store Data at Different Servers

Kirtish Tailor, Sharada Prasad Mishra, R. Brinda
Department of Computer Science
SRM University, Chennai, India

Abstract: Automated Encryption Technique is used to store the data by splitting and encrypting it with different algorithms. It provides strongly secured encryption algorithm to store data at different servers. The data is divided into number of data blocks. These data blocks or packets are encrypted by different algorithm such as AES, DES, RC4 etc. and for each packet a security key is generated. This encrypted data packets are stored in different servers. The location of the packet and key for each block is encrypted by master key and stored in the database.

Keyword: Data Encryption, Automated Encryption Standard (AES), RSA Key-Generation, Security, Data Storage, Cryptography.

I. INTRODUCTION

Storage of data on the internet has become a necessity for every individual in the electronic world. Thus data security is a major concern when a third party monitors the connection between the user and the service provider. Many organisations use segregated storage methods to store their data and important information. Thus cryptography is most commonly used to encrypt information for data confidentiality. It consist of two methods namely Encryption and Decryption. Encryption is the method which converts the original data or also known as plaintext to ciphertext, which is obtained by manipulation of plaintext in the restriction of defined protocols. The following are the criteria to keep in mind while choosing an encryption technique:

- Data confidentiality: The user data must remain confidential and any unauthorized party should not gain access to the information.
- Fine grained access tool: Each user must have different access rights to make the model much more reliable and efficient.
- Scalability: The system must work effectively even with an increase in number of users.
- User accountability: The user must be held accountable in case he/she shares any critical information with any unauthorized party.
- User revocation: Upon quitting the system the user rights are to be revoked and the access to the data is denied.
- User rejoin: The user must be able to join back hassle-free after revocation without disturbing the model.
- Ciphertext size: The size of the encrypted file after the plain text data file is encrypted.

Cryptography is majorly divided into two types depending on the type of key which is being used. One of them is Symmetric Key Cryptography in which only one key is used for encryption and decryption. Data encryption begins with segregation of data to either Stream Cipher or Block Cipher. Data is treated as many blocks arranged in certain manner. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two cryptographic standards by US government. These standards are used for encrypting the data sets using one secret key.

Public key cryptography uses two key for its cryptographic processes, one used for encryption and another is used for decryption. These keys have relation between them. RSA is the key generation technique for public key cryptography. The public key is used to encrypt the plaintext. Beside from the public key, it has one secret key which is used to decrypt back the data.

II. Literature Review

A. Existing System:

There are various encryption standards developed by computer scientist which is commonly used for encryption. Some of the standard are explained below:

- Data Encryption Standard (DES) is first encryption standard by US government. It is block cipher technique in which data is...
divided into blocks and these blocks are encrypted to ciphertext. It uses one secret key for encryption and decryption.

- Advanced Encryption Standard (AES) is also a block cipher technique developed by enhancing DES. It is symmetric key cryptographic technique which uses same key for encryption and decryption.
- RSA is cryptographic technique which uses two key in the cryptographic process. One key is used to encrypt and other to decrypt it.

B. Proposed System:

Proposed encryption technique uses several encryption algorithm at same time for encrypting a single data set. In this technique data is divided into several number of blocks or data packets, each data packet is encrypted by one unique encryption algorithm such AES,DES etc. ciphertext is stored in one of the servers. Likewise another packet is encrypted by other algorithm and stored in different server.

The data retrieval is done by bringing the ciphertext from the servers and decrypting each by its own decryption algorithm. All the decrypted text is arranged back to get the original text. It not only complexes decrypting data but also make it unreachable to hacker by storing different block at different servers.

There are three modules used to implement this technique which are following:
- Encryption Module
- Data Splitting and Algorithm Selection Module
- Data Retrieval Module

C. Advantages of Proposed System:

- Level of security can be varied depending on the number of servers installed.
- Multiple Encryption technique are used each time for every data set which make the system complex.
- The ciphertexts are stored at different servers for single data set.
- To retrieve the data completely one needs to decrypt ciphertext from all servers.

III. Encryption Module

This module will encrypt the data block with the specific algorithm and a random key. The Key is generated by RSA algorithm and its public key is used to encrypt the block and private key used to decrypt it. Each key is also stored in the database using location module.It uses any one of the following algorithm to encrypt its one of the packet:

A. Data Encryption Standard (DES):

It is symmetric key encryption technique which has only one key that is used for both encryption and decryption process. It is a block cipher technique, where each block goes through several rounds of operation and ciphertext is generated of that same fixed size. The size of the block is 64 bit and key is 56 bit.

B. Advanced Encryption Standard (AES):

It is an advanced encryption technique which is based on ‘Substitution and Permutation Network’. It is block cipher technique which has block size of 128 bits. These block are arranged in a matrix form.In this technique key size can be 128 bits or 192 bits or 256 bits. Each block goes through several operational rounds depending on the size of the key. Each round consist of some set of operations, that operation are performed on the block. Ciphertext obtained after encryption goes through back track sequence of round in order to get the original text or plaintext.

C. RSA Encryption Technique:

It is public key cryptographic technique which uses two key one is public and other is private. The public key is used to encrypt the data and private key is used to decrypt the data. Key generation is the main segment of the technique, public is first generated and then distributed over the network, it is used to encrypt the data.

RSA can be understood completely by the following example:

- Choose two prime numbers, let a = 3 and b = 11
- Compute range of the key which is the product of two prime numbers n = p * q = 33
- Compute φ(n) = (p - 1) * (q - 1) = 2 * 10 = 20
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime. Let e = 7
- Compute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (3, 33)
- The encryption of m = 2 is c = 2^7 % 33 = 29
- The decryption of c = 29 is m = 29^3 % 33 = 2
IV. Data Splitting and Algorithm Selection Module

Data is divided into three parts and each part or block is encrypted by one of the algorithm explained in Encryption Module. The data is divided on the basis of length, start to one third of its length will be treated as first block, from one third to two third as second block of data and remaining portion as third block. Each block is encrypted by one of the encryption algorithm and ciphertext is obtained from them. Ciphertext obtained from each block get stored in one of the servers.

Parameter responsible for splitting of data is not necessary to be only length. Data can be divided on the basis of size, pages, memory etc. Store each packet in the variable. Process this variable through sequence of the operation as defined in the encryption algorithm. The result obtained after all the operation is called ciphertext, store this variable value in the server. Likewise for each the ciphertext is generated and get store in one unique server.

This Module can understood by following block diagram:

V. Data Retrieval Module

This module is responsible for retrieval of data same as submitted by user. To retrieve the data back, ciphertext is obtained from servers. Each cipher block will be decrypted by its decryption algorithm and plaintext obtained from that will be stored in one data block. Likewise for each cipher block, one corresponding data block is generated by decrypting it. These data blocks will be appended together according to the Data Splitting module. The resulted appended data block is the original data, this data will be provided to user to download it.

This Module can understood by following block diagram:

VI. CONCLUSION

Storage of data on the internet has become a necessity for every individual for every individual in the electronic world. There are several Encryption standard developed for the security of data but it always less, everybody need more security of their data. The commonly used encryption technique can be easily identified by the hacker or intruder.

Keeping the data safe is become the priority for every individual. This Automated Encryption Technique will encrypt the data by many commonly used encryption technique which is more safer than any algorithm. Storage of the encrypted data (ciphertext) can be helpful in making the data more safe.

Data is divided several packets and each packet is encrypted by one commonly use encryption technique. Ciphertext for each block will stored in one server and ciphertext in another server. This make system more secure, in order to stole the data, intruder need hack all the server and get the ciphertext for all packet, by decrypting the following packet it need arrange back to defined manner in order to get the original data.
REFERENCES


