Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient and Secure Content Processing and Distribution by Cooperative Intermediaries

Pushpa B R
Lecturer, Department of Computer Science
Amrita Vishwa Vidyapeetham, Mysore Campus, Karnataka, India

Abstract—In the Centralized approach, one proxy can provide content service at a time to the client, which is less efficient. It must be overcome in order to support multiple proxies providing content services simultaneously. The proposed scheme is based on network security which provides the secure transmission of data over the network along with some content services provided by multiple intermediaries (proxies), The salient features of the proposed system Efficient, time is reduced, Confidentiality and integrity is ensured by using RSA.

Keywords— Network Security, RSA, Proxy and Asymmetric keys, Block Ciphers.

I. INTRODUCTION

In this paper "Efficient and secure content processing and distribution by cooperative intermediaries". The client make request of data from a data server. Besides the data it requests, it may also include some content service requirement. Data server is an entity that stores the data requested by a client. It has a group of cooperative intermediaries that can perform different content services. Dataserver maintains the information about the public keys of each cooperative proxy in an intermediary profile table. The data server will divide the requested file into segments, according to the content service requested by the client, it will send segment to a particular authorized proxy. Proxies are used to provide content services in response to requests by client. Intermediaries include logo adding, image filtering, text filtering, and virus scanning. After providing content service proxies will send segments to one main proxy (virus proxy) and this proxy merges the segments into a file and sends the requested file to client. The information security is provided by proxies, server intermediaries and client by making use of RSA public key algorithm to ensure confidentiality and integrity and they communicate through a secure channel.

II. OVERVIEW OF RSA CRYPTOSYSTEM

RSA is a widely used and well known algorithm in Cryptography. It can be used for user authentication, data encryption and digital data signing. It is a public key algorithm (i.e. two different keys are used to encrypt and decrypt the data). However these two keys are related. One of these two keys is used to encode (encrypt) the message on the sender side, another is used to decode (decrypt) the message on the receiver side. One of these two keys is usually kept secret, restricting access to it (private key) and another is public and can be known to everyone.

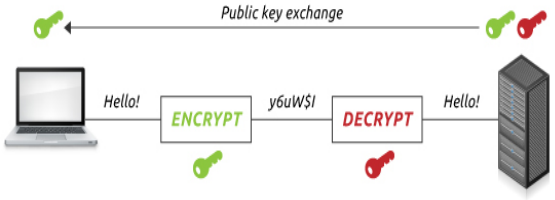


Fig. 1 The Block Diagram of RSA Cryptosystem

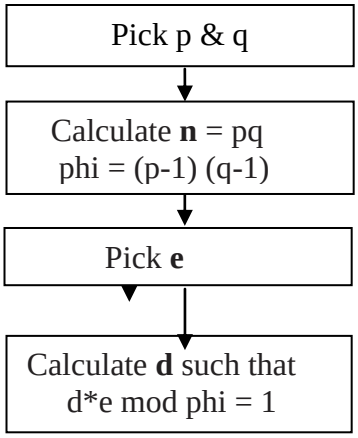
A. RSA key components

A public-key encryption scheme has six components

1) Plaintext::This is the readable message or data that is fed into the algorithm as input.
2) Encryption algorithm: The encryption algorithm performs various transformations on the\ plaintext.
3) Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
4) Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts.
5) Decryption algorithm: This algorithm accepts the cipher text and the matching key and produces the original plaintext. In RSA, the plaintext and the cipher text are considered as integers between 0and n-1, where n is

the modulus. The typical size of n is 1024 bits. However, the recommended length of n is 2048 bits as 640 bits key is no more secure by now.

The following are the steps involved in determining the public and private keys using the RSA algorithm



p,q - Are large randomly generated prime numbers.,n – One of the public keys. It is used as the modulus.phi – Or Φ(n) is used to find 'e'. phi is an Euler Totient ,e – Is the other public key. It should be relatively prime to phi.i.e. gcd(e, phi) = 1 d – Is the private key. It is relatively prime to phi and a multiplicative inverse of e. It is calculated using Extended Euclid's Algorithm. At this stage should discard p, q, and m values. Now we have the private key d, and the public keys e and n. If we want to encrypt text, we will need to first represent it in some numeric form (say P). Then apply the formula:

$$C = P^e \bmod n.$$ (Where C is the ciphertext)

To decrypt the ciphertext C to P, apply the formula:

$$P = C^d \bmod n$$ (Where P is the plaintext).

III. ROLE OF RSA AND PROXIES IN CONTENT PROCESSING

A. RSA

RSA algorithm is used to provide security to ensure confidentiality and integrity since it has different keys for encryption and decryption and the length of keys is so big(1024 bits) so that no one can factorize it. Because of this RSA is more secure compare to all other cryptographic primitives. It consists of four classes RSA, Encrypt, Decrypt and IO classes for implementing RSA Algorithm.

RSA: This class randomly generates the n and d values. Here 70001used as 'e' value to ensure that this number is relatively prime to phi.

Encrypt: This class helps to encrypt the data. Decrypt: This class helps to decrypt the data.

IO: This class facilitates opening and closing the necessary files and reading from them a line at a time.

The data security is ensured during the movement of the file or its segments between the modules until the process complete.Generates "p" and "q" values randomly by making use of the prime number 70001 which is taken as "e" value. RSA algorithm generates the public and private key. public key is sent to the server which it stores in one of the tables it maintains and sends it to proxies later. The public keys are used to encrypt the segments of the requested file.

B. Proxies

Proxy is a server that acts as a go-between for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. It acts as intermediaries between client and server. This proxies helps in secure transmission of data and also provide some content services according to the client request. The proxies are:

1) Logo adding: It will add date and time as a logo to the footer of the requested file.
2) Image filtering: It will filter the image which is present in the input file.
3) Text filtering: It will filter the extra commas present in the input file.
4) Virus scanning: Perform virus scan and merge the segments (default proxy).

Along with content service all these proxies helps in secure transmission of data this is done by using RSA algorithm for security purpose, each proxies public keys will stored in a profile table and it is maintained by server. Server send encrypted segments to the respective proxies and proxies will decrypt the segment, provide content service and again encrypt and send to one of the main proxy(virus proxy)and this proxy decrypt and merge the segments and do virus scan and again encrypt the file and send to the client.

IV. COMPARISON OF EXISTING AND PROPOSED SYSTEM

A. Centralized system(Existing system)

In the centralized system, the data server sequentially contacts each proxy to complete the requested content services. Once an intermediary has completed the operation, it sends back only the data that it has updated to the data server, and

the data server then prepares the data for the next proxy. Both the server and intermediaries use message digests to ensure data integrity, and they communicate through a secure channel. Once the data server receives the data from the last intermediary, it finally sends the data to the client. The centralized model has a star-shaped communication pattern, where the data server is at the center, and each proxy only communicates with the data server.

1) This approach is less efficient because only one proxy can provide content service at a time.
2) Overall content service time will increase because only one proxy can provide content service at a time.
3) Size of data will not be reduced, because of this large amount of bandwidth needed for data transmission.

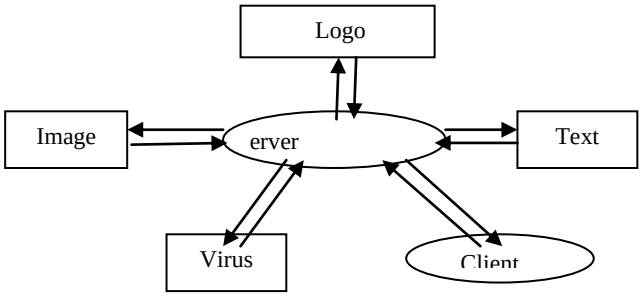


Fig. 2 The Block Diagram of centralised system

B. Parallelized system(Proposed system)

In parallelized system after the request from the client the data server will divide the requested file into segments, according to the content service requested by the client it will send particular segment to that particular authorized proxy and after providing content service proxies will send segments to one main proxy(virus proxy) and this particular proxy merge the segments in to a file and send the requested file to client it would not send again back to the data server like existing system. While transferring the information security is provided by proxies, server intermediaries and client use RSA public key algorithm to ensure confidentiality and integrity and they communicate through a secure channel.

1) This approach is more efficient because all the proxies will simultaneously provide content service at a time.
2) Overall content service time will reduced because all the proxies will simultaneously provide content service at a time.
3) Size of data will reduced since requested file will converted in to PDF file, because of this large amount of bandwidth needed for data transmission will reduced.

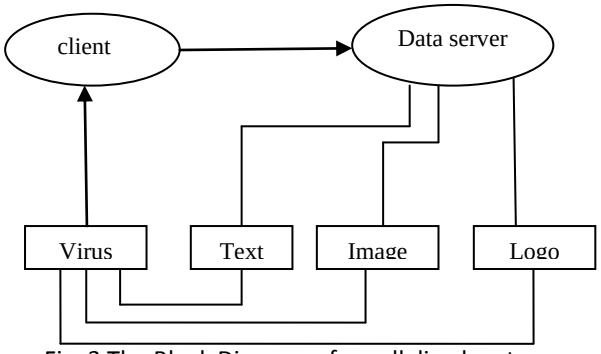


Fig. 3 The Block Diagram of parallelized system

V. REASONS FOR USE OF RSA

1) Supports Encryption and Digital Signatures.
2) Most widely used public key algorithm.
3) Gets its security from integer factorization problem.
4) Relatively easy to understand and implement.
5) RSA gets its security from factorization problem. Difficulty of factoring large numbers is the basis of security of RSA. Over 1000 bits long numbers are used.

VI. ROLE OF SERVER, CLIENT AND PROXIES IN CONTENT SERVICE SYSTEM

A. Dataserver

A frame is made to appear when the server program runs, where in a button called 'extract file' is provided to upload the files, the list of which is sent to any registered, requested client. It is made to register all proxies working on behalf of it, beginning with the antivirus proxy which is done by register proxy () method. When a client requests for the filelist from the server, the server takes the client information from the database, checks for valid client with the database and register the jdbc driver. This is implemented with the function Public Boolean CheckClient().The requested document file is segmented in to separate header, footer, Imagefile, textfile by the file segmentation program.

B. Intermediaries(proxies)

The proxies logo&imageproxy, textproxy are made to register with the server using registerproxy() method. These proxies get their respective segment from the dataserver and process them and send the processed segment to antivirus

proxy. During all these security is ensured using RSA encryption and decryption & content service like logo adding, text filtering, image filtering.It is registered with the server using the registerProxy() method. It gets segment from all other proxies, decrypts them merges them using the mergesegment class ,scans it and sends it to client by encrypting it.

C. Client module:

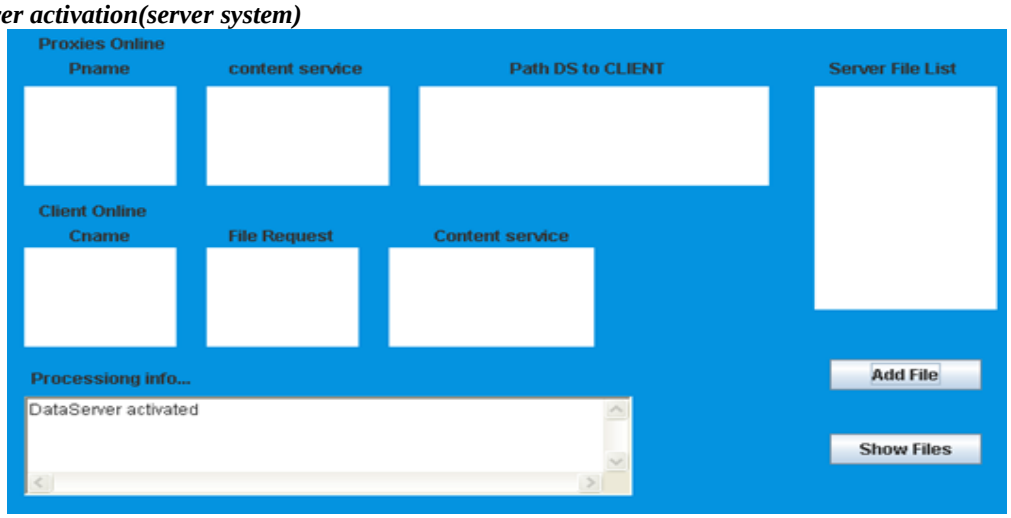
When the client program is run, a window is made to appear if it's a valid client wherein a button called ExtractFList is available. By clicking on it the list of files sent by server could be seen.One of these files should be entered in the EnterFile Name area. The services needed could be specified by checking the options provided. On clicking the download button, the file with the specified services on it gets downloaded.

D. RSA

This project consists of four classes RSA, Encrypt, Decrypt and IO classes for implementing RSA Algorithm. The below implementation is done in all the modules in our project namely client, server, logo &image proxy, text proxy and antivirusproxy. The data security is ensured during the movement of the file or its segments between the modules through the following implementation are done as explained below. First, the Antivirus proxy is registered. During which, the RSA algorithm in it generates the public and private key. This public key is sent to the server which it stores in one of the tables it maintains and sends it to other proxies later. Next, the other proxies are registered. Even here the RSA algorithm is used. During the registration, the proxies send their public key generated to the server and in turn gets the public key of the antivirus proxy. The public keys of all the proxies are used to encrypt the segments of the document meant for the respective proxies. The proxies then decrypt the segments they get and provide content service. The processed segments are encrypted using the pubic key of the Antivirus proxy which they got during the registration from server and send the encrypted ,processed segment to the antivirus proxy .The Antivirus proxy, then merges these segments ,scans and encrypts the merged file using the public key of the client .The client machine then decrypts this required file and renders it to the user.

VII. . SCREENSHOTS

*A. **Data Server activation(server system)***



B. Client registration(client system)

Requested file being downloaded along with services which is stored in D-drive of client system

VIII. CONCLUSION

The method proposed in this paper is simple and effective way for the text encryption and decryption. The simple key is used to encrypt and decrypt the file. This method is suitable for small amount of data. The proposed algorithm of symmetric encryption works better to encrypt and decrypt the file. the plain text is encrypted using key and again the same key is used for decrypting the file so that it provides better security.

REFERENCES

[1] S. William, Cryptography and Network Security:Principles and Practice, 2nd edition, Prentice-Hall, Inc.,1999.
[2] [2] S. Hebert, "A Brief History of Cryptography", an article available athttp://cybercrimes.net/aindex.htm

[3] Sumedha Kaushik1 "Network Security Using Cryptographic Techniques ", International Journal of Advanced Research in Computer Science and Software Engineering.
[4] Computer and Network security by ATUL KAHATE.

[5] Fundamentals of Computer Security, Springer publications -Basic Cryptographic Algorithms‖, an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoI ntro.htm#Algorithms
[6] http://library.thinkquest.org/27993/crypto/dig/block2.shtm.

