Journal of Management Engineering and Information Technology (JMEIT)
Volume -4, Issue- 6, Dec. 2017, ISSN: 2394 - 8124
Impact Factor : 4.564 (2015) | Index Copernicus - ICV 2016 = 51.4
Website: www.jmeit.com | E-mail: editorjmeit@outlook.com | jmeit@outlook.com

Development Of A Client / Server Cryptography-Based Secure Messaging System Using RSA Algorithm

Ferdi SÖNMEZ, Mohammed Khudhair Abbas

***Ferdi SÖNMEZ**,Computer Engineering Department, Istanbul Arel University, Turkey.,*
(e-mail: ferdisonmez@arel.edu.tr)
***Mohammed Khudhair Abbas ABBAS** , Computer Engineering Department, Istanbul Aydin University, Turkey*
e-mail:mkhudhairabbas@stu.aydin.edu.tr

Abstract— The efficiency and effectiveness of the information systems, in many ways, depend on its architecture and how data are transmited among different parties. Similarly, a very crucial aspect in the software development is the security of data that flows through open communication channels. One of the most popular architecture is client/server architecture that makes the centralization of data storage and processing enable, and provide flexibility for applying authentication methods and encryption algorithms within information systems. While the number of clients increase, its require increasing the authentication and encryption level as high as possible. Client/server is a technology that allows to open an interactive session between the user's browser and the server. In this study, we used client/server architecture to accomplish secure mesaging/chat between clients without the server being able to decrypt the message by applying two layer security: one layer of encryption between the clients and the server, and the second layer of encryption between the clients in the chat room. In this manner, a Client / Server Cryptography-Based Secure Messaging System using RSA (Rivest-Shamir-Adelman), which is a widely used public-key cryptograph and authentication system for data encryption of digital messaging transactions such as e-mail over the intranet, extranet and Internet, to encode and decode messages in a terminal window is developed.

Keywords—Authentication Methods, Encryption Algorithms, Secure Messaging, RSA

I. INTRODUCTION

In today's world, computer networking has become an integral part of life. There are many different networks available to share information between groups of devices through a shared communication medium [1]. They are mainly differentiated by the physical medium and protocol standards. Ethernet is a prime wired networking standard which is an obvious choice for many network applications due to reliability, efficiency, and speed. Ethernet standard is used in various application segments [1][2][3]. Figure 1 shows the Client/Server model architecture that has been used in most network systems and in this study specially.

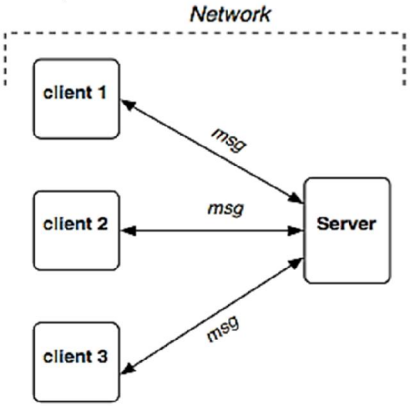

Figure 1: A Client/Server Architecture.

The client side could be any type of smart devices (desktop, laptop, smart phone, etc.). The server part is one device that control and pass messages and opining the connections among clients and/or between clients and server [4]. The Internet part could be one device to isolate the network overall into two main parts: client(s) and server, it could be a switch or hub or router or just a cable.

A very important aspect in the world of software development is the security of data that flows through open communication channels [3][5][6]. In our web applications, there is an intensive exchange of data via different protocols, like http, between client applications which presented as browser, mobile and desktop applications and server side applications. The importance and confidentiality of data may be different depending on the specifics of the web application, and the possibility of interception by a third party increases with perfection of hacking techniques in the world of IT [5][6]. What can be done to prevent access to the data by your traffic listener? If we exchange with data between the client applications and server we don't want the information to be stored as open text on the server, which will be accessible in case of server crack [3].

Every day people used chat area, through the users (clients) scan chat or send messages to selected users. However, the security components in chat area application are to make sure all information from clients is protected from hackers [4]. The chat messages from users can easily transform by expert hackers, without a good enough security components. In this way, a chat area interface (CAI) is required technique to secure a chat message from hackers. The cryptography is significant to keep private data secure and to avoid unauthorized access [7][8].

Journal of Management Engineering and Information Technology (JMEIT)
Volume -4, Issue- 6, Dec. 2017, ISSN: 2394 - 8124
Impact Factor : 4.564 (2015) | Index Copernicus - ICV 2016 = 51.4
Website: www.jmeit.com | **E-mail:** editorjmeit@outlook.com | jmeit@outlook.com

II: METHOD

Basically, the proposed messaging/chat system is expected to provide a communication channel between clients via a server using encryption based on RSA in a Client/Server environment [9][10]. The goal for this study is to use client/server architecture to accomplish secure chat between clients without the server being able to decrypt the message by using one layer of encryption between the clients and the server, and then a second layer of encryption between the clients in a chat room [10][11]. All the used encryption processes based on RSA algorithm. The implementation of this study is held in MATLAB environment.

The very term client-server was initially applied to the software architecture, which described the distribution of the execution process by the principle of interaction of two software processes, one of which in this model was called the client and the other the server. The client process requested some services, and the server process ensured their execution. It was assumed that one server process can serve a lot of client processes. One of the client/server application is that "chatting". Chatting alludes to one kind of correspondence over the Internet that offers a continuous transmission of instant messages from sender to beneficiary or over a server that is control and deal with the gatherings (customers) to convey.

A. Client/Server

The used client/server model describes how a server provides resources and services to one or more clients. Examples of servers including web servers, chat servers, and file servers [4][7]. Each of these servers provide resources to client devices. Most servers have a one-to-many relationship with clients, meaning a single server can provide resources to m Computers. In order to meet the main requirements of businesses, networks themselves are becoming quite complex multiple clients at one time [7].

B. Chat Service

A secure chat service provides the ability to have real time secure discussions among users electronically, one-to-one or in groups session [4][5]. A public network accumulates information slightly, rather than on a user's individual computer that is used to keep in touch with people. A secure chatting between client and server to make a safe and reliable communication, the benefits are [8][9]:

- Allows for instant communications between users.
- Uses real time chat over the network that can eliminate costly long distance charges.
- Allows for rapid query and rapid responses.

While the negative points of chat service can be listed as following [8][10]:

- Security problems of instant messaging program
- Secure chats in most cases are routed through a server system, where the service is provided and that is a single point where all messages can be intercepted.
- Chat programs can provide an open avenue of attack for hackers, crackers, spies and thieves.

C. RSA Encryption

In this study, an encrypted chat program designed to ensure a safe mode of communication between two users. It uses RSA encryption to encode and decode messages in a terminal window. RSA is widely used public-key cryptograph and authentication system for data encryption of digital messaging transactions such as e-mail over the intranet, extranet and Internet. Clients exchange public keys and encrypt outgoing text with the intended recipient's public key [7][9][10]. Each user connects to a central server which forwards messages to the intended recipient. On the receiving end, the program utilizes a client's private key to decrypt received messages. In 1977, Ron Rivest, Adi Shamir and Leonard Adleman introduced a cryptographic algorithm, RSA, which is named for the first letter in each of its inventors' last name [11]. RSA's motivation is Diffie-Hellman Algorithm which describes the idea of such an algorithm that enables public-key cryptosystem. Here are the steps of RSA Algorithm [10][11][12]:

- The first step of RSA Algorithm is to select two different prime number p and q.
- The second step is the calculation of n where N=p*q
- The calculation of φ(N)=(p-1)*(q-1) is the third step.
- As the fourth step, an integer e is selected as a public-key which is co-prime with φ(N)
- Finally, the inverse of e modulus φN) is taken to produce d, the private-key. By using e and d modulus N, the encryption and decryption are done.

In the RSA Algorithm, the public-key involves two numbers N and e while the private-key is N together with a different number d. To encrypt message M (plain text):

$$M \rightarrow Me(\text{mod } N)=C$$

To dencrypt message C (cipher text):

$$C \rightarrow Cd(\text{mod } N)=M$$

For the implementation of RSA, the number N is a product of two large prime numbers p and q [7][10]. If p and q are known then d can be obtained from e. As N is a part of the public-key and the multiplication of p and q then factorizing N to find p and q is possible [4][11]. Figure 2 shows the main components and processes for RSA algorithm.

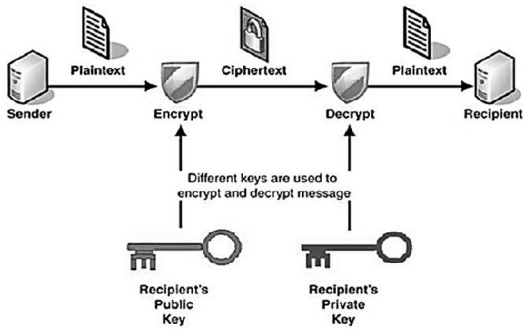

Figure 2: RSA algorithm main components and processes.

- RSA Key distributions

Each person or a party who desires to participate in communication using encryption and decryption operations [12][13]. Assume that Bob needs to send data to Alice. In the event that they choose to utilize RSA, Bob must know Alice's public key to encode the message and Alice must utilize her

Journal of Management Engineering and Information Technology (JMEIT)
Volume -4, Issue- 6, Dec. 2017, ISSN: 2394 - 8124
Impact Factor : 4.564 (2015) | Index Copernicus - ICV 2016 = 51.4
Website: www.jmeit.com | E-mail: editorjmeit@outlook.com | jmeit@outlook.com

private key to unscramble the message. To empower Bob to send his encoded messages, Alice transmits her open key (n, e) to Bob through a dependable, yet not really mystery, course. Alice's private key (d) is never dispersed.

- Encryption

After Bob acquires Alice's public key, he can send a message specific M to Alice. To do it, he initially turns M (entirely, the un-cushioned plaintext) into a whole number m (entirely, the cushioned plaintext), with the end goal that $0 \leq m < n$ by utilizing a settled upon reversible convention known as a cushioning plan [13][14]. He at that point processes the ciphertext c, utilizing Alice's public key e, corresponding to

$$c \equiv m^e \pmod{n}$$

This should be possible sensibly immediately, notwithstanding for 500-piece numbers, utilizing secluded exponentiation [14]. Weave at that point transmits c to Alice.

- Decryption

Alice can recuperate m from c by utilizing her private key type d by registering

$$c^d \equiv (m^e)^d \equiv m \pmod{n}$$

Given m, she can recuperate the first message M by turning around the cushioning plan.

III. PROPOSED SYSTEM

Encryption algorithm is deployed to encrypt messages exchanged with the proposed chat gateway. This study is about developing a new model to create private messaging network to transmit message contents over the network / intranet between client terminals. The chat messaging environment showed a great potential to host realtime interactive interaction system which is supported by RSA encryption methodology to preserve the security of the message stream [15][16].

Choosing the key size in RSA encryption is of great importance. As the size of the key increases, the security level of the system, the complexity and the resistance of encrypted text increases [15][17]. These advantages make it difficult to decrypt ciphertexts and break passwords. However, in addition to these advantages, the encryption key creation time, text encryption time, and mobile device RAM consumption increase [17][18]. These disadvantages are factors that will influence the effective use of the application. For this reason, the advantages and disadvantages of key dimensions should be determined and the most suitable key size should be preferred.

To accomplish the chatting and meet the goals of this study in client/server architecture, the need for authentication methods and encryption algorithms will be urgent [9][10][15][16]. RSA Algorithm for cryptography consists of three main stages: Key Generation Stage, Encryption Stage and Decryption Stage. Key Generation Stage is the process of generating keys for cryptography [19]. Keys, generated in this stage, are used to encrypt the plaintext in Encryption Stage and used to decrypt the cipher-text in Decryption Stage. Encryption Stage is the process of encoding messages in such a way that only authorized people can understand it [18]. By encryption, the message is converted into cipher-text. Decryption Stage is the process of decoding the cipher-text to get the original message. Theses three stages are followed both of the layers (first and second encryrption layers). The flowchart of the secure chat system is presented in Figure 3.

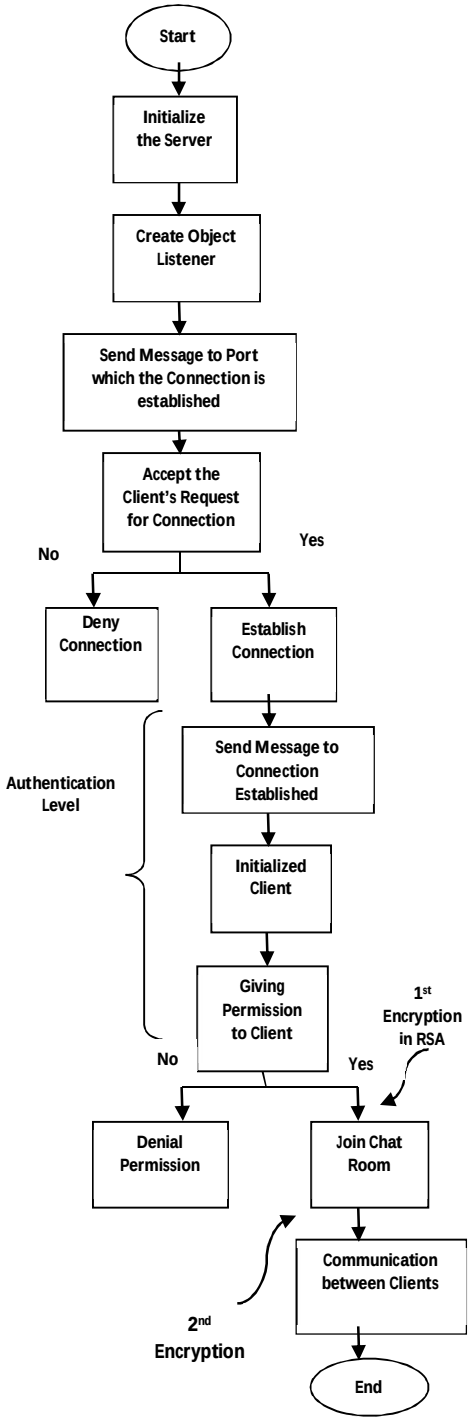

Figure 3: Flowchart of the proposed work.

Journal of Management Engineering and Information Technology (JMEIT)
Volume -4, Issue- 6, Dec. 2017, ISSN: 2394 - 8124
Impact Factor : 4.564 (2015) | Index Copernicus - ICV 2016 = 51.4
Website: www.jmeit.com | **E-mail:** editorjmeit@outlook.com | jmeit@outlook.com

Here, we used one authentication level and two encryption levels [17][19][20]. We used GUI in MATLAB to ask user for the server IP and the port that made the connection and the client ID and password [17][21][22]. We used RSA algorithm to encrypt messages between clients and the server as the first encryption level and then encrypt messages between clients and chat room [21]. By means of this model, secure messaging in corporational environments might be provided with the help of a two level authentication scheme.

IV. EXPERIMENTAL RESULTS

The results that we get after implementing the proposed chatlab system in Figure 3 will be followed figure by figure below (Figures 4, 5, 6, 7, 8).

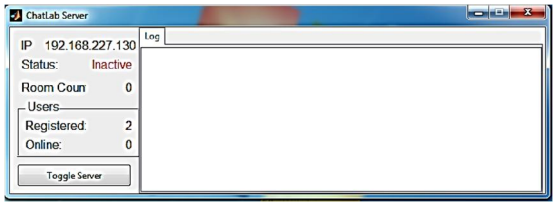

Figure 4: Starting the messaging environment.

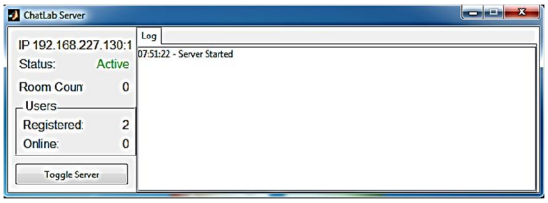

Figure 5: Initialize the server.

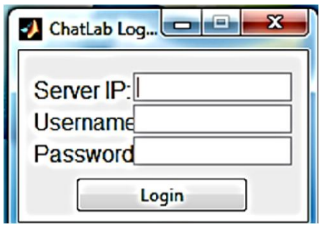

Figure 6: Authentication level.

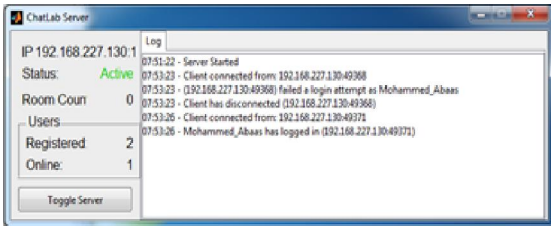

Figure 7: Initialize client(s).

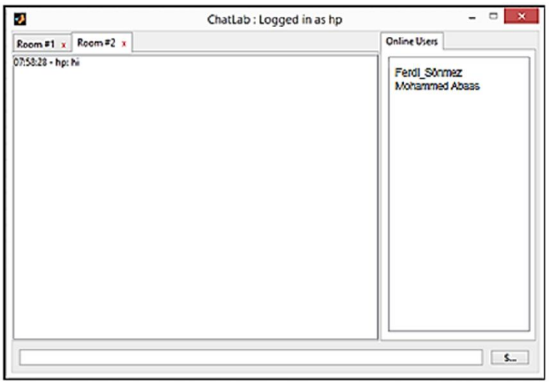

Figure 8: Secure messaging between two clients.

Since RSA cryptosystems use very large prime numbers, various algorithms have been developed to shorten both encryption and decryption time. To provide this, we considered the methods used to shorten the encryption and decryption time in 3 groups [24][25];

- Modular multiplication and exponentiation algorithms
- Fast RSA decryption algorithms
- Key management in RSA

Since the RSA cryptosystem needs to calculate both the encryption and the decryption process modal with very large numbers, the modularity of the computation algorithms has a big precaution for the acceleration of the RSA cryptosystem. Another way to reduce the length of encryption and decryption in the RSA cryptosystem is to use the generic and private key that is used in small selection [25]. But at the same time it is theoretically impossible to shorten both encryption and decryption keys.

V. CONCLUSIONS

Demonstrating of appropriate client/server applications is a basic figure for plannig, sending, and later adaptability. The demonstrating advances required in this exertion are not for the most part accessible, and not prepared for wide dispersion to application originators and organizers. This paper highlights the usefulness requirements for client/server models and depicts configuration inquiries to be tended to. A model reenactment demonstrates executed a large number of the prerequisites recorded, and its utilization was shown in a few genuine and speculative illustrations.

We developed a client/server encrypted chat based on RSA by using MATLAB software encryption polices. The result gave one authentication level and two encryption levels by secure chat data based on RSA algorithm. We have implemented the system in client/server architecture and in real-time network. We believe that the system prodvides high level in encryption and more flexibility in implementation. However, as a future work other encryption algorithms might be used and a hybrid algorithm can be developed for further purposes such as faster or wider messaging needs.

REFERENCES

[1.] Bibinagar, N., Kim, W. J. (2013). Switched Ethernet-based real-time networked control system with multiple-client–server architecture. *IEEE/ASME transactions on Mechatronics*, 18(1), pp.104-112.

[2.] Honda, K., Hu, R., Neykova, R., Chen, T. C., Demangeon, R., Deniélou, P. M., Yoshida, N. (2014). Structuring communication with session types. In *Concurrent Objects and Beyond*, pp. 105-127, Springer Berlin Heidelberg.

[3.] Lin, T., Zhou, K., Wang, S. (2013). Cloudlet–screen computing: a client–server architecture with top graphics performance. *International Journal of Ad Hoc and Ubiquitous Computing*, *13*(2), pp.96-108.

[4.] Iwamoto, M., Omino, T., Komano, Y., Ohta, K. A new model of Client-Server Communications under information theoretic security. In *Information Theory Workshop (ITW)*, pp. 511-515, 2014.

[5.] Chouhan, K., Ravi, S. (2013). Public Key Encryption Techniques Provide Extreme Secure Chat Environment. *International Journal of Scientific & Engineering Research*, 4(6), pp. 510-516.

[6.] Anjaneyulu, G.S.G.N., Reddy, U.M. (2012). Secured directed digital signature over non-commutative division semirings and Allocation of experimental registration number, *International Journal of Computer Science*, Vol. 9, Issue 5, No. 3, pp:376-386.

[7.] Desmet, L., Johns, M. (2014). Real-time communications security on the web. *IEEE Internet Computing*, *18*(6), pp.8-10.

[8.] David S. (2005), "Personal Encrypted Talk - Securing Instant Messaging with a Java Application", Rivier College Online Academic Journal, Vol. 1, No. 1, 2005.

[9.] Yusof M.K., Usop S.M., AmriAbidin A.F. Designing a Secure Architecture for Private Instant Messenger Application. *International Conference on Computer Science and Information Technology (ICCSIT'2011)*, 2011.

[10.] Jiangzhe Wang J, Peng C, Li C, Wakikawa R, Zhang L. Implementing instant messaging using named data. *Proceedings of the 6th Asian Internet Engineering Conference*, pp. 40–47, 2010.

[11.] Chandramouli, R., Iorga, M., Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In *Secure Cloud Computing* , pp. 1-30, Springer New York.

[12.] Joye M., Lepoint T. (2012). Partial key exposure on RSA with private exponents larger than N. In Mark D. Ryan, Ben Smyth, and Guilin Wang, editors, *Information Security Practice and Experience*, 7232, pp. 369–380. Springer Berlin Heidelberg.

[13.] Khanezaei, N., Hanapi, Z. M. A framework based on RSA and AES encryption algorithms for cloud computing services. In *Systems, Process and Control (ICSPC), 2014 IEEE Conference on*, pp. 58-62, 2014.

[14.] Stanisavljevic, Z., Stanisavljevic, J., Vuletic, P., Jovanovic, Z. (2014). COALA-System for visual representation of cryptography algorithms. *IEEE Transactions on Learning Technologies*, 7(2), pp. 178-190.

[15.] Ok, K., Coskun, V., Yarman, S. B., Cevikbas, C., Ozdenizci, B. (2016). SIMSec: A Key Exchange Protocol Between SIM Card and Service Provider. *Wireless Personal Communications*, 89(4), 1371-1390.

[16.] Vollala, S., Varadhan, V. V., Geetha, K., Ramasubramanian, N. (2017). Design of RSA processor for concurrent cryptographic transformations. *Microelectronics Journa*l, 63, pp.112-122.

[17.] Gupta, N., Saxena, A., Jain, N. (2016). Pairwise Independent Key Generation Algorithm: A Survey. *International Journal of Computer Applications*, 156(6), pp.12-18.

[18.] Jain, A., Kapoor, V. (2015). Secure Communication using RSA Algorithm for Network Environment. *International Journal of Computer Applications*, 118(7), pp.6-9.

[19.] Goshwe, N. Y. (2013). Data encryption and decryption using RSA Algorithm in a Network Environment. *International Journal of Computer Science and Network Security (IJCSNS)*, 13(7), pp.9-13.

[20.] Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. *International Journal of Computer Applications*, *67*(19), pp.33-38.

[21.] Rajanbabu, D. T., Raj, C. Implementing a reliable cryptography based security tool for communication networks. *In Science Engineering and Management Research (ICSEMR), 2014 International Conference on*, pp. 1-4, 2014.

[22.] Lent, C. S. (2013). *Learning to program with MATLAB: Building GUI tools*. John Wiley & Sons.

[23.] Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., Das, R. ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. In *Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual*, pp. 332-337, 2017.

[24.] Dhakar, R. S., Gupta, A. K., & Sharma, P. (2012, January). Modified RSA encryption algorithm (MREA). In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, pp. 426-429.

[25.] Genkin, D., Shamir, A., & Tromer, E. (2014, August). RSA key extraction via low-bandwidth acoustic cryptanalysis. In *International Cryptology Conference*, pp. 444-461, Springer, Berlin, Heidelberg.