International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S3, September 2019

A Secure Electronic Messaging System in Client Server Cryptography-RSA Algorithm

G. Geeta Sai Sruthi, M. Raghupathi

Abstract: ***The potency and effectiveness of the knowledge systems, in some ways, rely upon its design and the way knowledge area unit transmitted among totally different parties. Similarly, a really crucial side within the computer code development is that the security of knowledge that flows through open communication channels. one in all the foremost widespread design is client/server design that creates the centralization of knowledge storage and process modify, and supply flexibility for applying authentication strategies and coding algorithms inside info systems. whereas the amount of shoppers increase, its need increasing the authentication and coding level as high as potential. Client/server could be a technology that enables to open associate degree interactive session between the user's browser and also the server. during this study, we tend to used client/server design to accomplish secure messaging/chat between shoppers while not the server having the ability to decode the message by applying 2 layer security: one layer of coding between the shoppers and also the server, and also the second layer of coding between the shoppers within the chat space. during this manner, a shopper / Server Cryptography- based mostly Secure electronic messaging System mistreatment RSA (Rivest- Shamir-Adelman), that could be a wide used public-key cryptography and authentication system for encryption of digital electronic messaging transactions like e- mail over the computer network, extranet and net, to write in code and decipher messages in an exceedingly terminal window is developed.***

Keywords—Authentication Methods, Encryption Algorithms, Secure electronic messaging, RSA

I. INTRODUCTION

In today's world, pc networking has become integral a part of life. There are many alternative networks on the market to share info between teams of devices through a shared communication medium [1]. They're chiefly differentiated by the physical medium and protocol standards. Local area network could be a prime wired networking common place that is an evident alternative for several network applications because of reliability, efficiency, and speed. Local area network commonplace is employed in varied application segments [1][2][3]. Figure one shows the Client/Server model design that has been utilized in most network systems and during this study specially.

Manuscript published on 30 September 2019.
***** Correspondence Author (s)
G. Geeta Sai Sruthi, Assistant Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, India, Email id: saigeeta44@gmail.com
M. Raghupathi, Assistant Professor, Department of Computer Science and Engineering, MallaReddy Engineering College for Women, India, Email id: mraghu30@gmail.com

The client side may be any kind of sensible devices (desktop, laptop, sensible phone, etc.). The server half is one device that manage and pass messages and opining the connections among clients and/or between server [4]. The internet half may be one device to isolate the network overall into 2 main parts: client(s) and server, it may be a switch or hub or router or simply a cable.

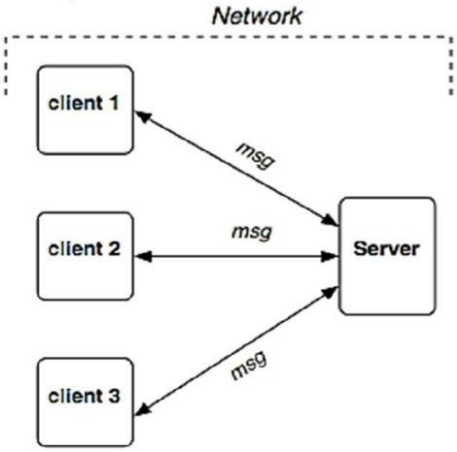

Figure 1: A Client/Server design.

A very necessary side within the world of computer code development is that the security of knowledge that flows through open communication channels [3][5][6]. In our net applications, there's intensive exchange of knowledge via totally different protocols, like http, between client applications that bestowed as browser, mobile and desktop applications and server facet applications. The importance and confidentiality of knowledge is also totally different depending on the specifics of the online application, and also the chance of interception by a 3rd party will increase with perfection of hacking techniques within the world of IT [5][6]. What will be done to stop access to the information by your traffic listener? If we tend to exchange with data between the client applications and server we tend to don't wish the knowledge to be hold on as open text on the server, which is able to be accessible just in case of server crack [3]. Every day folks used chat space, through the users (clients) scan chat or send messages to chose users. However, the safety elements in chat space application area unit to form certain all info from clients is shielded from hackers [4]. The chat messages from users will simply remodel by professional hackers, while not an honest enough security elements. During this manner, a talk space interface (CAI) is needed technique to secure a talk message from hackers. The cryptography is critical to stay personal knowledge secure and to avoid unauthorized access [7][8].

II. METHOD

Basically, the projected messaging/chat system is anticipated to supply a line 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 design to accomplish secure chat between clients while not the server having the ability to decode the message by mistreatment one layer of coding between the clients and also the server, so a second layer of coding between the clients in an exceedingly chat space [10][11]. All the used coding processes supported RSA algorithmic rule. The implementation of this study is command in MATLAB setting.

The terribly term client-server was at first applied to the computer code design, that represented the distribution of the execution method by the principle of interaction of 2 computer code processes, one in all that during this model was known as the client and also the alternative the server. The client method requested some services, and also the server method ensured their execution, it had been assumed that one server method will serve a great deal of client processes. one in all 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 cryptography 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 that the third step.
As the fourth step, associate degree number e is chosen as a public-key that is co-prime with φ(N)
Finally, the inverse of e modulus φN) is taken to supply d, the private-key. By using e and d modulus N, the coding and coding area unit done.
In the RSA algorithmic rule, the public-key involves 2 ranges N and e whereas the private-key is N in conjunction with a unique number d. To code message M (plain text):

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

To decrypt message C (cipher text): $C \rightarrow Cd(\text{mod } N)=M$

For the implementation of RSA, alphabetic N could be a product of 2 giant prime numbers p and q [7][10]. If p and Q area unit legendary then d will be obtained from e. As N could be a a part of the public-key and also the multiplication of p and Q then factorizing N to seek out p and Q is feasible [4][11]. Figure a pair of shows the most elements and processes for RSA algorithmic rule.

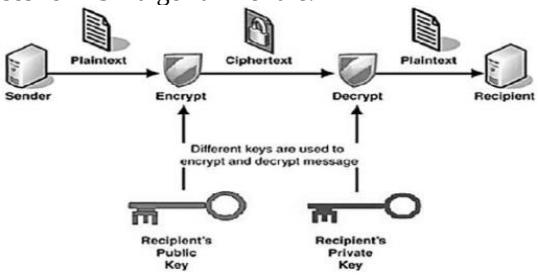

Figure 2: RSA algorithmic rule main elements and processes.

RSA Key Distributions

Each person who desires to participate in communication mistreatment using encryption and decryption operations [12][13]. Assume that Bob has to send knowledge to Alice. In the event that they prefer to utilize RSA, Bob should apprehend Alice's public key to write in code the message and Alice should utilize her private key to unscramble the message. To empower Bob to send his encoded messages,

Alice transmits her open key (n to Bob through a dependable, nonetheless not very mystery, course. Alice's personal key (d) isn't distributed.

Encryption

After Bob acquires Alice's public key, he will send a message specific M to Alice. To do it, he at first turns M (entirely, the un-cushioned plaintext) into a full range m (entirely, the padded plaintext), with the top goal that zero ≤ m < n by utilizing a settled upon reversible convention called a padding set up [13][14]. He at that time processes the cipher text c, utilizing Alice's public key e, comparable to

$c \equiv me \pmod n$

This should be potential reasonably straightaway, even so for 500-piece numbers, utilizing secluded mathematical operation [14]. Weave at that time transmits c to Alice.

Decryption

Alice will recuperate m from c by utilizing her personal key sort d by registering

$cd \equiv (me)d \equiv m \pmod n$

Given m, she will be able to recuperate the primary message M by turning round the padding set up.

III. PROPOSED SYSTEM

Encryption algorithmic rule is deployed to code messages changed with the projected chat entrance way. This study is concerning developing a brand new model to form personal electronic messaging network to transmit message contents over the network / computer network between client terminals. The chat electronic messaging setting showed a good potential to host real time interactive interaction system that is supported by RSA coding methodology to preserve the safety of the message stream [15][16].

Choosing the key size in RSA coding is of nice importance because the size of the key will increase, the safety level of the system, the quality and also the resistance of encrypted text will increase [15][17]. These blessings build it troublesome to decode cipher texts and break passwords. However, additionally to those advantages, the coding key creation time, text coding time, and mobile device RAM consumption increase[17][18]. These disadvantages area unit factors which will influence the effective use of the applying. For this reason, the benefits and drawbacks of key dimensions ought to be determined and also the best suited key size ought to be most popular.

To accomplish the chatting and meet the goals of this study in client/server design, the necessity for authentication strategies and coding algorithms are going to be imperative [9][10][15][16]. RSA algorithmic rule for cryptography consists of 3 main stages: Key Generation Stage, coding Stage and coding Stage. Key Generation Stage is that the method of generating keys for cryptography [19]. Keys, generated during this stage, area unit wont to code the plaintext in coding Stage and wont to decode the cipher-text in coding Stage. Coding (Encryption)Stage is that the method of coding messages in such the way that solely approved folks will know it [18]. By encryption, the message is reborn into cipher-text. coding Stage is that the method of decipherment the cipher-text to induce the initial message. These 3 stages area unit followed each of the layers (first and second encryption layers). The flow chart of the secure chat system is bestowed in Figure 3.

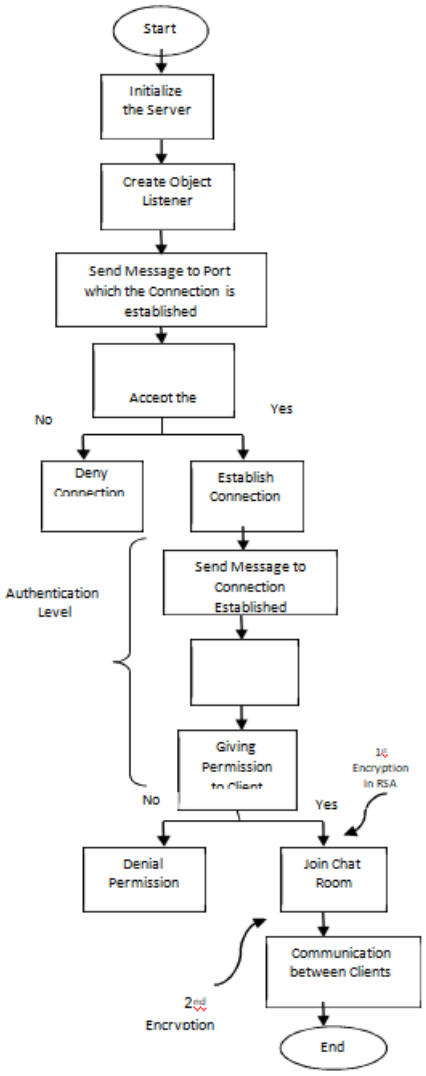

Figure 3: Flowchart of the proposed work.

Here, we used one authentication level and 2 coding levels [17][19][20]. we used GUI in MATLAB to raise user for the server IP and also the port that created the affiliation and also the client ID and password [17][21][22]. we used RSA algorithmic rule to code messages between client and also the server as the first encryption level and then encrypt messages between clients and chat space [21]. By means that of this model, secure electronic messaging in corporational environments may be supplied with the assistance of a 2 level authentication theme.

IV. EXPERIMENTAL RESULTS

The results that we tend to get once implementing the projected chat lab system in shown below in the figure.

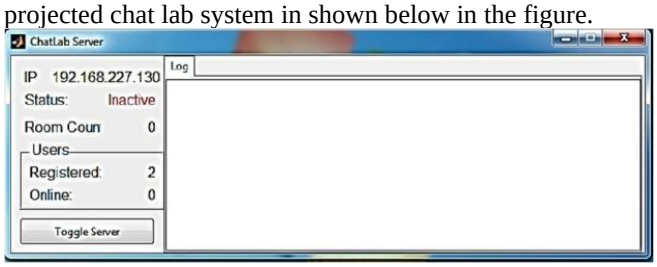

Figure 4: Starting the messaging environment.

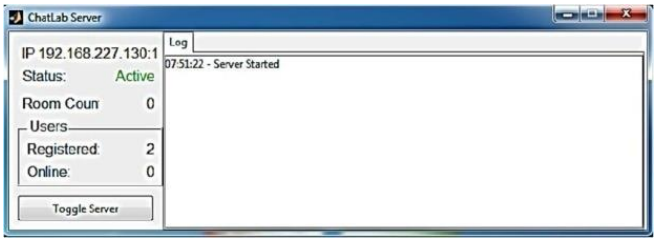

Figure 5: Initialize the server.

Figure 5: Authentication level.

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.CONCLUSION

Demonstrating of applicable client/server applications could be a basic figure for planning, sending, and later ability. The demonstrating advances needed during this labor aren't for the foremost half accessible, and not ready for wide dispersion to application originators and organizers. This paper highlights the utility needs for client/server models and depicts configuration inquiries to be attended. A model reenactment demonstrates dead an outsized range of the conditions recorded, and its utilization was shown in an exceedingly few real and speculative illustrations.

We tried with a client/server encrypted chat supported RSA by mistreatment MATLAB computer code coding polices. The result gave one authentication level and 2 coding levels by secure chat knowledge supported RSA algorithmic rule. We've enforced the system in client/server design and in period of time network. We tend to believe that the system provides high level in coding and additional flexibility in implementation. However, as a future work alternative coding algorithmic rules may well be used and a hybrid algorithm will be developed for more functions like quicker or wider electronic messaging wants.

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
10. Secure Architecture for Private Instant Messenger Application. International Conference on Computer Science and Information Technology (ICCSIT'2011), 2011.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. Vollala, S., Varadhan, V. V., Geetha, K., Ramasubramanian, N. (2017). Design of RSA processor for concurrent cryptographic transformations. Microelectronics Journal, 63, pp.112-122.
18. Gupta, N., Saxena, A., Jain, N. (2016). Pairwise Independent Key Generation Algorithm: A Survey. International Journal of Computer Applications, 156(6), pp.12-18.
19. Jain, A., Kapoor, V. (2015). Secure Communication using RSA Algorithm for Network Environment. International Journal of Computer Applications, 118(7), pp.6-9.
20. 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.
21. 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.
22. 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.
23. Lent, C. S. (2013). Learning to program with MATLAB: Building GUI tools. John Wiley & Sons.

24. 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.
25. 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.
26. 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.
27. N. Nithiyanandam, K. Venkatesh, M. Rajesh, Transfer The Levels Of The Monitored Carbon, Nitrogen Gases From The Industries, International Journal of Recent Technology and Engineering, Volume-7 Issue-6S3 April, 2019.
28. Sivanesh Kumar, A., Brittoraj, S., Rajesh, M., Implementation of RFID with internet of things, Journal of Recent Technology and Engineering, Volume-7 Issue-6S3 April, 2019.
29. Rajesh, M., Sairam, R., Big data and health care system using mlearningJournal of Recent Technology and Engineering, Volume-7 Issue-6S3 April, 2019.
30. Rajesh, M., and J. M. Gnanasekar. "Path Observation Based Physical Routing Protocol for Wireless Ad Hoc Networks." Wireless Personal Communications 97.1 (2017): 1267-1289.