Public Key Encryption Techniques Provide Extreme Secure Chat Environment

Kuldeep Chouhan and S.Ravi

Abstract— A secure chat scheme is readily accessible and very useful to communicate with people that might be anywhere in the world. Internet chat service provides the convenience of communicate with the people in real time. The objective of this work is to build a secure chat server utilizing public key encryption to send secure chat messages across the internet. It provides a technical implementation of a new structural design for encrypting the database in the network. This paper shows results that what security features should implement to accomplish a highly secured chat present a standalone system that can be implemented on any legacy systems with efficiently. This work classifies the protocol used by servers to talk with each other.

Index Terms— Chat Interface Area (CAI), Encryption technique, Public Key Encryption, Secure Chat, Secured Encrypted Chat (SEC), Security Threats, TCP/IP.

1 INTRODUCTION

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. 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 asignificant to keep private data security in order to avoid unauthorized access. The symmetric cryptography is be appropriate in the chat area is chaotic (a state of confusion) encryption method that is defined as a state of a nonlinear dynamical system and emerge only in certain circumstance, where for certain values of the system parameters and only in dynamical system characterized. To implement chaotic encryption, there are four characteristics,

(i) The chaotic maps have unpredictable trajectories where applied the confusion technique for build the cryptography.
(ii) The chaotic encryption has arbitrariness behaviour that caused by a high dependence on primary conditions exhibited in chaotic regimes.[1]
(iii) Chaotic algorithm is sensitive to initial condition and parameters that each point is arbitrarily closely approximated by other points with significantly different future trajectories.
(iv) The chaotic algorithm are used a nonlinear dynamical system exhibiting sensitively to mismatch parameters to both sender and receiver [19].

The secure chaotic encryption technique has an appropriate algorithm implemented to make a CAI application for more secure and reliable chat [6,19]. Everyone at any time may be sniffing our network activity, but, it's difficult to understand what data we send, because the public key can be received by any one. A chat message encrypted with it can be decrypted with the private key.

(i) Public key encryption
(ii) Delegates and Events
(iii) Thread safe events
(iv) TCP/IP

Several features proposed to both sender and receiver as follows:

(i) The intendrequest is flexible in a sense that gives ability to various tasks on the network.
(ii) Flexibility to change passwords that provides highly secure apparent environment to the users [22].
(iii) A secure data makes sure that if a user forgets password, then user does not completely lose their data.

The security measures consider during the design and development of the targeted secure chat is as logged all accesses activities to the server and provide features in the secure chat to search for unusual access patterns. It puts an upper limit on the number of data that a single user can access data to ensure impartiality. The secure chats have a permission system to the data that determines if a user is permitted to access it. An idea of a secure data is to provide secure storage of the server data as well as maintaining authorized access for the authorized users also. In order to maintain this level of security, there is a need to design a strong and secured data that let the data of the server being kept secret by implementing data Integrity and confidentiality as well as making the data partially shared.

A. Benefits of Chat Service

A secure chat provides the ability to have real time secure discussions among users electronically, one-to-one or in groups session. A public networks accumulate 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,

- *Mr. Kuldeep Chouhan is a Research Scholar in Electronics and Communication Department, Dr.MGR Educational and Research Institute, University, Chennai. PH- +91 9952059401. E-mail: kuldeep0009@gmail.com*
- *Dr. S. Ravi is Professor and Head in Electronics and Communication Department, Dr.MGR Educational and Research Institute, University, Chennai. PH- +91 9840148981. E-mail: ravi_mls@yahoo.com*

(i) Allows for instant communications between users [9,20].
(ii) Uses real time chat over the network that can eliminate costly long distance charges.
(iii) Allows for rapid query and rapid responses.

B. Negative of Chat Service

(i) Security problems of instant messaging program [12].
(ii) 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.
(iii) Chat programs can provide an open avenue of attack for hackers, crackers, spies and thieves.
    (a) eavesdrop: intercept messages.
    (b) actively insert messages into connection
    (c) removing sender or receiver, inserting himself in place.

C. Architecture of Chat Area Interface (CAI)

In Figure 1, the architecture of CAI is divided into two parts as, sender and receiver, where sender is needed to enter a chat message using CAI and the message will encrypt using encryption algorithm and then the message will send to receiver. In receiver part, decryption process will occur.

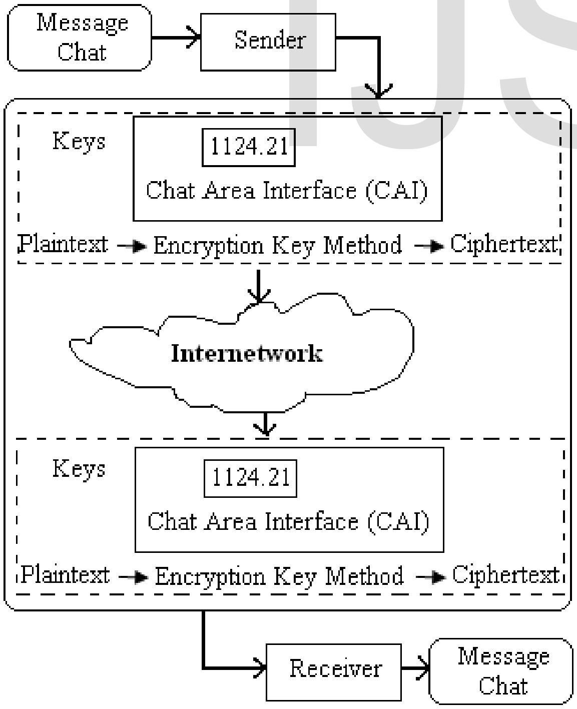


Fig. 1 Chat Area Interface Application

D. Weak spots in Secure Chat Issue

The security of the hierarchy is considered when organizing public key systems, conflict to attacks of particular keys from aside. Several attacks are based on suspicious measurements of the accurate time that take hardware to encrypt plaintext is used to simplify the search for likely decryption keys. Therefore, measly use of asymmetric key algorithms does not make sure security. Encrypted messages and responses should be intercepted, decrypted and re-encrypted by the attacker using the public key for different communication segment, in all occurrences, so as to avoid suspicion. An approach to prevent attacks involves a trusted third party responsible for verifying the identity of a user of the system [23]. For e.g., an authority should have a trusted certificate to contain appropriately checked the identity of the key-authority, must ensure the correctness of the public key.

2. PUBLIC-KEY CRYPTOGRAPHY

In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt [3]. Security depends on the secrecy of the private key [2,4]. In some related signature schemes, the private key is used to sign a message, anyone can check the signature using the public key. Public-key cryptography refers to a cryptographic system requiring two separate keys, (i) secret and (ii) public [8,11,18]. One key encrypts the plaintext and the other decrypts the cipher text. Public-key cryptography uses asymmetric key algorithms referred to used for public key cryptography is based on integer factorization and discrete logarithm problems [14,17]. Although it is easy for the intended recipient to generate the public and private keys, to decrypt the chat communication is using the private key and easy for the sender to encrypt the chat communication using the public key. A public key algorithm does not require a secure initial exchange of one or more secret keys between the sender and receiver [7]. The basic cryptographic model is shown in Figure 2.

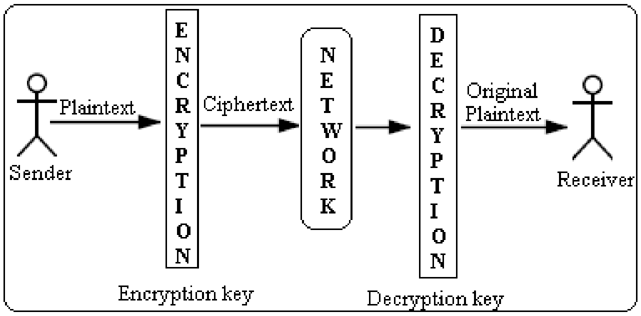


Fig. 2 Basic cryptographic model

A. Process of the Public-key cryptography

The public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. The publicly available encrypting-key is widely distributed, while the private decrypting-key is known only to the recipient [16]. Messages are encrypted with the recipient's public key and can be decrypted only with the corresponding private key. The discovery of algorithms that could produce public/private key pairs revolutionized the practice of cryptography. A symmetric-key algorithms variations use a single secret key, which is shared and kept private by both the sender and the receiver, for encryption and decryption [10]. To use a symmetric encryption scheme, the sender and receiver must securely share a key in advance.The main two uses for public-key cryptography are,

(i) A chat message encrypted with a recipient's public key cannot be decrypted by anyone except a possessor of the matching private key.

(ii) In digital signatures, a chat message signed with a sender's private key that is verified by anyone who has access to the sender's public key, thus, proving the sender had access to the private key.

3. IMPLEMENT SOLUTION FOR ENCRYPTION TECHNIQUE

It utilizes public key encryption to securely transmit messages between users, where each message with public key of target recipient. Since, chat messages are normally not long, requires less processing time for the program to encrypt the message. In encryption technique, interception occurs but, the interceptor cannot decipher the message [13]. An insertion of data can happen, but, the digital signature ensures that message is authentic.

A. Secure Chat Protocol

The following secure chat protocols has been defined are,

(i) Two clients connect to a server.

(ii) Once connected, each client generates their public and private keys locally.

(iii) The public key sent to the server and is set so, when a user clicks their name any message sent will be encrypted with that public key.

When message is sent out, the client program downloads the public key and encrypts the intended message and then applies the digital signature which is created with the private key and then sends the encrypted message out. When the packet is received by the specified person, the client program automatically applies the private key on the text and outputs the message so that the user can see it decrypted and then double checks the digital signature with a public key. Once completed with each step, we have successfully transmitted a secure message.

B. Secure Chat Protocol with Security Threats

This protocol provides message security that does not provide protection against faking to be the person client is talking to another.

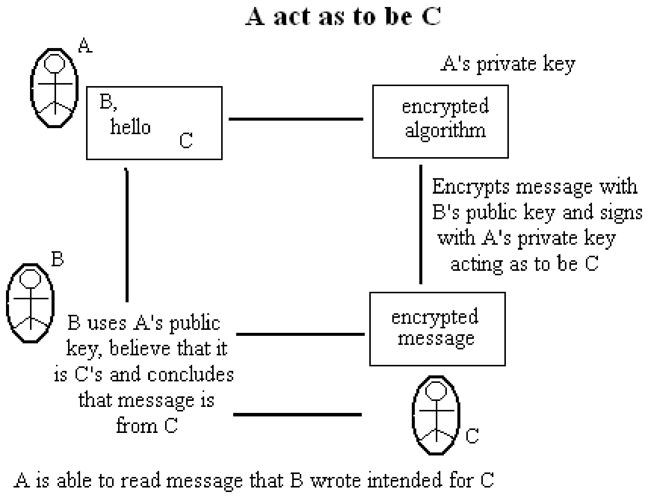


Fig. 3 Secure chat protocol process

Figure 3 shows the process that utilizing chat protocol created a secure chat program that successfully communicates securely. The RSA algorithm was utilized in encrypting and decryptingthe small messages sent between users [1,5,8,11]. The secure chat program allows for two users to connect to the server and encrypts messages with each other's public keys.

4. COMPONENTS OF THE PROPOSED ARCHITECTURE

A. User Authentication and Authorization

The secure chat data is necessary to use a strong mechanism to verify the clients. The most constantly used approach is request for a client name and password to authenticate the client [14]. Some of key points that consider in the design of authentication mechanism are: transmitting the password in to protect the client privacy [6,15] and to safe the data during chat process occur and also, required the secure data provides secure storage of the client names and passwords along with a method to manage them, including reset the passwords. During the preliminary design of secure chat is whether to store the password (store in hash/plain text format) as the client cross the threshold [21].

B. Secure Encrypted Chat (SEC) Process

In this section, state chart provides more aspect into the interaction of multiple user with the SEC application. It observes the exchange of public keys to concur on a shared secret key. It sets up the shared secret between the two SEC Client, which is used to share a secret key. The state chart diagram for SEC system Client operations is shown in Figure 4.

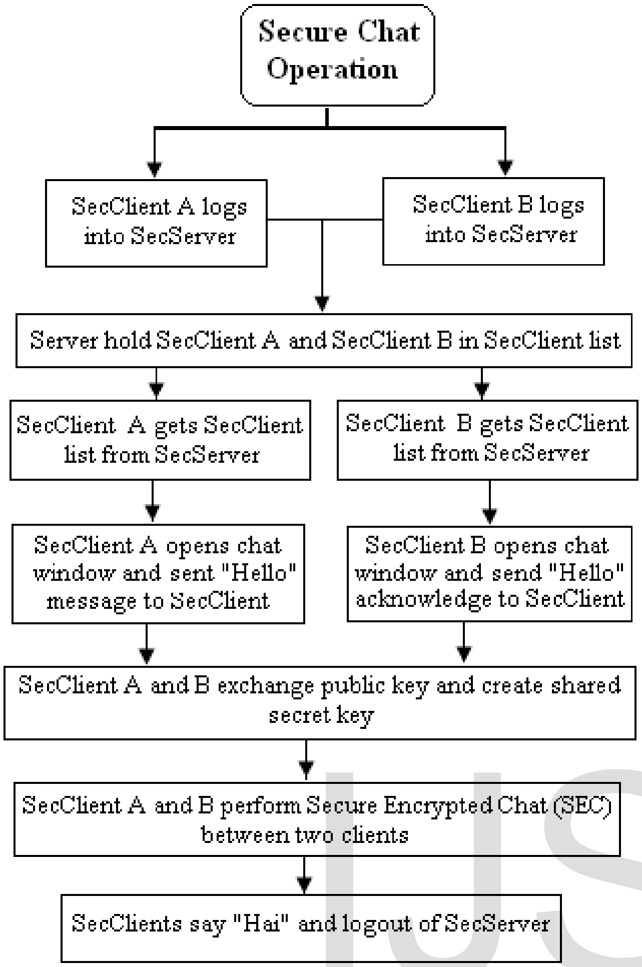

Secure Chat Operation
SecClient A logs into SecServer
SecClient B logs into SecServer
Server hold SecClient A and SecClient B in SecClient list
SecClient A gets SecClient list from SecServer
SecClient B gets SecClient list from SecServer
SecClient A opens chat window and sent "Hello" message to SecClient
SecClient B opens chat window and send "Hello" acknowledge to SecClient
SecClient A and B exchange public key and create shared secret key
SecClient A and B perform Secure Encrypted Chat (SEC) between two clients
SecClients say "Hai" and logout of SecServer

Fig.4 State Chart diagram for SEC system for Client operations

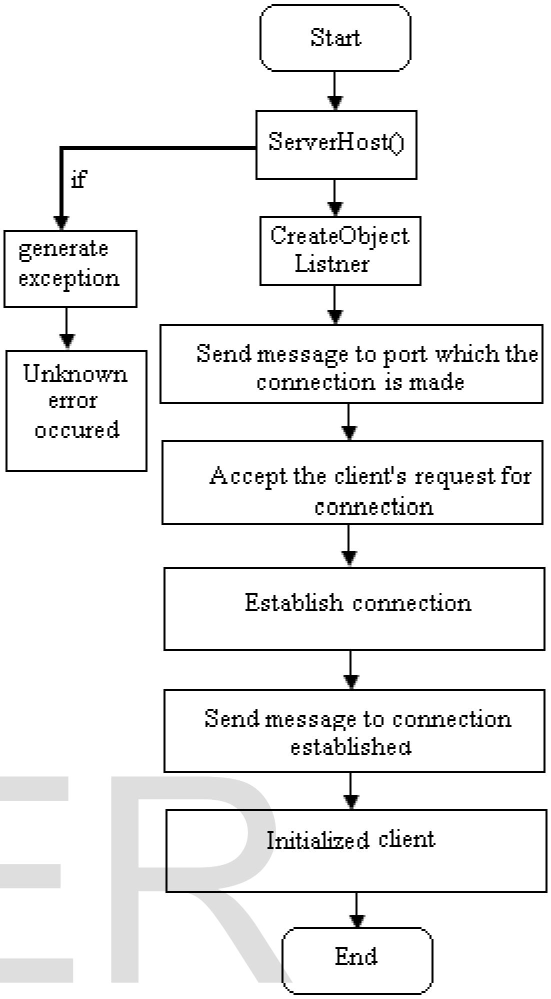

Start
ServerHost()
if
generate exception
Unknown error occured
CreateObject Listner
Send message to port which the connection is made
Accept the client's request for connection
Establish connection
Send message to connection established
Initialized client
End

Fig. 5 Flow chart of Secure chat Session

5. SECURE CHAT SESSION

When initialize method, it follows the steps which is shown in Figure 6.

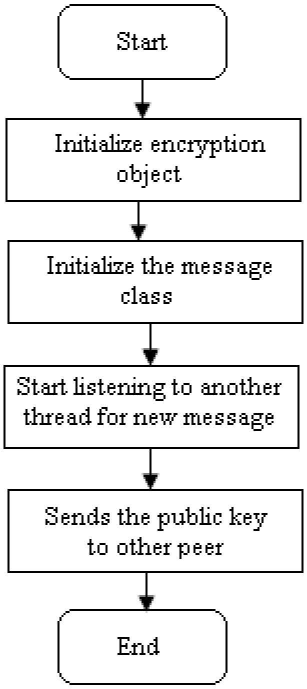
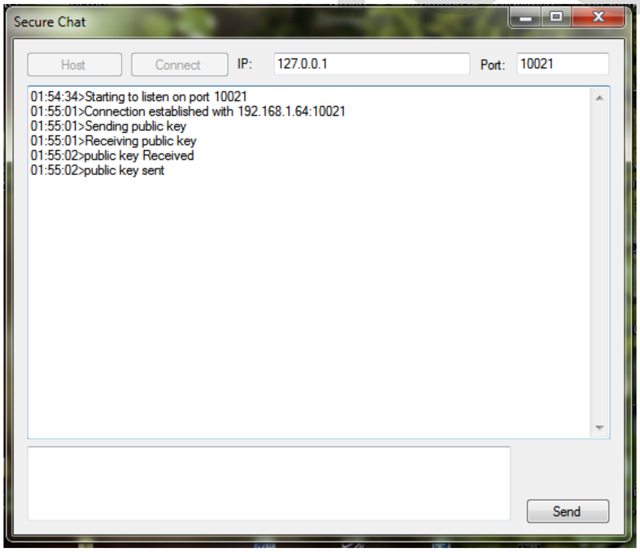

Start
Initialize encryption object
Initialize the message class
Start listening to another thread for new message
Sends the public key to other peer
End

Fig. 6 Steps of initialization for message transmission

6. RESULTS AND DISCUSSION

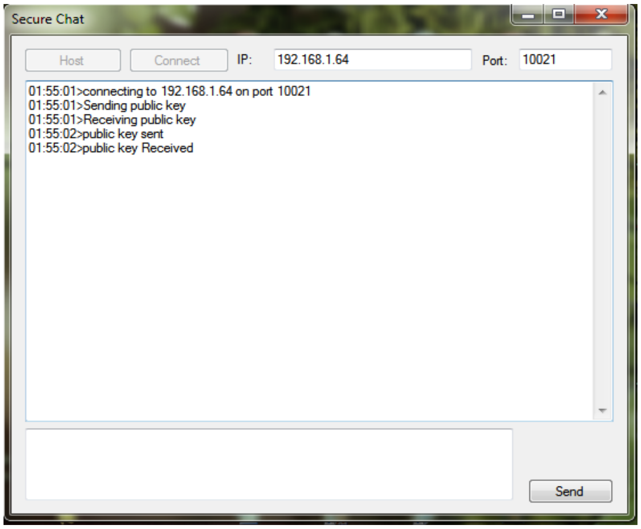
In this section, CAI is developed using this technology that is embedded with cryptography which is chaotic encryption to secure chat data is shown in Figure 7 to 10.

Screen Shots:-



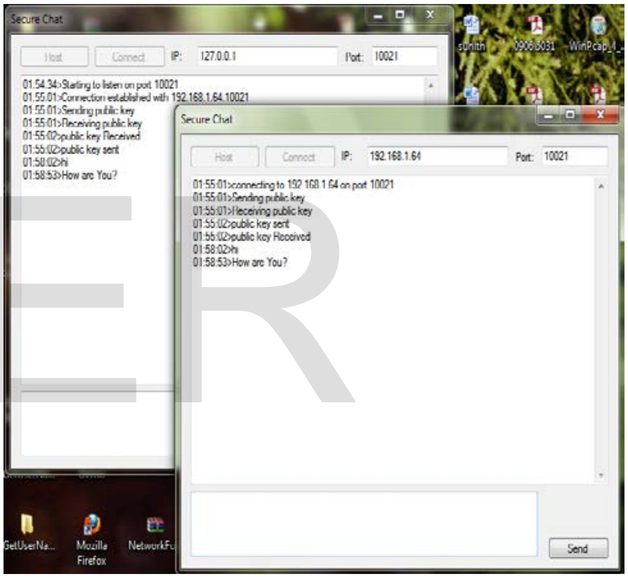
```
01:54:34>Starting to listen on port 10021
01:55:01>Connection established with 192.168.1.64:10021
01:55:01>Sending public key
01:55:01>Receiving public key
01:55:02>public key Received
01:55:02>public key sent
```

Fig. 7 Listen message on port in secure chat



```
01:55:01>connecting to 192.168.1.64 on port 10021
01:55:01>Sending public key
01:55:01>Receiving public key
01:55:02>public key sent
01:55:02>public key Received
```

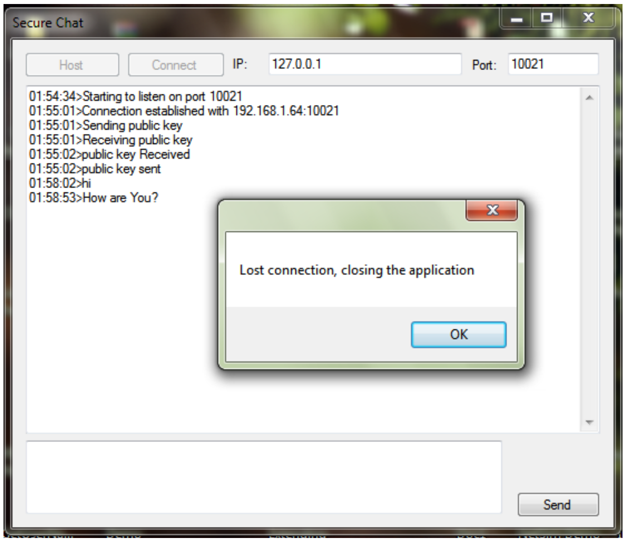
Fig. 8 Connection with an IP port



```
01:54:34>Starting to listen on port 10021
01:55:01>Connection established with 192.168.1.64:10021
01:55:01>Sending public key
01:55:01>Receiving public key
01:55:02>public key Received
01:55:02>public key sent
01:58:02>hi
01:58:53>How are You?
```

```
01:55:01>connecting to 192.168.1.64 on port 10021
01:55:01>Sending public key
01:55:01>Receiving public key
01:55:02>public key sent
01:55:02>public key Received
01:58:02>hi
01:58:53>How are You?
```

Fig. 9 Sending and Receiving message in Secure Chat



```
01:54:34>Starting to listen on port 10021
01:55:01>Connection established with 192.168.1.64:10021
01:55:01>Sending public key
01:55:01>Receiving public key
01:55:02>public key Received
01:55:02>public key sent
01:58:02>hi
01:58:53>How are You?
```

Lost connection, closing the application

Fig. 10 Connection lost between sender and receiver process

7. CONCLUSION

In this work, it focuses on implementation an appropriate encryption technique in chat area interface (CAI). A chaotic was chosen, because it sends a short message and secure chat message. In this work, we found that chat encryption prevents a message from unauthorized person to view or modify a message. CAI is become more secure and reliable with implementation of chaotic encryption and executes SEC provided an opportunity to use the software design skills.

ACKNOWLEDGEMENT

The authors heartly thank M/s. MicroLogic Systems, Chennai-600017, for the infrastructure to carry out this work successfully.

REFERENCES

[1] A.S.C. Crepeau, "Simple backdoors for RSA key generation", proceeding of Cryptographers" Track at the RSA Conference, pp. 403-416, 2003.

[2] Anjaneyulu, G.S.G.N., and Reddy, U.M., "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, 2012.

[3] Anshel I., Anshel M., and Goldfeld D., "An algebraic method for public-key cryptography", Math. Research letters 6, pp. 287-291, 2003.

[4] A. Datta, A. Derek, J. Mitchell, and B. Warinschi, "Key exchange protocols: Security definition, proof method and applications", 19th IEEE Computer Security Foundations Workshop (CSFW 19), Venice, Italy, 2006.

[5] Constantinos Patsakis, "Number Theoretic SETUPs for RSA Like Factoring Based Algorithms", Journal of Information Hiding and Multimedia Signal Processing Volume 3, Number 2, April 2012.

[6] Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune, Ahren Studer, Adrian Perrig, Bo-Yin Yang and Tzong-Chen Wu, "GAnGS: Gather authenticate 'n group securely", in proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MobiCom), September 2008.

[7] David J. Malan, Matt welsh and Michael D. Smith, "Implementing Public-Key Infrastructure for Sensor Networks", ACM Transactions on Computational Logic, Vol. 5, No.7, pp. 1-7, December 2007.

[8] D. Aggarwal and U. Maurer, "Breaking RSA generically is equivalent to factoring", Proceeding of 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, vol. 5479, pp. 36-53, 2009.

[9] David Snogles, "Personal Encrypted Talk - Securing Instant Messaging with a Java Application", Rivier College Online Academic Journal, Vol. 1, No. 1, Fall 2005.

[10] E. Filiol, "Anti-forensic techniques based on malicious cryptography", Proceeding of the 9th European Conference on Information Warfare and Security, pp. 63-70, 2010.

[11] J. S. Coron, A. Joux, I. Kizhvatov, D. Naccache and P. Paillier, "Fault attacks on RSA signatures with partially unknown messages", Proceeding of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, vol. 5747, pp. 444-456, 2009.

[12] Jiangzhe Wang, Chunyi Peng, Chiyu Li, "Implementing Instant Messaging Using Named Data", AINTEC'10, Bangkok, Thailand, November 15–17, 2010.

[13] Ko, K.H., Lee.S. J., Cheon, J.H, Han,J.W., Kang.J.S.,Park, C., "New public-key cryptosystem using braid", Crypto, pp. 166-184, 2010.

[14] Michel Abdalla, Emmanuel Bresson, Olivier Chevassut and David Pointcheval, "Password-based group key exchange in a constant number of rounds", in Public Key Cryptography (PKC), pages 427–442, 2006.

[15] Maheswara Rao Valluri, "Authentication Schemes using Polynomials Over Non-commutative Rings", International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.4, December 2012.

[16] Manoj Kumar, Pratibha Yadav, Meena Kumari, "Rectified Differential Cryptanalysis of 16 Round Present", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.4, December 2012.

[17] M. Backes, I. Cervesato, A.D. Jaggard, A. Scedrov and J.-K. Tsay, "Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos", Springer-Verlag Berlin Heidelberg, ESORICS-2006, LNCS 4189, pp. 362–383, 2006.

[18] M. Backes and B. Pfitzmann, "Relating symbolic and cryptographic secrecy", IEEE Transactions, Dependable Secure Computer, 2(2):109–123, April–June 2005.

[19] Mohd Kamir Yusof, Nor Surayati Mohamad Usop and Ahmad Faisal Amri Abidin, "A Secure and Reliable Chat Room Application via Embedded Chaotic Encryption", Smart Computing Review, vol. 2, no. 2, April 2012.

[20] Mohd Kamir Yusof, Surayati Mohammad Usop, Ahmad Faisal AmriAbidin, "Designing a Secure Architecture for Private Instant Messenger Application", International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya Dec. 2011.

[21] R. Kayalvizhi, R. Harihara Subramanian, R. Girish Santhosh, J. Gurubaran, V. Vaidehi, "VLSI Design and implementation of combined secure hash algorithm SHA-512. CNSA 2010, CCIS 89, pp. 105-113, 2010.

[22] Syed S. Rizvi, Aasia Riasat, Khaled M. Elleithy, "Combining private and public key Encryption techniques for providing Extreme secure environment for an Academic institution application", International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[23] Yue-Hsun Lin, Ahren Studer, Hsu-Chun Hsiao, Jonathan M. McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, and Bo-Yin Yang, "SPATE: Small-group PKI-less authenticated trust establishment", in proceedings of the 7th Annual International Conference on Mobile Systems, Applications and Services (MobiSys), June 2009.

BIOGRAPHIES

KuldeepChouhan received M.Tech. (CSE) degree in the year 2009. He is a Research Scholar in Dr. MGR University, Chennai. He published Two International journals and one International conference. His area of interests is Wireless sensor network (WSN), Cryptography, Image noisy filter, system and Intelligent system.

Dr. S. Ravi received DEEE, A.M.I.E (ECE), and M.E. (CS) degree in the year 1989, 1991 and 1994 respectively and Doctorate degree from Anna University, Chennai in the year 2004. He is having 19 years of teaching experience. His areas of interests are VLSI, Embedded Systems, Image Processing and Simulation and Modelling. He has published more than 40 papers in International / National Conferences and 30 in Journals. He is a member of IEEE and ISTE and Life member of IETE and IETUK.