JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-3, Issue-9 E-ISSN: 2347-2693

Advanced Data Encryption/Decryption using Multi Codes for One Character

R. Durga Prasad[1*], R.N.D.S.S Kiran[2], Andey Krishnaji[3]

[1*,2,3]*Department of MCA,* Swarnandhra College of Engineering and Technology,
JNTUK University, Narasapuram

www.ijcseonline.org

Received: Aug/12/2015 Revised: Aug/20/2015 Accepted: Sep/17/2015 Published: Sep/30/2015

Abstract— Cryptography is one way of providing security using the process of encryption and decryption. An original message is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as enciphering or encryption and that of restoring the plaintext from the cipher text is deciphering or decryption. The purpose of the proposed system is to encrypt the sending message using a very sophisticated 5-codes encryption method to encrypt the data so as to ensure no leakage of sensitive and confidential information while sending a message. The proposed technique converts each character represented as a 5 codes, each code consist of a 5 digits. In order to provide advanced level of security we proposed a multi-codes generation algorithm which generates the code dynamically every time a message is initiated from either sender or receiver. The main objective of the software is to maintain the security of information transmitted via modern means of transportation such as the internet, mobile and so on. In this work, a robust RMI-based Multi Client Chat application is designed in which multiple clients can communicate through a secure RMI communication channel by sending and receiving messages between/among them. The application uses advanced encryption and decryption algorithm which uses the character codes for encryption and decryption. Each character is represented by 5 codes, each code consists of 5 digits. For example, A= {95231, 45672, 11132, 22367, 95267}.

keywords- RMI (Remote Method Invocation), Data Encryption, multi codes, Cryptography

I. INTRODUCTION

A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

A. *Network Security Applications:*

- *Transport-Level Security*: Virtually all businesses, most government agencies, and many individuals now have Web sites. The number of individuals and companies with Internet access is expanding rapidly and all of these have graphical Web browsers. As a result, businesses are enthusiastic about setting up facilities on the Web for electronic commerce. But the reality is that the Internet and the Web are extremely vulnerable to compromises of various sorts. As businesses wake up to this reality, the demand for secure Web services grows. The topic of Web security is a broad one and can easily fill a book. In this chapter, we begin with a discussion of the general requirements for Web security and then focus on three standardized schemes that are becoming increasingly important as part of Web commerce and that focus on security at the transport layer: SSL/TLS, HTTPS, and SSH.

- *Wireless Network Security:* There are two important wireless network security schemes. First, we look at the IEEE 802.11i standard for wireless LAN security. This is devoted to security standards for Web access from mobile wireless devices, such as cell phones. An overview of the Wireless Application Protocol (WAP), which is a set of standards for communication between mobile devices attached to a cellular network and a Web server. Then we examine the Wireless Transport Layer Security (WTLS) protocol, which provides security between the mobile device and a gateway that operates between the cellular network and the Internet. Finally, we cover end-to-end security services between WAP devices and Web servers.

- *Electronic mail Security:* Users expect to be able to, and do, send e-mail to others who are connected directly or indirectly to the Internet, regardless of host operating system or communications suite. With the explosively growing reliance on e-mail, there grows a demand for authentication and confidentiality services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (PGP) and S/MIME.

- *IP Security:* Users have security concerns that cut across protocol layers. IP-level security encompasses three functional areas: authentication, confidentiality, and key management. The authentication mechanism assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit. The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties. The key management facility is concerned with the secure exchange of keys. We begin this chapter with an overview of IP security (IP sec) and an introduction to the IP sec architecture. We then look at each of the three functional areas in detail.

B. RMI client/server model

RMI (Remote Method Invocation) is the Java version of what is generally known as a remote procedure call (RPC), but with the ability to pass one or more objects along with the request. The object can include information that will change the service that is performed in the remote computer. For example, when a user at a remote computer fills out an expense account, the Java program interacting with the user could communicate, using RMI, with a Java program in another computer that always had the latest policy about expense reporting. In reply, that program would send back an object and associated method information that would enable the remote computer program to screen the user's expense account data in a way that was consistent with the latest policy. The user and the company both would save time by catching mistakes early. Whenever the company policy changed, it would require a change to a program in only one computer

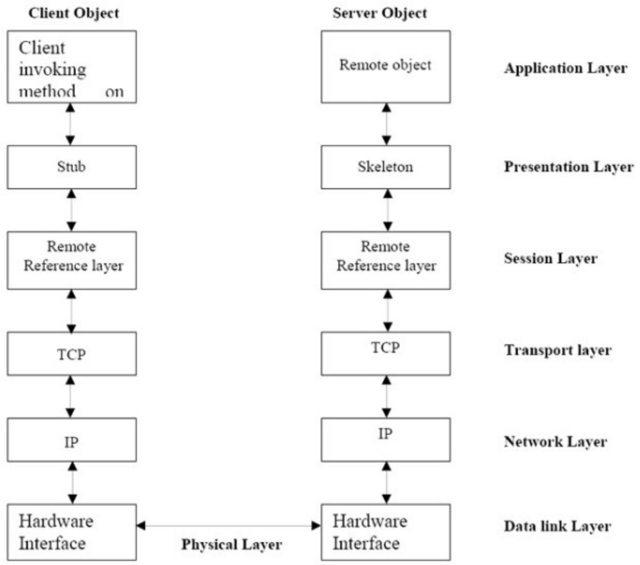


Fig 1: client/ server architecture using RMI

II. LITERATURE SURVEY

A. AES (Advanced Data Encryption)

The four finalists were all determined to be qualified as the AES.

The final evaluation, which also solicited worldwide public input, was based on three characteristics:

Security: It encompassed resistance to known attacks, mathematical soundness, randomness of output and security compared to other algorithms.

Cost: Encompassed encryption speed, required memory, and no licensing agreements i.e. the algorithm had to be available worldwide royalty free.

Algorithm and implementation characteristics: The algorithm had to be suitable across a wide range of hardware and software systems. The algorithm had to be relatively simple as well. After extensive review the Rijndael algorithm was chosen to be the AES algorithm [1].

B. Triple DES

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It derives from single DES but the technique is used in triplicate and involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length Known for its compatibility and flexibility can easily be converted for Triple DES inclusion [2].

B. Secure RSA (Rivest Shamir Adelman)

It generates two keys: public key for encryption and private key to decrypt message.RSA algorithm consist of three phases, phase one is key generation which is to be used as key to encrypt and decrypt data, second phase is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third phase is decryption, where encrypted text is converted in to plain text at other side. As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message. Secure RSA prevents files from hackers and help safe transmission of files from one end to other [3].

C. DES (Data Encryption Standard)

The encryption transformation depends on a 56-bit secret key and consists of sixteen Feistel iterations surrounded by two Permutation layers: an initial bit permutation IP at the input, and its inverse IP−1 at the output. The structure of the cipher is depicted. The decryption process is the same as the encryption, except for the order of the round keys used in the Feistel iterations. The 16-round Feistel network, which constitutes the cryptographic core of DES, splits the 64- bit data blocks into two 32-bit words, LBlock and RBlock (denoted by *L*0 and *R*0). In each iteration (or round), the second word Ri is fed to a function ***f*** and the result is added to the first word *Li*. Then both words are swapped and the algorithm proceeds to the next iteration [4].

D. Diffie Hellman

The algorithm itself does not encrypt data, but instead it generates a secret key common to both the sender and the recipient. Although they never agreed on using a particular key, through mathematically linked processes the two parties can independently generate the same secret key and then use it to build a session key for use in asymmetric algorithm. This procedure is called key agreement, meaning that the two parties are agreeing on a key to use [5].

III. PROBLEM STATEMENT

A message is to be transmitted from one party to another across a secure communication channel. The problem of this paper is to encrypt the message using a very sophisticated technique called Multi Codes for One Character so as to ensure no leakage of sensitive and confidential information while sending the message. In the proposed work, the system works by converting plain text to encrypted text by using character codes. A robust RMI-based Multi Client Chat application is designed in which multiple clients can communicate through a secure RMI communication channel by sending and receiving messages between/among them. It uses advanced encryption and decryption algorithm which uses the character codes for encryption and decryption. Each character is represented by 5 codes, each code consists of 5 digits. For example, A= {95231, 45672, 11132, 22367, 95267}.

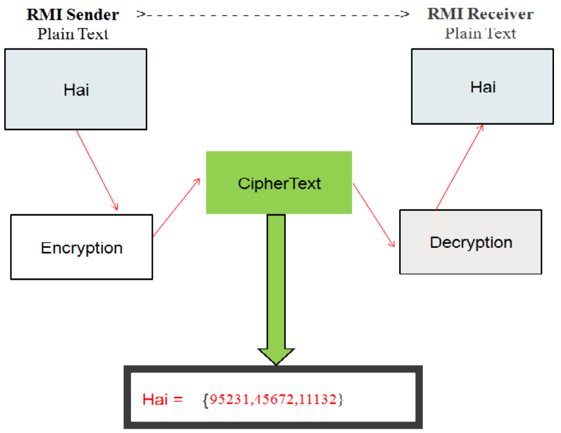


Fig 2: RMI based Client/Server Secure Communication Channel

IV. OBJECTIVES

- The main objective of this software is to encrypt the message using a very sophisticated technique to encrypt the data so as ensure no leakage of sensitive and confidential information while sending the message.
- To proposed a multi-codes generation algorithm which generates the codes dynamically every time a message is initiated from either sender or receiver.
- To represent each constituent character of the message using randomly generated character codes during encryption. Each character is represented by 5 codes, each code consists of 5 digits.

V. METHODOLOGY

In the proposed work, the system works by converting plain text to encrypted text by using character codes. A robust RMI-based Client/Server architecture is designed in which client and server communicates through a secure communication channel by sending and receiving messages between them. It uses advanced encryption and decryption algorithm which uses the character codes for encryption and decryption. Each character is represented by 5 codes, each code consists of 5 digits. For example, A= {95231, 45672, 11132, 22367, 95267}. The high level diagram of the proposed system is shown in the following figure.

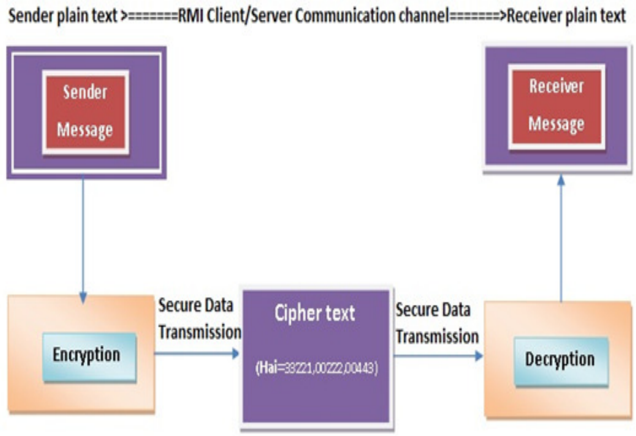
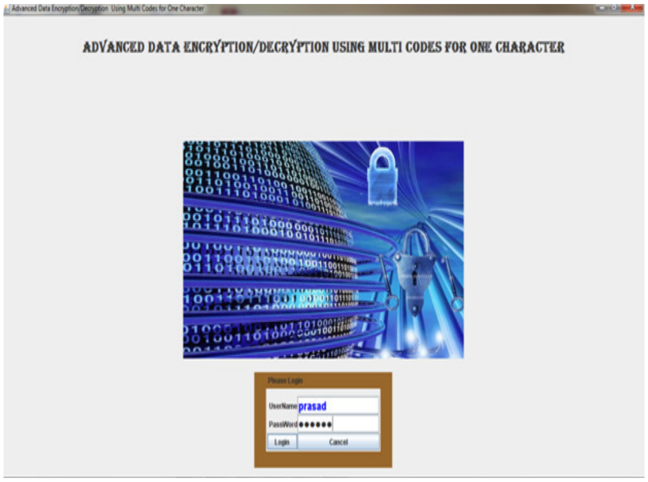


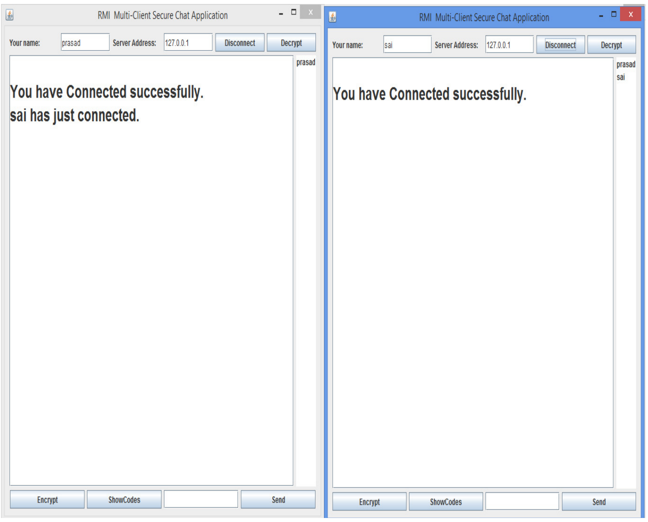
Fig 3: RMI based Client/Server Secure Communication Architecture

VI. RESULTS AND DISCUSSION


Advanced Data Encryption/Decryption Using Multi Codes for One Character
ADVANCED DATA ENCRYPTION/DECRYPTION USING MULTI CODES FOR ONE CHARACTER
Please Login
Login
Cancel

UserName prasad
PassWord ●●●●●●

Fig 4: Login Window


RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send
RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send

Your name: prasad Server Address: 127.0.0.1

You have Connected successfully.
sai has just connected.

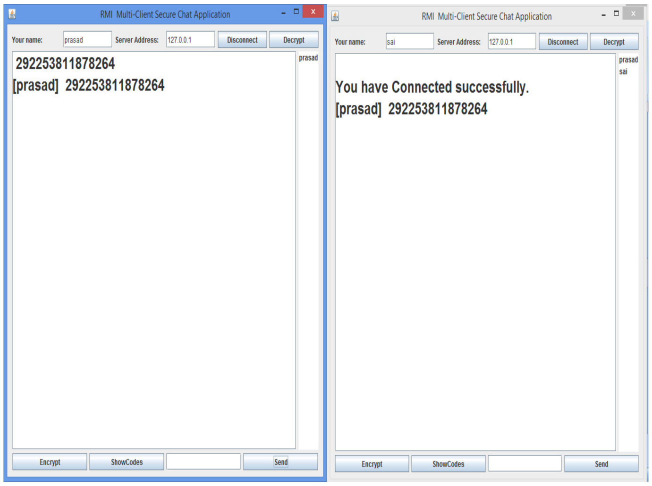
prasad

Your name: sai Server Address: 127.0.0.1

You have Connected successfully.

prasad
sai

Fig 5: Clients Connection Window


RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send
RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send

Your name: prasad Server Address: 127.0.0.1

292253811878264
[prasad] 292253811878264

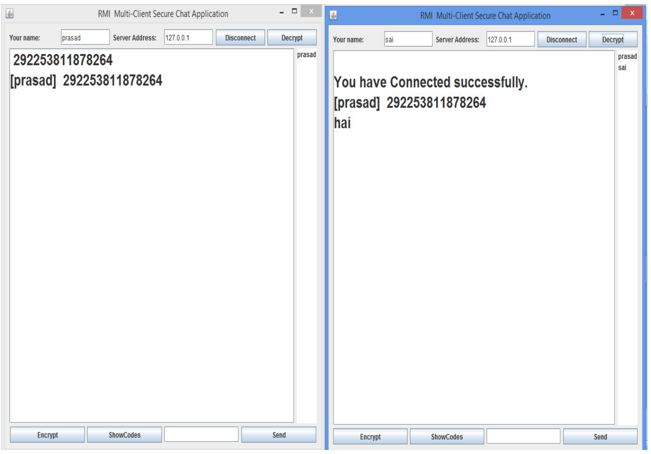
prasad

Your name: sai Server Address: 127.0.0.1

You have Connected successfully.
[prasad] 292253811878264

prasad
sai

Fig 6: Encryption Process


RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send
RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send

Your name: prasad Server Address: 127.0.0.1

292253811878264
[prasad] 292253811878264

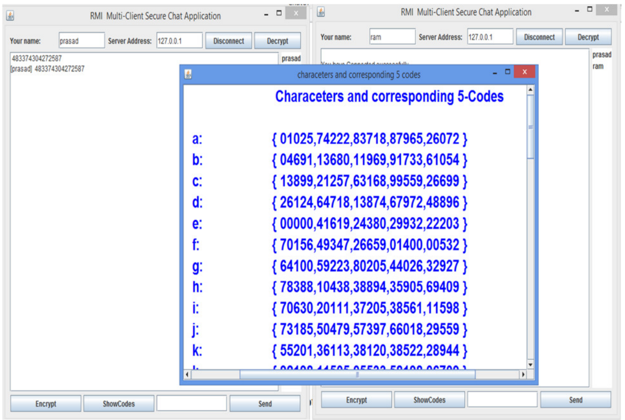
prasad

Your name: sai Server Address: 127.0.0.1

You have Connected successfully.
[prasad] 292253811878264
hai

prasad
sai

Fig 7: Decryption Process


RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send
RMI Multi-Client Secure Chat Application
Disconnect
Decrypt
Encrypt
ShowCodes
Send
characeters and corresponding 5 codes

Your name: prasad Server Address: 127.0.0.1

483374304272587
[prasad] 483374304272587

prasad

Your name: ram Server Address: 127.0.0.1

prasad
ram

Characeters and corresponding 5-Codes

a: { 01025,74222,83718,87965,26072 }
b: { 04691,13680,11969,91733,61054 }
c: { 13899,21257,63168,99559,26699 }
d: { 26124,64718,13874,67972,48896 }
e: { 00000,41619,24380,29932,22203 }
f: { 70156,49347,26659,01400,00532 }
g: { 64100,59223,80205,44026,32927 }
h: { 78388,10438,38894,35905,69409 }
i: { 70630,20111,37205,38561,11598 }
j: { 73185,50479,57397,66018,29559 }
k: { 55201,36113,38120,38522,28944 }

Fig 8: Characters and Corresponding 5-Codes

VII. CONCLUSION

Cryptography is one way of providing security using the process of encryption and decryption. An original message is known as the plaintext, while the coded message is called the cipher text. The process of converting from plaintext to cipher text is known as encryption. The process of restoring the plaintext from the cipher text is decryption. In this work, the proposed system encrypt the message sent by the sender using a very sophisticated 5-codes encryption method to encrypt the data so as to ensure no leakage of sensitive and confidential information while sending a message. We designed and implemented an algorithm that creates 5 different codes for each character in the message wherein each code consist of a 5 digits. In order to provide advanced level of security we proposed a multi-codes generation algorithm which generates the code dynamically every time a message is initiated from either sender or receiver. The system has been tested with different types of messages in multi-client environments. The results are found to have been impressive when compared with other existing algorithms.

VIII. ACKNOWLEDGEMENT

I would like to acknowledge the support and encouragement received from my guide Sri.R.N.D.S.S Kiran, Assistant Professor of the Department of MCA. I do express my heart-felt gratitude to Dr. S. Ramesh Babu, Secretary Correspondent, Swarnandhra College of Engineering and Technology. In addition, I am thankful to all the faculty members and other staff members of the Department of Master of Computer Applications and my friends for providing me adequate help and support whenever required. I am thankful to Andey Krishnaji, my project coordinator for his guidance and support throughout the duration of this work. I am deeply indebted to my parents for their support.

IX. REFERENCES

[1] Roshni Padate, Amana Patel," Encryption and Decryption of Text Using AES Algorithm ", International Journal of Emerging Technology and Advanced Engineering , ISSN 2250-2459, ISO 9001:**2008** Certified Journal, Volume 4, Issue 5, May 2014.

[2] Karthik, Muruganandam, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System ", International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878, Volume 2 Issue 11, November **2014**.

[3] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA ", International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February **2013**.

[4] Prashanti.G, Deepthi.S, Sandhya Rani.K," A Novel Approach for Data Encryption Standard Algorithm ", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-2, Issue-5, June **2013**.

[5] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb Omotunde ," Diffie-Hellman and Its Application in Security Protocols ", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November **2012 .**

[6] Raymond, J.F. and Stiglic, A. (2000) Security Issues in the Diffie-Hellman Key agreement protocol.(http://crypto.cs.mcgill.ca/~stiglic/publications.html)[Accessed 17 March **2012**].

[7] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma, — Analysis and Comparison between AES and DES Cryptographic Algorithm‖, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December **2012**, pp 362-365.

[8] Sattar J Aboud, "An efficient method for attacking RSA scheme", IEEE **2009**.

[9] About AES – Advanced Encryption Standard‖, Copyright 2007 Svante Seleborg Axantum Software AB.

[10] Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and **2003**.

[11] Data Encryption Standard (DES), FIPS PUB 46-3 - **1999**.

[12] "A public key cryptosystem and a signature scheme based on discrete locarithms" TaherElGamal **1998**, Springer-Verlag.

[13] William Stallings, Network Security Essentials: Applications and Standards, 4th ed., Prentice Hall.

[14] New Approach of Data Encryption Standard Algorithm Shah Kruti R., Bhavika Gambhava.

[15] Abdul kader, Diaasalama and Mohiv Hadhoud, "Studying the Effect of Most Common Encryption Algorithms," International Arab Journal of e-technology, Vol.2. No.1. **2014**

AUTHORS PROFILE

Mr. Durga Prasad Rapaka is a student of MCA Final year from Swarnandhra college of Engineering and Technology, Narasapur. His areas of interest are Core Java, Network Security, and Data Mining.

Mr. R.N.D.S.S Kiran, working as a Assistant Professor, Department of MCA, Swarnandhra college of Engineering and Technology, Narasapur. His areas of interest are Data Mining, Network Security.

Mr. Andey Krishnaji is a project coordinator at Department of Computer Applications in Swarnandhra College of Engineering and Technology. His areas of interest are Neural Networks, Data mining, Fuzzy logic Computational analytics. He is a popular trainer in the areas of Core Java, Advanced Java, c and data structures. He has developed a good number of software applications. He can be reached through his blog www.ijice.org which contains a good number of articles on Technology and Programming.