ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

A Dynamic and Trust Based Privacy Preserving Mechanism to Secure the Data during Transmission using Cryptography

E.Soumya[1], Dr. R. China Appala Naidu[2], A. Santhoshi[3], A S V R R Prasada[4]

Asst. Professor, Dept of IT, St.Martin's Engineering College, Hyderabad[1, 3]

Professor, Dept of CSE, St.Martin's Engineering College, Hyderabad[2]

Student, B. Tech, Malla Reddy Institute of Engineering and Technology, Hyderabad[4]

Abstract: In today's world of computer security, integrity and confidentiality of data is the most important and a primary concern. The issue related to the security of electronic data when transmitted over the internet is dealt in this paper. Data encryption is widely used to ensure security of the data. The encryption standards such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are widely in use to resolve the issues of transmission over an insecure channel. With the advancement in computer software and hardware, these standards seem not to be so secure and fast as one would like. In this paper we have proposed a fast and secure dual encryption algorithm using permutations, shifting operations. The proposed symmetric encryption procedure has two advantages over conventional schemes. Firstly, the encryption and decryption processes are much simpler and faster. Secondly, the security level is higher due to the application of dual encryption on the data which is being transmitted. The encryption and decryption procedures are explained in this paper.

Keywords: Integrity, Confidentiality, Encryption, Decryption, Symmetric Key, Permutations, Cryptography.

I. INTRODUCTION

Data security refers to providing privacy to the data. It is nothing but something is covered to the data. Each and every organization will have some data, where it should get protected.

We are living in the information age. We need to have record of every aspect in our lives. The value of information is same as the value of other assets. As it is an asset, proper measures should be taken to ensure it is safe from attacks.[12,5]

To be secured, the information needs to be hidden from unauthorized access (confidential), protected from unauthorized change (integrity) and available to an authorized entity when it is needed.

Until few decades ago, the information collected by an organization was stored on physical files. The confidentiality of the files was achieved by restricting the access to a few authorized and trustworthy people in the organization. Similarly only few authorized people were allowed to change the contents of the file.

With the invention of computers, information storage became electronic. Instead of being stored on physical media, it is stored in computers. The files stored in computers require confidentiality, integrity and availability. Information is now distributed. Authorized people can send and retrieve information from a distance. Not only the information be confidential, it should also be a way to maintain its confidentiality when it is transmitted from one place to another place. Integrity means changes need to be done only by authorized entities and through authorized mechanisms. Information tends to be useless if it is unavailable. Information needs to be constantly changes, which mean it must be accessible to authorized entities. [14]

Providing security to the data is not an easy task. A number of techniques have been developed which when combined together provide a high level of confidence that any information relating to the transaction that is received from the network.

Cryptography has become one of the main tools for privacy, trust, access control, electronic transactions, corporate security assistance and other countless fields. [6] Cryptology is the hiding of data so that it is unintelligible to those we do not wish to read it and intelligible to those we do. The art of devising cipher is cryptography and the art of breaking cipher is called crypt analysis. Cryptographers are the people who invent cipher. Crypt analysts are code breakers. The data which we are trying to hide is the information that we want to keep private. For instance, bank account numbers, social security numbers, military plans etc.

The most idea in cryptology is the idea of a cryptosystem. The first component of a cryptosystem is the original information set called the plain text. The next component of cryptosystem is the algorithm known as the Cipher. [9]

The main limitations on cryptography are ability of the code clerk to perform the obligatory transformations. Another limitation is switching quickly from one cryptographic method to another one. However, the peril of code clerk being confined by the enemy has made it essential to be able to alter the cryptographic method.

Only for encryption and decryption of message using secret keys, today it is defined in three distinct

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

mechanisms. Symmetric key encipherment, Asymmetric key encipherment and hashing.

In symmetric key encipherment an entity can send message to another entity over an insure channel where the hacker cannot understand the contents of the message. The user 1 encrypts the data and send message to user2. Then after receiving the message the user 2 decrypt the message where user 2 can view original data. This key uses single key for both encryption and decryption. In asymmetric key encipherment, we have the same situation as the symmetric key with few changes. Here two keys are used named public and private key. User 1first encrypts the message using public key. User 2 decrypts the message, using his/her own private key. In hashing a fixed length message digest is created out of a variable length message. This method is used to provide check values. Data encipherment involves a sending party. For example the application protocol entity in processing all data prior to transmission so that if it is accidental intercepted while it is being transferred it will be incomprehensible to the intercepting party. [11] The most encryption methods involve the use of an encryption key which is hopefully known only by the two correspondents, the key feature in both encryption and decryption process.

A cipher is a character-for-character or bit-for-bit transformation. A code replaces one word with another word. Initially four groups of people have used and contributed to the art of cryptography - lovers, military, diarists and the diplomatic crops. From these the military had the most important role within military organizations, the messages to be encrypted have traditionally been given to poorly paid, low - level cadre i.e., clerks for encryption and transmission purposes.[10]

The message to be encrypted, known as the plain text , are transformed by a function that is parameterized by a key. The output of the encryption process is known as the cipher text. It is then transmitted, by various media. However, unlike the intended recipient, the intruder (or) enemy does not know what is the decryption key and so he cannot decrypt the cipher text easily.[13] Occasionally the intruder can not only listen to the communication channel (Passive Intruder) but can also record the messages and play them back later, inject his own message (or) modify legitimate messages before they get transmitted to the receiver (Active Intruder). The art of breaking ciphers, called Cryptanalysis, and the art of devising them is collectively known as Cryptology. [7]

The need of encryption is to provide security of data that is free from intruders or hackers. The main motto is to provide security to data that is data should be unreachable to hackers. In order to ensure that security is properly provided we are making use of few algorithms. By performing encryption we are providing security to the data. Different algorithms are used accordingly to get the final encrypted data. [6] The main reason to perform encryption is to provide confidentiality and integrity to the data that is supposed to be accessed.

By performing encryption we are providing security to the data. Different algorithms are used accordingly to get the final encrypted data. The main reason to perform encryption is to provide confidentiality and integrity to the data that is supposed to be accessed. However the process of converting plain text to cipher text is encryption; restoring the plain text from cipher text is decryption. Technique used for decryption without any knowledge of the enciphering details which fall into the area crypt analysis.[4] In encryption, the algorithm performs various substitutions and transformations on the plain text. Where as in decryption, the algorithm runs reverse to the decryption. It takes cipher text and security key and produces original plain text. We need decryption to get the original data, which was encrypted. Here various algorithms are used to run this method.

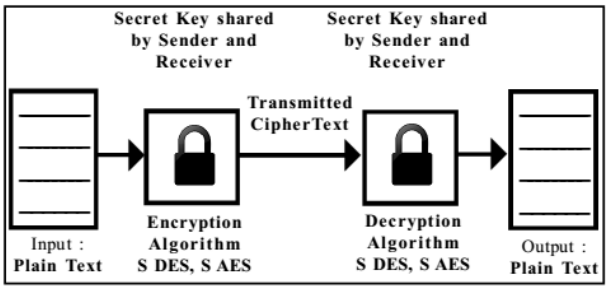

Figure 1: The systematic process of Cryptology.

Threat is a harm or danger. It can be mentioned in various ways according to the situations. It is a kind of an indication that something might take place. Threat can be either intentional or accidental. A threat can make serious harm in various ways or events. The most publicized threats to security are the intruder. There are 3 classes of intruders. **Masquerade** - He is an individual who is not authorized to use the computer, who penetrates a system's access controls to exploit a legitimate users account. **Misfeasor**- is a legitimate user who accesses data, programs or resources for which is authorized for such access but misuses his or her privileges. **Clandestine** user -is an individual who seizes the supervisory controls of the system and uses this control to evade auditing, access controls.

Breaching of security is done basically when security measures are not properly provided. Different security attacks methods are followed by hackers to get our confidential data.

The main motto of intruder is to gain access to the system or to increase the range of privileges accessible on a system. A system must maintain a file that associates a password with each authorized user. If such file is sorted with no protection, then it is easy to access and learn passwords. Password file can protect in two ways. One way encryption – system stores only an encrypted form of the user's password. The system performs a one way transformation in which the passwords is used to generate a key for the encryption function and in which a fixed length output is produces. Access control-access to the password file is limited to one or a very few account.

Attacks are basically classified into two types.

A) Passive Attacks
B) Active Attacks.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

In **Passive Attacks**, the goal of opponent is to obtain information which is transmitted through the network. There are two types of passive attacks. Release of message content which is easily understood. Firstly phone conversation, electronic mail message viz., the second is traffic analysis which is subtler. We had a traditional way of masking the message content or other information traffic so that even if the message is captured by opponents, they cannot extract the information from that message. Here we use the technique called encryption. The passive attacks are very complex to detect because they do not involve in any alteration of data.

Active attacks can be anyone of the following. They are Masquerade, Replay modification of message and Denial of service (DOS). A masquerade takes place when one entity pretends to be different entity. Replay involves the passive capturing of a data unit and its subsequent re transmission to produce an unauthorized effect. In Modification of messages attacks, some portion of a legitimate message is altered or delayed or recorded, to produce unauthorized effect. Denial of service prevents the normal use or management of communication facilities. This attack may have specific target. Active attacks are quite difficult because they are of wide variety potential, physical, software and network.

Intrusion detection is based on the assumption that the behaviour of the assumption that the behaviour of the intruder differs that of a legitimate user in ways that can be quantified. If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised. An effective intrusion detection system can serve as a deterrent, so acting to prevent intrusions. Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

II. RELATED WORK

In the field of information security various kinds of algorithm, like genetic evolution algorithm, adaptive are used. In [1] they proposed security for traffic information system using kernel principal component analysis (KPCA). It is to map the input vector to high dimensional space to extract to replace the inequality
constraint the non linear component and also support vector machine (SVM) model adopts equality constraint to replace inequality constraints.

In [2] this paper they published on RFID system focused on radio frequency indication security and have investigated on the limitations of tradition security solutions based on cryptographic primitives and protocols. To detect anomalous behaviour in the network and improved resilience to security attacks are proposed. To eliminate the redundancy KPCA was used. Here they proved KDD. In this the data is divided into five types. Based on those they are providing transportation information system.

On network intrusion detection [3] proposed two network intrusion detection techniques (IDS) a) C4.5 decision tree b) Ripper rules (RLD09 data set). These IDSs classify the network of service because of which unknown or new attacks will be found based on decision tree.

The paper published on design and implementation of campus network intrusion detection system [4] focused on the issue of data protection. In this author analysed the data to be protected using acquisition and data analysis module. A new methodology is proposed on security.[5] Providing security in reversibility. The data is encrypted by some image in some reverse order. Here they can achieve reversibility data and images are free from error.

III. PROPOSED SYSTEM

In this proposed system, the data which is being transmitted is subjected to encryption and decryption twice. Initially, the data is encrypted by the sender using **S-DES**. The obtained cipher text is transmitted to the local server, where the cipher text is again encrypted by the server using **S-AES**. Because of this dual encryption, the chance of data being misused during its transmission phase is very less thereby enhancing its security parameters. The local server at the receiver end decrypts the cipher text obtained from the local server at the sender's side. This obtained output on reaching the destination is decrypted by the receiver, where he can actually understand the received information.

The below block diagram explains the whole process used in the proposed system.

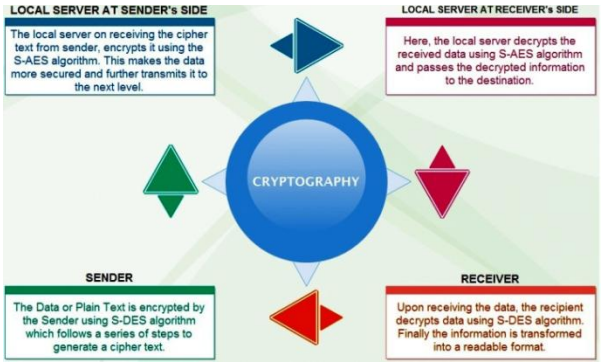

Figure 2: The process of double cryptography in the proposed system

The following are various operations performed during the whole process.

(I) THE PROCESS TAKING PLACE AT THE SENDER AND RECEIVER SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)

3.1 PERMUTATIONS

Permutations can be defined as the method of rearranging the bits of data wherever needed. The various permutations used in both encryption and decryptions are as follows:

- P1
- P2
- P3
- Expand and Per mutate (**EP**)
- Initial Permutation (**IP**)

DOI 10.17148/IJARCCE.2015.41041

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

- Inverse Permutation($\mathbf{IP^{-1}}$)

3.2 SHIFT OPERATIONS

We make use of two kinds of shift operations. They are:

- LSHFT-1 (Left Shift by one position)
- LSHFT-2 (Left Shift by two positions)

The other operation we make use during the process is **XOR.**

3.3 S-BOXES

In S-DES, substitutions are performed using S-Boxes.

- Each S-Box is considered as a matrix: input is used to select

a row/column; selected element is the output.

- It accepts a 4-bit input. (bit1,bit2,bit3,bit4)
- bit1 bit4 specifies row (0,1,2 or 3 in decimal)
- bit2 bit3 specify column
- Finally the output is 2-bit.

$$S0=\begin{bmatrix}01 & 00 & 11 & 10\\ 11 & 10 & 01 & 00\\ 00 & 10 & 01 & 11\\ 11 & 01 & 11 & 10\end{bmatrix} \quad S1=\begin{bmatrix}01 & 01 & 10 & 11\\ 10 & 00 & 01 & 11\\ 11 & 00 & 01 & 00\\ 10 & 01 & 00 & 11\end{bmatrix}$$

3.4 KEY GENERATION PROCESS

The following is the process of generating two 8-bit round keys K1 and K2. The keys K1, K2 are used as inputs in the encryption and decryption processes. Assume **K** as **10-bit input** key. The steps for generating the two 8-bit round keys K1 and K2 are:

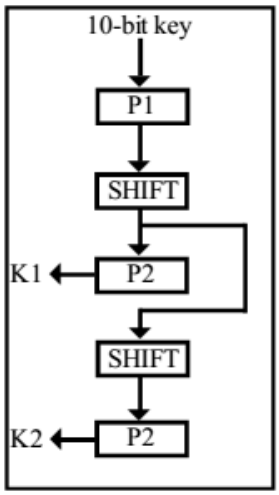

Figure 3: 10-Bit Key Generation.

1. Rearrange **K** using **P1**.
2. Left shift by 1 position both the left and right halves of key **'K'**.
3. Rearrange the halves with P8 to produce **'K1'**.
4. Left shift by 2 positions the left and right halves.
5. Rearrange the halves with P8 to produce **'K2'**.

3.5 ENCRYPTION PROCESS

Assume a **8-bit** plaintext, **P**. The steps for encryption are:

1. Apply the Initial Permutation, **IP** on Plain Text **P**.
2. Assume the input from step1 into two halves, L and R.
3. Expand and per mutate **'R'** using **E/P**.
4. XOR input from step 3 with **K1**.
5. Input left halve (L) of step 4 into S-Box S0 and right halve into S-Box S1

a. For S0: L as input: b1,b4 for row, b2,b3 for column.
b. For S1: R as input.

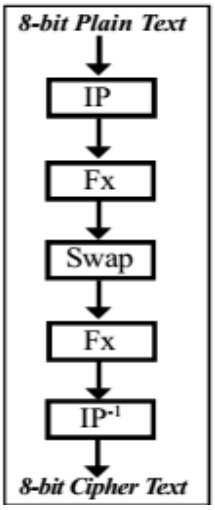

Figure 4: Encryption Process.

6. Rearrange outputs from step 5 using **P3**.
7. XOR output from step 6 with **L** from step 2.
8. Now we have the output of step 7 as the left half and the original R as the right half. Switch the halves and move to round 2.
9. E/P with right half.
10. XOR output of step 9 with **K2**.
11. Input to s-boxes.
12. Rearrange output from step 11 using **P3**.
13. XOR output of step 12 with left halve from step 8.
14. Input output from step 13 and right halve from step 8 into inverse IP.

Thereby the result is the encrypted text obtained from the plain text using a key.

3.6 DECRYPTION PROCESS

The process of decryption follows the same operations as mentioned in the previous encryption section. Here all the operations are to be performed in the reverse order of the above encryption process.

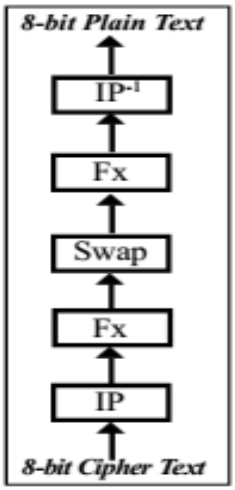

Figure 5: Decryption Process

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Decryption is performed using the same algorithm which is used in encryption, except that key K2 is used in the first round, the key K1 in the second round. All the other operations like permutations, shift operations remain the same.
Thus the output obtained from the decryption is plain text which is used as an input for the encryption process. The process of decryption is very important because it is very difficult for the recipient to understand the encrypted message which is in the binary format.

(II) THE PROCESS TAKING PLACE AT THE LOCAL SERVERS OF SENDER AND RECEIVER SIMPLIFIED ADVANCED ENCRYPTION STANDARD (S-AES)

The following are the various steps performed during the whole process that takes place at both the Local Servers. Let us assume the inputs for the encryption are:

- 16-bit Plaintext, PT.
- 16-bit Key, K.

3.7 KEY GENERATION

The first step is to generate the sub-keys. This is called **Key Generation** or **Key Expansion**.
The input key, **K**, is split into 2 parts, A0 and A1: The first sub-key, Key0= A0A1 = K.
The other sub-keys are generated as follows:
A2 = [A0 XOR 10000000] XOR [SubNib (RotNib (A1))]
A3 = A2 XOR A1
A4 = [A2 XOR 0011 0000] XOR [SubNib (RotNib (A3))]
A5 = A4 XOR A3
Therefore, the sub-keys are:
Key0 = A0A1
Key1 = A2A3
Key2 = A4A5

3.8 ENCRYPTION PROCESS

The following are the steps involved in encryption.
(I) Initial Operation or Add Round Key.
(II) Main round.
(III) Final round.
NOTE: The output of each operation is used as the input to the next operation, always operating on 16-bits. The 16-bits can be viewed as a state matrix of nibbles.

3.8.1 ADD ROUND KEY 0

Plain Text XOR **Key0**
Let us assume above R0 as output of the above operation.

3.8.2 ROUND1

A series of operations which are performed further are as follows:
1. Nibble Substitution (S-boxes):
Each nibble in the input is used in the Encryption S-Box to generate an output nibble. Consider input as **R0** and output as **R0'**.
2. Shift Row:
Swap 2nd nibble and 4th nibble.
3. Mix Columns:
Apply the matrix multiplication with the constant matrix,Me, using GF (2^4), For GF (2^4), the addition operation is simply an XOR, and for the multiplication operation you can user lookup table.

M = 1 4
4 1

S' = M x S
Output = S00' S10' S01' S11'
4. Add Round Key1:
Output XOR Key1.

3.8.3 FINAL ROUND

A series of operations are performed further same as above except Mix Columns.
1. Nibble Substitution (S-boxes) :
Each nibble in the input is used in the Encryption S-Box to generate an output nibble. Consider input as **R0** and output as **R0'**.
2. Shift Row:
Swap 2nd nibble and 4th nibble.
3. Add Round Key2:
Above Output XOR Key2.Assume the output as **'C'**.
Now we have the final **CIPHERTEXT.**

3.9 DECRYPTION PROCESS

Now let us perform decryption. Note that we use the same keys generated during the encryption (that is, the decryptor would generate the round sub-keys using the input key K, using the encryption S-Box).
The following are the steps involved in the process of decryption.
(I) Add Round 2 Key.
(II) Inverse Shift Row (same as normal)
(III) Inverse Nibble Substitution.
(IV) Add Round Key1
(V) Inverse Mix Columns
(VI) Finally Add Round Key 0.
After performing all the above said operations we obtain the required Plain Text.

IV. CONCLUSION

Now-a-days security plays a major role in the world. On performing single encryption hackers are capable of easily cracking the information which is being transmitted through the network. To overcome this problem we have proposed a new methodology which makes the unauthorized user unable to identify the information or crack the data in the network. First the data is encrypted in the local system and then sent to the local server, here the data is encrypted again. On the receiver's side, first the local server decrypts the received information and then the information is decrypted by the local system. Therefore, the user views the information in a secured way. The proposed methodology is used for transmitting the information in a secured manner.

REFERENCES

[1] Geethapriya Thamilarasu and Ramalingam Sridhar University at Buffalo, Buffalo, NY 14260-2000" Intrusion Detection in RFID Systems"
[2] Thanvarat komviriyavut, phurivit sangkatsanee, Naruemon Wattanapongsakorn and chalermpol charnsripinyo "Network Intrusion Detection and classification with Decision Tree and Rule Based Approaches" 978-1-4244-4522-6/094)

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

[3] Hu Ruipeng "Design and Implementation of Campus Network Intrusion Detection System".
[4] Yonghui Shi, Hui Li, Jun Bao, Zhongzhen Yan and Shengping Jiang "Research on the Improved SVM Model for Intrusion Detection of Transportation Information Security Systems"
[5] Kede Ma, Weiming Zhang, Xianfeng Zhao, Member, IEEE, Nenghai Yu, and Fenghua Li "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption"
[6] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled rfid device," in SSYM'05: Proceedings of the 14th conference on USENIX Security Symposium, 2005.
[7] L. Mirowski and J. Hartnett, "Deckard: A system to detect change of RFID tag ownership," International Journal of Computer Science and Network Security, vol. 7, pp. 89–98, July2007.
[8] M. Mitra, "Privacy for RFID systems to prevent and cloning," International Journal of Computer Science and Network Security, vol. 8, pp. 1–5, January 2008.
[9] J. Ayoade, "Privacy and RFID systems: Roadmap to solving security and privacy concerns in rfid systems," Computer Law and Security Report, vol. 23, no. 6, pp. 555–561, 2007.
[10] M. Rieback, B. Crispo, and A. Tanenbaum, "The evolution of RFID security," IEEE Pervasive Computing, vol. 5, pp.62-69, January–March 2006.
[11] T. Karygiannis, B. Eydt, G. Barber, L.Bunn, and T. Phillips,"Guidelines for securing radio frequency identification systems," NIST Special Publication 800-98, April 2007.
[12] Zhao Xi-bin, Jing Ran-zhe, Gu Ming. Adaptive intrusion detection algorithm based on rough sets. J Tsinghua Univ (Sci & Tech), 2008,48 (7): 1165-1168.
[13] V. N. Vapnik. The nature of statistical learning theory. 1st Edition, Berlin: Springer-Verlag, 1995.
[14] Ren Xun-yi, Wang Ru-chuan, Kong Qiang. Principal component analysis and support vectormachine based anomaly detection. Application Research GU Jun. Research on intrusion detection system based on KPCA and SVM. Journal of Computer Simulation, 2010, 27(7): 105-107.
[15] Wu De-hui. Nonlinear feature extraction method using LS-SVM and its relation with PCA. Journal of Chinese Computer Systems, 2008, 29(7): 1296-1300. Xiong Wen, Wang Cong. Hybrid feature transformation based on modified particle swarm optimization and support vector machine. Journal of Beijing University of Posts and Telecommunications, 2009, 32(6): 24-28.

BIOGRAPHY

E. Soumya, Completed her M.Tech from Kakatiya University, Warangal and she has 7 years of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is Network Security, Computer Networks, Data ware Housing.

Dr. R. Ch. A. Naidu completed his M.Tech, Ph.D from University of Mysore, Mysore and Andhra University, Vishakhapatnam respectively. He has more than 13 years of teaching experience. He is presently working in CSE Dept as a Professor in St Martin's Engineering College, Hyderabad. He has life membership in professional bodies like ISTE, CSI. His area of interest is Network security, Computer networks, Digital Image processing, Data base management systems.

A. Santhoshi completed her M.Tech from JNTU Hyderabad and she has 8 years of teaching experience. She is presently working in IT Dept as an Assistant Professor in St Martin's Engineering College, Hyderabad. Her area of interest is Network Security, Security in Big Data, Data ware Housing.

A S V R R Prasada, completed his B.Tech in Computer Science Engineering from JNTU-Hyderabad, preparing to pursue Masters in Computer Science (MS) with Database Systems and Data Mining as his primary area of concentration.