Significance of Finger Prints in Prevention of Cyber Crimes - An Approach

Bhavana Desai[1], Sachidananda Joshi[2]

[1]Junior Research Fellow, Dept of Criminology and Forensic Science, Karnatak Science College, Dharwad, Karnataka, India

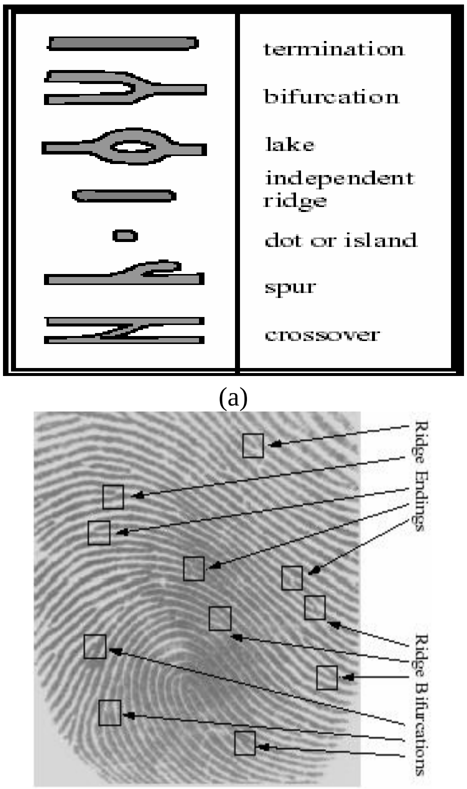
[2]Assistant Professor, Dept of Information Science, SDM College of Engineering and Technology, Dharwad, Karnataka, India

Abstract: ***With the development of science and technology human beings all over world live life of comfort and conveniently enjoy fruits there off. But people are being cheated by the misuse of Information Technology and the security of the Electronic Records is also at stake. Hacking or Unauthorized access to files or computer systems is one of the monsters existing in cyber space now a day. Here we are proposing an approach based on finger print identification where the files are transferred from a particular user using his finger print for authentication purpose. The Thinning algorithm is used for generating a unique key for each user. Proposed approach works such that user can select any type, any number of file he wants. The RSA algorithm is cryptographic encryptive algorithm used for encrypting the files. This algorithm uses two keys: Public and Private Key. Each user will be provided with this key pair. All the user information will be maintained in database. The main objective of this approach is transferring the file in encrypted format using finger print security which helps in preventing unauthorized access to important files by the other person***.

Keywords: Electronic records, Algorithm, Encrypt, Finger print, Unauthorized access, Authentication

1. Introduction

Using fingerprint for person identification is in practice from late nineteenth century which defined some of the points or characteristics from which fingerprints can be identified. These “Galton Points” referred to as ‘minutiae’ are the foundation for the science of fingerprint identification, which has expanded and transitioned over the past century. Fingerprint identification began its transition to automation in the late 1960s along with the emergence of computing technologies .With the advent of computers, a subset of the Galton points has been utilized to develop automated finger print technology. Fingerprint identification is one of the most well-known and publicized biometrics. Because of its uniqueness and consistency over time fingerprints have been used for identification for over a century, more recently becoming automated due to advancement in computing capabilities. Fingerprint identification is popular because of the ease in acquisition, the numerous sources available for collection and their established use and collections by law enforcement and immigration. Most automatic systems for fingerprint comparison are based on minutiae matching. Minutiae are local discontinuities in the fingerprint pattern. A total of 150 different minutiae types have been identified. In practice only *ridge ending* and *ridge bifurcation* minutiae types are used in fingerprint recognition. Examples of minutiae are shown in figure below.



(a)

(b)

Figure 1: (a) Different minutiae types, (b) Ridge ending & Bifurcation

Many known algorithms have been developed for minutiae extraction based on orientation and gradients of the orientation fields of the ridges. The building blocks of a fingerprint recognition system are:

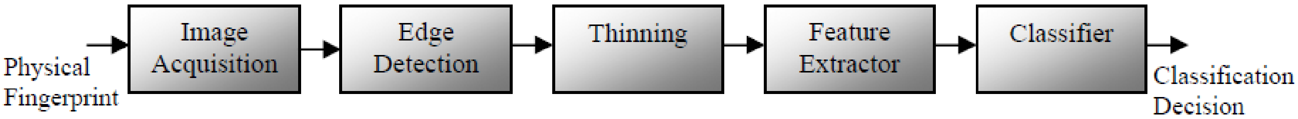


Figure 2: Fingerprint Recognition System

a) Image Acquisition

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process. Fingerprint quality is very important since it affects directly the minutiae extraction algorithm. Two types of degradation usually affect fingerprint images: 1) the ridge lines are not strictly continuous since they sometimes include small breaks (gaps); 2) parallel ridge lines are not always well separated due to the presence of cluttering noise. The resolution of the scanned fingerprints must be 500 dpi while the size is 300x300.

b) Edge Detection

An edge is the boundary between two regions with relatively distinct gray level properties. The idea underlying most edge-detection techniques is on the computation of a local derivative operator such as 'Roberts', 'Prewitt' or 'Sobel' operators. In practice, the set of pixels obtained from the edge detection algorithm seldom characterizes a boundary completely because of noise, breaks in the boundary and other effects that introduce spurious intensity discontinuities. Thus, edge detection algorithms typically are followed by linking and other boundary detection procedures designed to assemble edge pixels into meaningful boundaries [10]

c) Thinning

An important approach to representing the structural shape of a plane region is to reduce it to a graph. This reduction may be accomplished by obtaining the skeleton of the region via thinning (also called skeletonizing) algorithm. Hilditch thinning algorithm is widely used as a useful method of pre-processing in image process. There are two versions for Hilditch's algorithm, one using a 4x4 window and the other one using a 3x3 window. In this approach, the 3x3 window version is considered and the algorithm is described below.

A set of 8-neighbourhood of a pixel p0 is defined and the notation is shown as above.

P_4	P_3	P_2
P_5	P_0	P_1
P_6	P_7	P_8

$$N_8 \equiv \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8\}$$

$$N_{odd} \equiv \{p_1, p_3, p_5, p_7\}$$

Figure 3: A pixel of 8-neighbourhood

For the pixel p0, the aim of thinning algorithm is to decide whether to keep it as part of the result skeleton or delete it from the image. For this purpose, the 8 neighbors of pixel p0 must be investigated, when pixel p0 is part of a skeleton, pixel p0 will be deleted or not deleted according to the 5 conditions described below, the 5 conditions must be considered together. But during one path process, the value of pixel p0 should be set to another value such as –1 according to the Hilditch's algorithm; it will be set to 0 until all pixels in the image have been investigated during this path. Then this process is repeated until no changes are made. Before introduce the five conditions mentioned above, supposed for every pixel pi here i is from 1 to 8, its value of one pixel is represented by B (pi). The five conditions are described as below.

1. The pixel p0 is part of a skeleton.
2. It will not be deleted when pixel p0 is boundary of one skeleton.
3. It will not be deleted when pixel p0 is isolate pixel.
4. It will not be deleted when pixel p0 is a connective pixel.
5. Only one side will be deleted when the width of skeleton is two pixels.

d) Feature Extraction

Extraction of appropriate features is one of the most important tasks for a recognition system.

e) Classifier

Classifies the fingerprint images according to the location of minutiae.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data

2. RSA Algorithm

This Algorithm was proposed by by Rivest, Shamir & Adleman (RSA) in 1977. The RSA algorithm involves the use of two key:

- a public key, which may be known by anybody, and can be used to encrypt messages
- a private key, known only by the recipient, and used to decrypt messages

Operations of the RSA algorithm

i. Key generation: here key is generated based on randomly chose 2 prime numbers with the application of (Euler's totient function)

ii. Encryption: To encrypt a message the sender has to
- obtain public key of recipient (e; n)
- represent the message as an integer m in [0; n□1]
-compute: c = m (pow) e mod n

iii. Decryption: To decrypt the cipher text c the recipient
- uses his private key (d; n)
- Computes: m = c (pow) d mod n

3. Proposed Approach

3.1 Working Procedure

a. First step of implementation involves reading the fingerprint image from a .bmp, .jpg, .png file.
b. Pass the fingerprint image file to thinning algorithm to generate the key for user.
c. Design the client-server environment.
d. The server maintains the log of all the clients and the request from clients will be handled by the server.
e. Register the different clients by storing there information i.e. user name (Key) and key (generated by thinning algorithm) into the server database.
f. Validating the user at the time of user login.
g. If current user wants to transfer the files to other users, then encrypt those files using RSA encryption algorithm

and transfer them to server so that it can maintain the encrypted files.

h. The server intimates the list of the files to the corresponding user logged in when he wants to retrieve the files.

i. Once the client request for the files corresponding to him, transfer those files.

j. The file encryption and decryption happens at the client side. The encryption takes place by using public key of destination client and decryption takes place by using the ++++private key of destination client.

k. Finally, the user can sign out once he completes with his operations.

3.2 Block Diagram

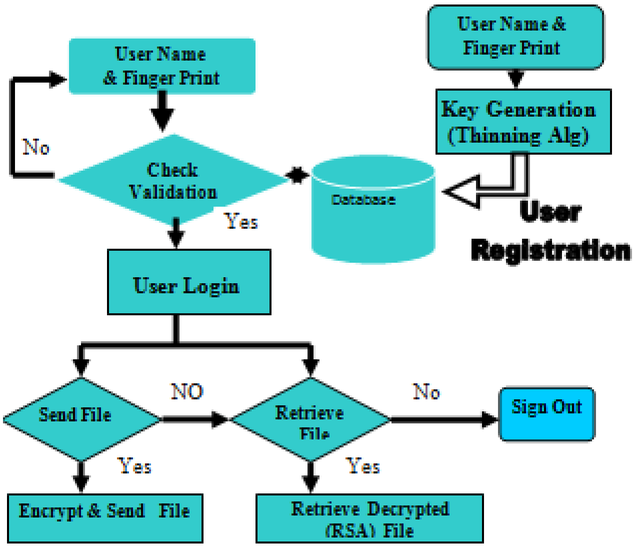


Figure 4: Block diagram of proposed approach

3.3 System Design

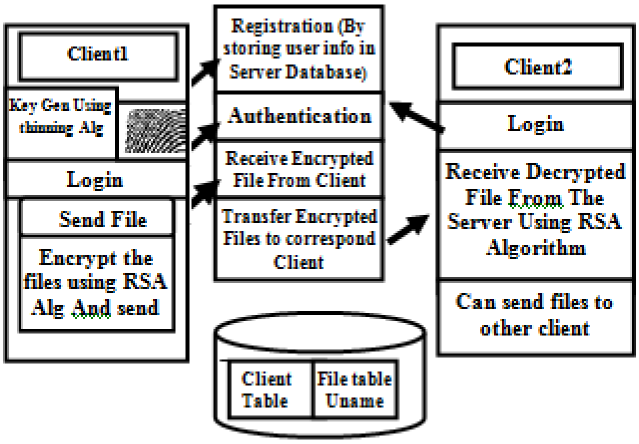
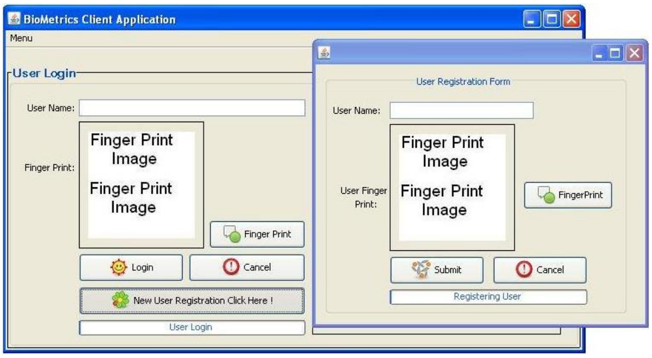

Client1
Key Gen Using thinning Alg
Login
Send File
Encrypt the files using RSA Alg And send
Registration (By storing user info in Server Database)
Authentication
Receive Encrypted File From Client
Transfer Encrypted Files to correspond Client
Client Table
File table Uname
Client2
Login
Receive Decrypted File From The Server Using RSA Algorithm
Can send files to other client

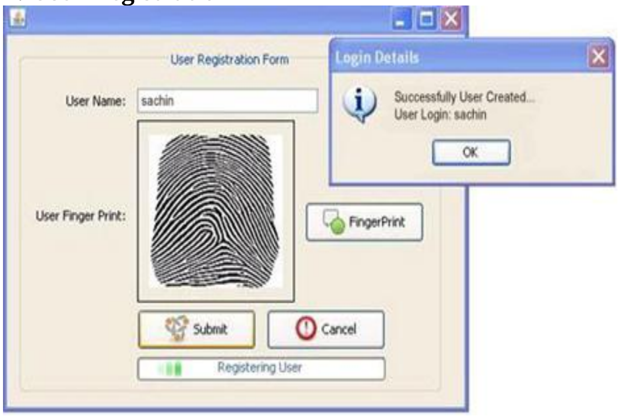
Figure 5: Proposed System Design

4. Results

1. Client User Interface



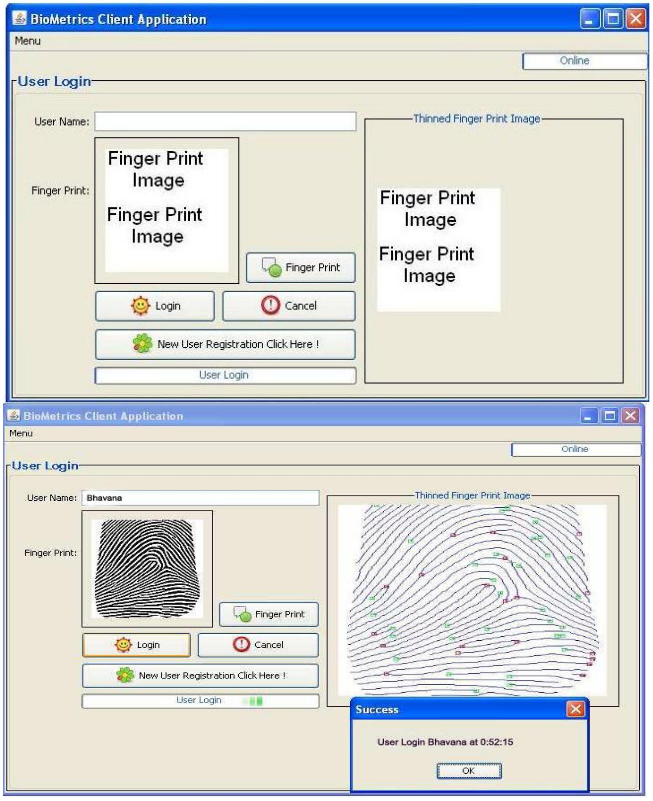
2. User Registration



User Name: sachin

Successfully User Created...
User Login: sachin

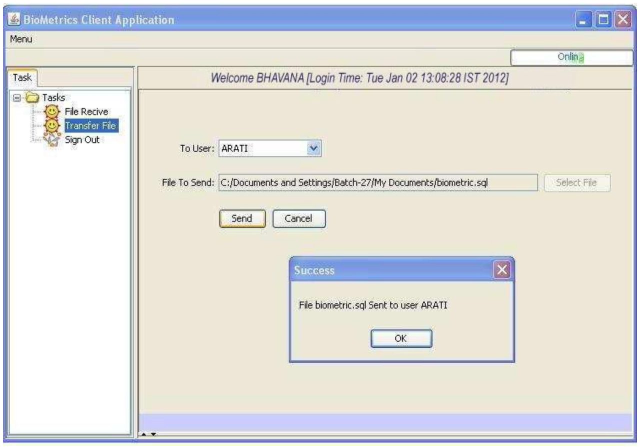
3. User Login



User Name: Bhavana

User Login Bhavana at 0:52:15

4. File Transfer



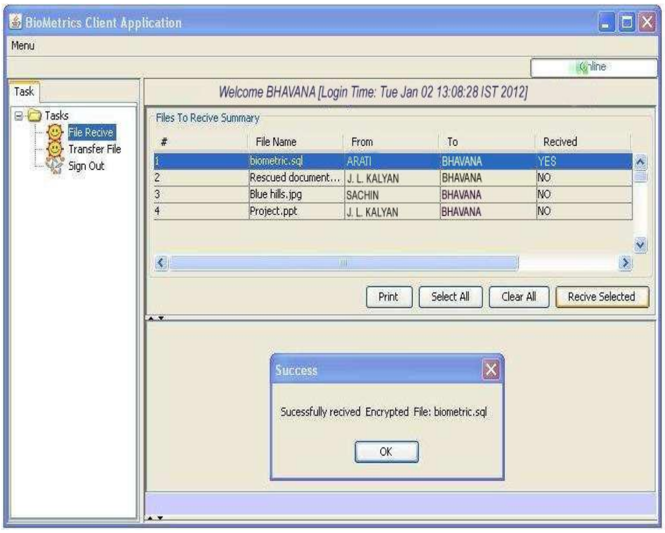
Welcome BHAVANA [Login Time: Tue Jan 02 13:08:28 IST 2012]

To User: ARATI

File To Send: C:/Documents and Settings/Batch-27/My Documents/biometric.sql

File biometric.sql Sent to user ARATI

5. File Receive



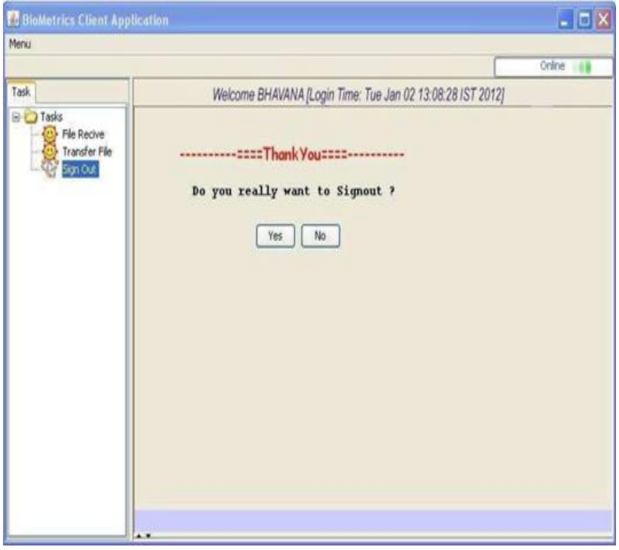
Welcome BHAVANA [Login Time: Tue Jan 02 13:08:28 IST 2012]

Files To Recive Summary

#	File Name	From	To	Recived
1	biometric.sql	ARATI	BHAVANA	YES
2	Rescued document...	J. L. KALYAN	BHAVANA	NO
3	Blue hills.jpg	SACHIN	BHAVANA	NO
4	Project.ppt	J. L. KALYAN	BHAVANA	NO

Sucessfully recived Encrypted File: biometric.sql

6. Sign Out

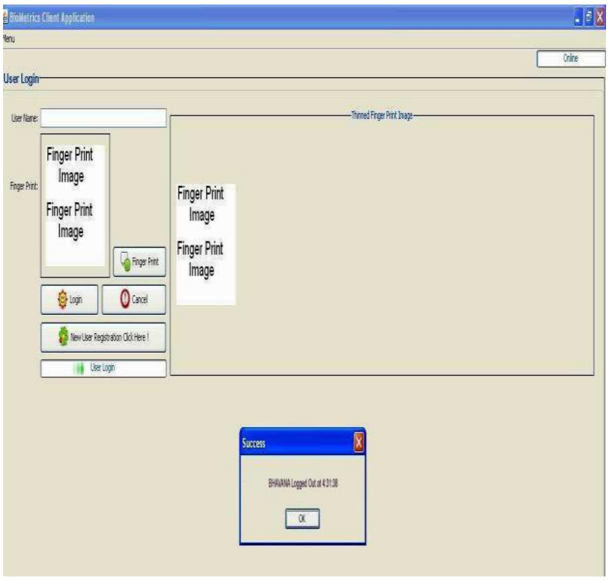


Welcome BHAVANA [Login Time: Tue Jan 02 13:08:28 IST 2012]

----------====ThankYou====----------

Do you really want to Signout ?

7. Logout Message



BHAVANA Logged Out at 4:31:38

5. Law Provisions Relating To Cybercrimes

Some important provisions relating to cyber crimes are dealt in Information Technology Act, 2000 (amended in the year 2008). Present paper is an approach to prevent hacking or unauthorized access to important files. Therefore we found it necessary to discuss some of the important provisions relating hacking and unauthorized access in brief.

The section 66 of IT Act deals with ‘hacking’. However, the scope and meaning of hacking under section 66 is much beyond mere ‘illegal access’ under IT Act. It states that whoever with the intent to cause or knowing that he likely to cause wrongful loss or damage to public or any person destroys or deletes or alters ant information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack. Thus, the emphasis for committing ‘hacking’ under the IT Act is effect on the information residing in the computer and any subsequent wrongful loss due to access rather than mere access to a computer itself If someone only accesses a computer system without authorization, he cannot be booked under section 66 of the IT Act. However, that does not mean that any person accessing without any right would go scot-free. The IT Act has dealt with unauthorized access in section 43(a) where the person accessing without authorization is liable to pay compensation. Any access to a computer without the permission of the owner or any other person, who is in charge, would entail civil consequences. There is no requirement of any actual damage, either data or information damage or computer damage, for liability under section 43(a), mere unauthorized access is enough. Hacking of a protected system is punishable under sec. 70 of the IT act. It would be an offence punishable with imprisonment of either description for a term, which may extend to ten years and shall also be liable to fine under subsection (3) of section 70[12].

6. Conclusion:

We have tried to implement a security system where a person can be authenticated by using his fingerprint which will be “The easiest way for the user to authenticate him and impossible way for Hackers to retrieve the files”. As we see the disadvantages of traditional password system. i .e. the passwords can be guessed or they can be hacked and the problem with remembering the passwords or carrying the ID cards etc can be overcome. Here in this approach there is no question of guessing passwords because the data used for authentication is a FINGER PRINT which never changes from life till death and differs with every individual. Therefore this approach helps prevent cyber crimes specially unauthorized access to certain important files by hackers.

One more important aspect of our approach is that all the files transmitted in the network will be in encrypted format. Hence the information transmitted will not be leaked. Since RSA is one of the best public key algorithm used in this approach the confidentiality level is substantially increased. One of the applications of this approach is that it can be used in organizations where the employees need to maintain highly confidential data with an authenticated precise security.

7. Future Enhancements

- In this approach there is no option for changing the password of a user (i.e. Fingerprint).Suppose if the user loses his fingerprint in an accident, it is possible that he may lose all his data. So a future development can be made by informing into Admin and getting it changed.
- The RSA Algorithm used here generates the key by itself. A facility to the user must be given so that he can choose his own key.

References

[1] Bruce. Eckel (2002), *‘Thinking in Java’*, Prentice- Hall, Inc, USA. (book style)
[2] Donald. Bales O’ Reilly (2002), ‘*Java Programming with Oracle JDBC’*, O’Reilly & Associates, Inc, USA. (book style)
[3] Elmasri & Navathe (2008), *‘Fundamentals of Database Systems’*, 5th Edition, Dorling Kindersley (India) Pvt Ltd, Delhi. (book style)
[4] http://en.wikipedia.org (online)
[5] http://time.imag.fr/mns/reasearch/finger/fingerprint (online)
[6] http://www.securitydatabase.com (online)
[7] Mary. Lourde R & Dushyant Khosla, *‘Fingerprint Identification in Biometric Security Systems’*, International Journal of Computer and Electrical Engineering’, Vol-2, Oct 2010. (journal style)
[8] Patrick Naughton & Herbelt Schildt (1999), *‘Java2, Complete Reference’*, McGraw Hill, USA. (book style)
[9] Prof. Vimlendu Tayal (2011), ‘Cyber Law, Cyber Crime Internet and E- Commerce’ Bharat Law Publications, Jaipur. (book style)
[10] Rafael. C. Gonzalez & Richard. E. Woods (2009), *‘Digital Image Processing’*, Dorling Kindersley (India) Pvt Ltd, Delhi. (book style)
[11] webfea.fea.aub.edu.lb/dsaf/labs/projectv1.1.pdf
[12] Information Technology Act. 2000

Author Profile

Smt. Bhavana. Desai, Junior Research Fellow, pursuing Ph. D in Forensic Science from Karnatak University, Dharwad, Karnataka. Her areas of interest are Finger Crime, Questioned Documents, Cyber Crimes etc

Sri. Sachidananda. Joshi., has secured B. E, M. Tec in Computer Science. He is presently working as Assistant Professor at SDM College of Engineering and Technology from Dharwad, Karnataka. His areas of interest are Network Security, Computer Networks.