SECURED FRAMEWORK FOR PERVASIVE HEALTHCARE MONITORING SYSTEMS

N Rukma Rekha[1] and Prof.M.S.PrasadBabu[2]

[1]Department of CIS, University of Hyderabad, India
rukmarekha@gmail.com
[2]Department of CSSE, Andhra University, India
msprasadbabu@yahoo.co.in

ABSTRACT

*'**Pervasive Healthcare Monitoring System (PHMS)**' is one of the important pervasive computing applications aimed at providing healthcare services to all the people through mobile communication devices. Pervasive computing devices are resource constrained devices such as battery power, memory, processing power and bandwidth. In pervasive environment data privacy is a key issue. In this application a secured frame work is developed for receiving the patient's medical data periodically, updates automatically in Patient Record Database and generates a Checkup Reminder. In the present work a light weight asymmetric algorithm proposed by the authors [26] is used for encrypting the data to ensure data confidentiality for its users. Challenge response onetime password mechanism is applied for authentication process*

KEYWORDS

Pervasive computing, Health Monitoring, Encryption, Light Weight Cryptography

1. INTRODUCTION

The recent advances in Science & Technology have changed the life style and provide prolonged life span of the people. Pervasive Computing is one such modern technology, which is slowly merging in to the background and makes the user least distracted about the technology [1]. Pervasive applications enable the user to make use of the advanced technology to improve his living standards everywhere and at every point of time. Pervasive applications enhance the user friendliness of a system with maximum automation and minimal user involvement. The most promising applications of pervasive computing are pervasive health care, smart homes, and transportation applications with the aid of vehicle sensors, national defense applications and environment monitoring systems. Pervasive healthcare applications include pervasive health monitoring, intelligent emergency management systems, pervasive healthcare data access, and ubiquitous mobile telemedicine [12]. This present work is focused on providing security solutions in pervasive healthcare monitoring systems.

The outline of this paper is as follows: An overview of the pervasive environment in health care applications that are available in literature and its security aspects are presented in Section 2. Proposed Pervasive Healthcare Monitoring (PHM) system and its architecture are given in Section 3 and Section 4. Section 5 discusses about the implementation details of the PHM system. Section 6 presents the performance analysis of the system. Concluding remarks are given at the end.

DOI : 10.5121/ijscai.2013.2203

2. RELATED WORK ON PERVASIVE HEALTHCARE SYSTEMS

Elham et.al [10] proposed a system on health care which is based on Electronic Medical Record database that coordinates application services over network to form a service environment for medical and healthcare. But every person in the system namely doctors, nurses and patients are supposed to carry an RFID tag to access the pervasive environment. Usage of RFID technology and implantation of different sensors and monitoring devices in the pervasive hospital system may not be feasible instantly.

Andre Canha et.al [11] dealt with two systems namely Altcare and SmartCondo for pervasive healthcare in smart home. They monitor every movement of the patient and store the data. Additional infrastructure such as installation of cameras everywhere in the home, maintaining data base of 2D and 3D pictures along with the privacy of the patient are debatable issues here.

Upkar Varshney [12] developed wireless patient monitoring system using wireless LANs and adhoc networks. Xiaohui Liang et al [13] introduced a Remote Health Monitoring (RHM) system which sends data from users wearable sensors to the personal server. Then, through any wireless connection, the data are sent through an internet gateway and the RHM servers, to a remote medical doctor's site for real-time diagnosis, and then updated in database.

Rusyaizila Ramli et.al [15] has proposed an architecture that can be used to develop a privacy-sensitive application for the end users where the users can frame their own privacy policies. Changyu Dong et.al [16] implemented a privacy preserving trust negotiation protocol using Extended Trust Target Graph (ETTG) protocol that establishes mutual trust between interacting parties if their access-control and disclosure policies comply.

Anastasios Fragopoulos et.al [17] developed a system using MPEG-21 Intellectual Property Management and Protection (IPMP) components which are used to protect transmitted medical information and enhance patient's privacy.

Munirul Haque et.al [19] discussed the various open issues in the security of pervasive computing. Importance of security and the role of authentication in a pervasive environment for the security of the data being communicated were discussed. Venkatasubramanian and Gupta [18] made a survey on security solutions for pervasive healthcare. They mentioned that cryptographic primitives may be used for securing data and for establishment of secure communication between two entities. Satyanarayanan [2] while discussing about the different challenges mentioned that privacy is the biggest thorn in pervasive environment.

RukmaRekha and M.S. Prasad Babu [26] have proposed a light weight asymmetric cryptographic algorithm suitable to pervasive applications and applied for SMS banking application. This paper mainly deals with application of light weight asymmetric cryptography algorithm, proposed in [26], to pervasive healthcare applications. In addition, a new authentication layer is introduced for PHMS. The features of the proposed system are given in the following sections.

3. PERVASIVE HEALTHCARE MONITORING SYSTEM (PHMS)

Pervasive healthcare monitoring applications provide continuous health monitoring to patients at high risk of falls and with chronic diseases such as cardiovascular disease, arthritis, diabetes, diminished hearing and eyesight, Parkinson's etc. [13]. Aged people, who are vulnerable to helplessness may also avail PHMS services by staying at home and is also relatively economical. By deploying body sensors on, or around the human body, the fundamental bio medical health parameters can be measured in a situation where diagnostic equipment and standard medical examination procedures are not available.

Mobile phones can be used as communication devices and the ubiquity of communication between mobile and healthcare server makes pervasive healthcare overcome time and location barriers. Cost of the health care being economical, accessibility of expert care to more people, making health care more personalized are the various reasons for the prominence of pervasive healthcare monitoring systems [8].

Medical information of the patients is highly sensitive data which needs data privacy as users will not compromise unauthorized access to their personal data [14]. Also pervasive health care solutions come with legal and ethical issues on inappropriate disclosure of user's personal medical data.

4. PROPOSED SYSTEM ARCHITECTURE

The proposed 'Pervasive Healthcare Monitoring System' is designed to maintain data confidentiality and data integrity along with authentication in a pervasive health environment. The proposed model operates in a computing environment consisting of a health care server and a remote ad-hoc network of handheld or portable pervasive computing devices (PDAs, laptop computers, and mobile phones). Based on limitations, it is assumed that pervasive device is a mobile phone, which is already possessed by most of the users. This eliminates the need for additional hardware device/ token for pervasive health care maintenance.

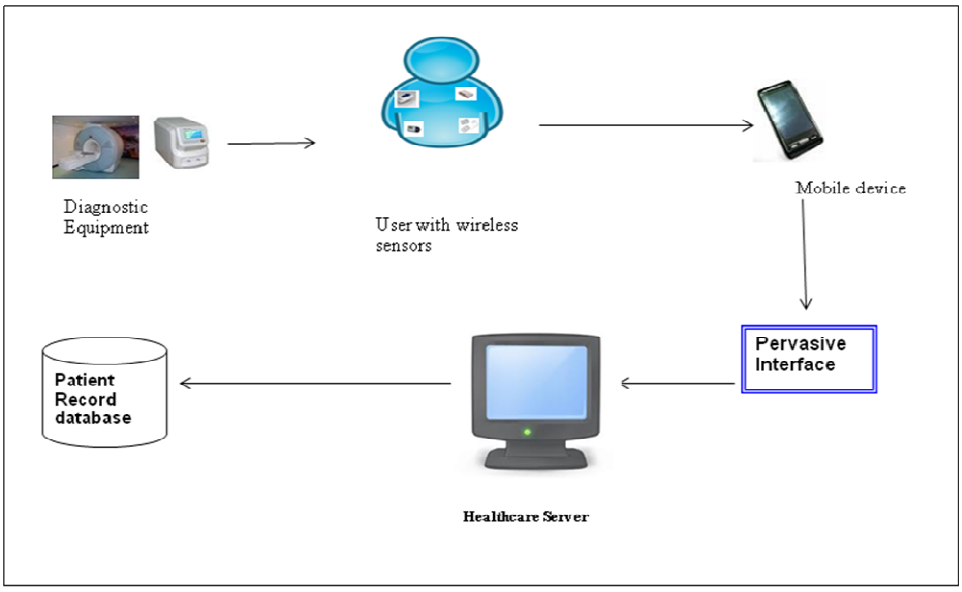

Fig1: Pervasive Healthcare Monitoring System Architecture

Fig1 shows the architecture of the proposed PHMS. The Components of PHMS are:
1. User with wearable sensors, 2. Pervasive Interface, 3. Mobile device, 4. Health Care Server (HCS), 5. Patient Record Database (PRD),
The HealthCare Server itself is comprised of three sub components namely Registered Patient List (RPL), Checkup Reminder (CR) and a security module which takes care of the encryption and authentication for ensuring data privacy. A pervasive interface may be designed which can transfer the (data) different signals emitted by different sensors (temperature sensor, body pulse, heart beat etc) arranged in, on or around human body and segregate them to user's mobile for transmitting the same to Patient Record Database through Healthcare Server.

The Registered Patient List contains the information of the patients along with their periodical check up dates. Whenever the system reaches that date a Checkup Reminder is generated for the patient. This Checkup Reminder is sent as a message to the pervasive device of the user. User on checking the message will upload his medical data collected based on other diagnostic services (such as MRI) as a message and encrypts it using the public key sent for his mobile. Along with the encrypted data the response generated from the random number is sent to the health care server.

The health care server decrypts the medical data using the private key generated at the time of key generation and updates the message received into the Patient Record Database. Since the data also involves in suggesting further medication for the user, there is at most necessity to ensure that the data is not altered and it came from the authenticated user.

5. IMPLEMENTATION DETAILS

The main steps in Pervasive Healthcare Monitoring System Implementation are: Registration, Encryption and Authentication.

Step1: Registration

All the users have to register with healthcare system. They have to enter their user name, mobile number and other information including proposed check-up dates. Then a unique user id is generated for each patient and this information is stored in the Registered Patient List (RPL list of the server. This Registered patient list contains the medical data of all the users and hence there is a need to protect this data. Authorized users are only allowed to access the data with the login access provided by the administrator. Whenever the system reaches the periodical check-up date a Check-up reminder containing patient id, patient name, check-up date is generated. This Check-up reminder is sent as a message to the user through mobile device.

Step 2: Encryption with Light Weight Asymmetric Encryption Algorithm

Doctors regularly monitor the updated values for diagnosis and suggest the patients either to continue with their medication or change their medication through mobile communication. In certain cases the patient may even be asked to go through some medical tests for further diagnosis or meet the doctor in person. When sending the message from the pervasive device to the Healthcare Server through a wireless network there is a chance for the attacker to perform over the air trade attacks or eaves dropping.

N.RukmaRekha and M.S.Prasadbabu [26] proposed a light weight asymmetric cryptographic algorithm which is quite suitable for a pervasive environment or resource constraint applications.

In case of symmetric cryptographic algorithm, key distribution is a major hurdle. If the key is compromised the attacker is likely to know all the further messages generated from the same key. Where as in an asymmetric algorithm, the message is encrypted with the public key and then transferred to health care server where it gets decrypted.

To perform asymmetric encryption a public key is sent to the user as a part of checkup reminders. The details of the algorithm are given below:

In this algorithm first an elliptic curve E is defined over Z_p (p is a prime, p>3), such that E contains a cyclic subgroup H in which the discrete log problem is intractable. Then it defines a key pair K= {(E,α,a,β): β=aα}; where α ε E. Now, the medical data generated by the user is converted to an elliptic curve point (x_1, x_2) and then it is encrypted using the public key (α, β) generated from the key generation step. The encrypted elliptic curve point (y_1, y_2) is then transferred to Healthcare Server and gets decrypted using the private key *a*. The decrypted point is again converted into message and then passed to Patient Record Database for updating.

Step 3: Authentication with Challenge Response One Time Password Method

Authentication is provided to the Healthcare system by using challenge response one time password mechanism. Here a random number, namely challenge, is generated at the time of Checkup Reminder generation and the user is supposed to generate a onetime password namely response, for that random number. Random number is generated using Blum Blum Shub algorithm. Blum Blum Shub takes the form: $x_{n+1}=x_n^2 \bmod M$, where $M=pq$ is the product of two large primes p and q. x_0 is a seed which is a quadratic residue modulo M. The cryptographic security of the Blum-Blum-Shub random generator algorithm is based on quadratic residuosity problem [27].

Generation of response involves calculation of an output value for the given challenge over any simple mathematical function. Only authorized user can evaluate the response because the mathematical function is known only to him, thus making the medical data transfer an authenticated transaction. Also, the mathematical function can be modified periodically if required.

6. PERFORMANCE ANALYSIS

Pervasive Healthcare Monitoring System meets all the requirements of data confidentiality, data integrity and authentication.

Authentication is assured by generating one time password (OTP) by using challenge response mechanism which is free from all traditional password attacks because of the randomness involved in it. OTP is generated by using Blum Blum Shub algorithm for each check-up reminder message and hence avoids the chance of having basic password attacks like brute force attack. Also Cryptanalysis doesn't help here because of the randomness of the password and hence there will be no specific relationship between the passwords generated for each message.

Data confidentiality and integrity are assured by encrypting the medical data using light weight asymmetric algorithm. The medical data is encrypted during the message transfer in order to avoid it from falling into attacker hands. Usage of standard encryption algorithms like DES, RSA is not feasible because of the resource constraints that we have for the pervasive devices. Standard cryptographic algorithms involve high computation and processing capability which

pervasive devices may not be able to bear for execution. Light Weight asymmetric encryption algorithms are used for minimizing the memory, power, and computational complexity. In this algorithm, the message data is transferred by converting it into an elliptic curve point. Advantage of elliptic curve cryptosystem is that encryption and decryption speeds up because of small key sizes and also there is memory and bandwidth savings. This reduces the computational and memory load on the mobile communication and offers as much security as a standard algorithm like RSA.

The performance features of PHMS are presented in table1 and compared with the existing frameworks that are available in literature.

Table1: Comparison of Performance features of PHMS with existing frameworks.

S.No	Framework	Encryption	Authentication	Additional Infrastructure Required
1	PCHS, Elham Rastegariet.al, [10]	No	No	Sensors, RFID Tags. Readers, Mobile Device
2	PHSH,André Canha, et.al, [11]	No	No	Sensors, Cameras, Display Devices, Mobile Device, 2D and 3D data
3	EPHCRM, Xiaohui Liang, Etal [13]	No	No	Sensors, Mobile Device, RFID Tags
4	SPCEHM, Shilpa Lakhina et.al, [20]	Yes	No	Remote Agents , Sensors, Mobile Device
5	PHMS	Yes	Yes	Sensors, Mobile Device

From Table1 it is evident that PHMS is more secured frame work than the others because it offers both encryption and authentication for the system. Also, in addition to sensors and mobile device, other infrastructure such as RFID tags, Readers, Cameras, Display Devices and Remote Agents are required for other frameworks whereas PHMS requires only sensors and mobile device and hence it uses minimal infrastructure.

The computational complexities of the different algorithms are computed and presented in Table2. Here, three features namely key size, brute force and attack time in years are compared for both traditional and light weight symmetric and asymmetric cryptographic algorithms.

Table2: Comparison of key size, brute force complexity and attack time in years with existing algorithms.

S. No	Algorithm	Key size	Brute Force	Attack time in years
1	Symmetric	112	2^{1126}	$1.37X\ 10^{11}$
2	Asymmetric	1024	2^{1024}	$2.40X10^{17}$
3	Light weight symmetric	80	2^{80}	$2.4\ X10^{9}$
4	Light weight Asymmetric	160	2^{160}	$5\ X10^{10}$

Graphical representation of the above results are represented in fig 2

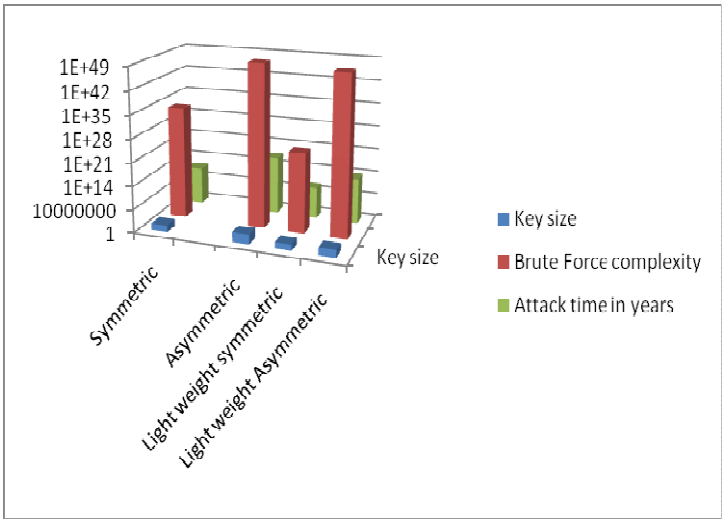

Fig2: Graphical representation of Comparison of key size, brute force complexity and attack time in years with different algorithms

In the graph presented in Fig 2, X-axis represents the three features of different algorithms and Y-axis represents the numbers in billions. Blue color represents the key size of the algorithm, red color represents brute force complexity, and green color represents attack time in years. The following are the observations.

The first observation is that the key size of light weight asymmetric algorithm is less compared to traditional symmetric and asymmetric algorithms. But, it is relatively more compared to light weight symmetric algorithm. Second observation is that the time taken to attack light weight asymmetric algorithm is almost close to traditional asymmetric algorithm and is more than the traditional symmetric and light weight symmetric algorithms. Third observation is that the brute force complexity of light weight asymmetric algorithm is more compared to both traditional and light weight symmetric algorithms and it is less when compared to traditional asymmetric algorithm This is because of the huge key size. Hence it can be concluded that despite the small key size the present light weight asymmetric algorithm gives more security than other traditional algorithms in the resource constrained environment.

7. CONCLUSION

Pervasive Healthcare Monitoring System was developed for continuous health monitoring of patients who are having long term diseases. Medical data of user is transmitted to the Healthcare Server using mobile communication. It is shown in Section 6 that the main advantage of this system is that data privacy of the user is more compared to existing algorithms. PHMS also assures the authentication of the user such that only authorized user will send the data.

REFERENCES

[1]. Mark Weiser, The Computer for the 21st Century, Scientific American, September 1991

[2]. M.Satyanarayanan, Pervasive Computing Vision and Challenges, IEEE Personal Communications,2001

[3]. Andreas Butz, Antonio Kr¨uger, User-centered development of a pervasive healthcare application, " *Pervasive Health Conference and Workshops, 2006* , vol., no., pp.1-8, Nov. 29 2006-Dec. 1 2006

[4]. Jurgen Bohn, Felix G¨artner, and Harald Vogt, Dependability Issues of Pervasive Computing in a Healthcare Environment, Proceedings of the First International Conference on Security in Pervasive Computing, volume 2082 of Lecture Notes in Computer Science,2003, pages53-70, Springer-Verlag

[5]. Jakob E. Bardram, Hospitals of the Future – Ubiquitous Computing support for Medical Work in Hospitals, In UbiHealth 2003: The 2nd International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications. (2003)

[6]. Rifat Shahriyar, Md. Faizul Bari, Gourab Kundu, Sheikh Iqbal Ahamed, and Md. Mostofa Akbar , Intelligent Mobile Health Monitoring System (IMHMS), International Journal of Control and Automation, Vol.2, No.3, September 2009

[7]. Jong Hyun Lim, Andong Zhan, Andreas Terzis, Poster: HealthOS: A Platform for Integrating and Developing Pervasive Healthcare Applications, MobiSys'11, June 28–July 1, 2011, Bethesda, Maryland, USA. ACM 978-1-4503-0643-0/11/06.

[8]. Gaetano Borriello, Vince Stanford, Chandra Narayanaswami, Walter Menning, Pervasive Computing in Healthcare, IEEE Pervasive Computing 2007

[9]. Vince Stanford, Pervasive Healthcare Applications face tough Security Challenges, IEEE Pervasive Computing 2002

[10]. Elham Rastegari, Amirmasood Rahmani, Saeed Setayeshi, Pervasive Computing in Healthcare Systems, World Academy of Science, Engineering and Technology 59, 2011

[11]. André Canha, Mauro Gama, Rui Monteiro, Pervasive Healthcare in Smart Homes, http://www.ee.oulu.fi/~vassilis/courses/ubicomp10S/projects/11_healthcare.pdf

[12]. Upkar Varshney, Pervasive Healthcare and Wireless Health Monitoring, Mobile Network Applications (2007) 12:113–127 , Springer

[13]. Xiaohui Liang, Xu Li, Mrinmoy Barua, Le Chen, Rongxing Lu, Enable Pervasive Healthcare through Continuous Remote Health Monitoring, IEEE Wireless Communications, vol. 19,no.6, 2012, pages 10-18.

[14]. X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for ehealth systems," IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365-378, 2009.

[15]. Rusyaizila Ramli, Nasriah Zakaria, Putra Sumari, Privacy Issues in Pervasive Healthcare Monitoring System: A Review, World Academy of Science, Engineering and Technology, 48, 2010

[16]. Changyu Dong and Naranker Dulay, Privacy Preserving Trust Negotiation for Pervasive Healthcare, Pervasive Health Conference and Workshops, 2006 In Pervasive Health Conference and Workshops, 2006 (2006), pp. 1-9

[17]. Anastasios Fragopoulos, John Gialelis, and Dimitrios Serpanos , Security Framework for Pervasive Healthcare Architectures Utilizing MPEG21 IPMP Components, International Journal of Telemedicine and Applications , Volume 2009, Article ID 461560, 9 pages

[18]. K. Venkatasubramanian and S. Gupta, "Security for pervasive healthcare," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, chapter 15, pp. 349–366, CRC Press, Boca Raton, Fla, USA, 2007.

[19]. Munirul Haque and Sheikh Iqbal Ahamed, Security in Pervasive Computing: Current Status and Open Issues, International Journal of Network Security, Vol.3, No.3, PP.203–214, Nov. 2006

[20]. Shilpa Lakhina , Zeenat Mahmood , Sarwesh Site, Secure Pervasive Computing Environment for Health Monitoring, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1 , Issue 2

[21]. Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle, Security for Pervasive Healthcare, *Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International* , vol., no., pp.1-2, 13-16 July 2009

[22]. Pardeep Kumar and Hoon-Jae Lee, Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey, *Sensors* 2012, *12*, 55-91

[23]. Sheikh I Ahamed, Nilothpal Talukder, and Achilles D. Kameas, Towards Privacy Protection in Pervasive Healthcare, In Proceedings of the 3rd IET International Conference on Intelligent Environments, Ulm, Germany, p.269-303 (2007)

[24]. Yanmin Zhu, Morris Sloman, Emil Lupu, Sye Loong Keoh, Vesta: A Secure and Autonomic System for Pervasive Healthcare, 3rd Int. Conference on Pervasive Computing Technologies for Healthcare (Pervasive Health 09), London, April 2009.

[25]. N.RukmaRekha, M.S.PrasadBabu, Design and Development of Light Weight Asymmetric Cryptographic Algorithm – An Implementation of SMS Banking System, International Journal of Computational Intelligence and Information Security (IJCIIS) , ISSN:1837-7823, Vol. 3 No. 10 December 2012, Pages 30-35

[26]. J. P. Black, W. Segmuller, N. Cohen, B. Leiba, A. Misra, M. R. Ebling, and E. Stern, Pervasive Computing in Health Care: Smart Spaces and Enterprise Information Systems, Proceedings of the MobiSys 2004 Workshop on Context Awareness, Boston, (June 2004)

[27]. http://www.cs.miami.edu/~burt/learning/Csc609.062/docs/bbs.pdf

Authors

Ms.N.RukmaRekha obtained her B.Tech, M.Tech degrees from Andhra University in 2003 and 2005 respectively. Currently, she is pursuing her Ph.d as part-time from the same university. She has around 7 years of teaching experience. She has the experience of guiding around 16 Post graduate students for their M.Tech/M.C.A Project Thesis. Ms. Rukma Rekha is now Assistant professor from school of Computer and Information Sciences in University of Hyderabad.

Prof. Maddali Surendra Prasad Babu obtained his B. Sc, M.Sc and M. Phil and Ph.D. degrees from Andhra University in 1976, 1978, 1981and 1986 respectively. During his 29 years of experience in teaching and research, he attended about 28 National and International Conferences/ Seminars in India and contributed about 33 papers either in journals or in National and International conferences/ seminars. Prof. M.S. Prasad Babu has guided 98 student dissertations of B.E., B. Tech. M.Tech. & Ph.Ds. Prof Babu is now Professor in the Department of Computer Science & Systems Engineering of Andra University College of Engineering, Andhra University, Visakhapatnam. Prof. M.Surendra Prasad Babu received the ISCA Young Scientist Award at the 73rd Indian Science Congress in 1986 from the hands of late Prime Minister Shri Rajiv Gandhi. Prof. Babu conducted the proceedings of the Section of Information and Communication & Sciences and Technology including computer Science of the 94th Indian Science Congress as a president of that section in January 2007. Prof. Babu was also the sectional committee member of the Indian Science Congress in the sections of Mathematics and ICT in 1988 and 2005 respectively. He is also sectional secretary for the section of Information and Communication & Sciences and Technology of Indian Science Congress. He is currently professor and chairman, Board of Studies at Andhra University.