IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, p-ISSN: 2278-8719, www.iosrjen.org
Volume 2, Issue 10 (October 2012), PP 16-22

Prevention of Attacks in internet controlled Embedded Applications

[1]Prof.P.Rama Bayapa Reddy,[2]Dr.K.Soundararajan,[3]Dr.M.H.M.Krishna Prasad
[1]*Professor, Dept. of CSE, Dhruva Institute of Engineering and Technology, Hyderabad, India,*
[2] *Professor, Department of ECE, JNTUACE, of Jawaharlal Nehru Technological University College of Engineering, Anantapur, A.P, India,*
[3]*Associate Professor of CSE & Head, Dept. of Information Technology University College of Engineering JNTUK – Vizianagaram, A.P, India.*

Abstract: *Embedded systems are becoming a main solution to many specific tasks because of this high stability, minimal power consumption, portability and numerous useful. Nowadays, many new applications are developed using embedded system. This paper deals with the issues related to embedded applications when they are implemented in internet. There are various attacks in embedded systems when implemented in the internet. These attacks have a negligible effect in the operating system which results in the decrease in the system performance. But in embedded system case, it has life and death consequence attached to it. Many of these embedded systems work in hazardous environment where a system failure results to catastrophic effects. Here a study of various attacks are discussed and a new architecture has been proposed to secure Web based embedded systems from the attacks.*

Keywords*: Embedded systems, Web, Internet, attacks, secured layer, Computer Security, DDoS Attack*

I. INTRODUCTION

Embedded system is a system that is designed to serve specific tasks. Almost all embedded systems come in compact size, so users are able to use them as additional parts to other devices or to construct specific applications with them. Embedded systems have many advantages like high efficiency, long life usage, and economical energy consumption. Embedded systems have become ubiquitous as can be found in many new devices and systems such as cellular phones, PDAs and wireless networks. Older technologies also reap the benefits of embedded processing, for example a typical automobile now includes two–dozen microprocessors [1], Over 98% of all microprocessor are now deployed in embedded systems [2]. Unfortunately, security research targeting resource–constrained distributed embedded systems has not kept pace with the growing application of embedded systems. Distributed Denial of Service (DDoS) attacks continue to be a prominent threat to cyber infrastructure. A DDoS attack [3, 4] involves multiple DDoS agents configured to send attack traffic to a single victim computer to exhaust its resources. DDoS is a deliberate act that significantly degrades the quality and/or availability of services offered by a computer system by consuming its bandwidth and/or processing time. As a result, the legitimate users are unable to have full quality access to a web service or services. This may also include data structures such as open file handles, Transmission Control Blocks (TCBs), process slots etc. Because of packet flooding in a DDoS attack that typically strives to deplete available bandwidth and/or computing resources, the degree of resource depletion depends on the traffic type. DDoS attacks today are part of every internet user's life. The sole purpose of DDoS attacks is to disrupt the services offered by the victim. DDoS attacks can take several forms and can be categorized by several parameters, which can be classified based on how they affect a victim computer or based on how they are generated [5]. According to Computer Emergency Response Team Coordination Center (CERT/CC) [6], there has been an increase in use of Multiple Windows based DDoS agents. There has been a significant shift from UNIX to Windows as an actively used host platform for DDoS agents. Furthermore, there has been increased targeting of windows end-users and servers. The CERT/CC published a tech tip entitled "Home Network Security" in July of 2001 [7] to raise awareness of such vulnerabilities. According to the CERT/CC [6], there is a perception that windows end-users are generally less security conscious, and less likely to be protected against or prepared to respond to attacks compared to professional industrial systems and network administrators. Furthermore, large populations of windows end-users of an Internet Service Provider are relatively easy to identify and hence the attackers or intruders are leveraging easily identifiable network blocks to selectively target and exploit windows end–user servers and computer systems. There are a number of security algorithms which prevent attacks when Web services are implemented. In general purpose operating systems, there are hardly a handful of algorithm which prevents Web attacks in Embedded systems. This paper gives a general study of various attacks that

happens in Web based embedded systems. Dong Haung [1] proposed a new ontology for representing security constraints as policy and a semantic policy framework for the management of the policies. The growth of internet has accompanied the growth of e services which resulted in increasing attacks on them by malicious individuals. The authors [4] highlighted the need of security.

II. RELATED WORK:

The conceptions about security of Web services and Degree of Safety for Web Services (WS-Dos), and the duration of Web service execution time, are introduced in the paper. In addition, a securing logical hierarchical structure for Web Service application based on an extended Web Services security architecture model with five elemental objects, such as resources, services, roles, protocols and methods object is analyzed Moreover, an integrated security solution has been developed and the results of application showed that the solution builds a confidence and authentication security environment for all roles in the process of dynamic B2B trade [8]. The authors [5] sketched the MAWeS architecture, illustrating how to use it to optimize the performance of a typical compound Web Services application while at the same time guaranteeing that a set of security requirements, expressed by a security policy, are met.Chen el al [6] aimed at clarifying security concern by conducting a quantitative performance evaluation of WSS overhead. Based on the evaluation, an extension of the existing Web services performance model is made by taking the extra WSS that overheads into account. The extended performance model is validated on different environments with different messages sizes and WSS security policies. Micheal lesk et al [7] explained Web Service security in a federated environment that describes how the Web services are implemented and are secured in a Web environment Kevin [2] described the objective of improving Internet messaging by redesigning it as a family of Web services, an approach that is call WSEmail. This paper illustrated architecture and describe some applications. Since increased flexibility often mitigates against security and performance, here the steps for proving security properties and measuring the performance of the system with its security operations are focussed. The authors proposed [3] an agent based policy aware framework for Web Services security. In this framework, a policy language called ReiT which is a declarative language based on the rules and ontology is introduced. The non-structural knowledge is represented by rules and the structural temporal knowledge is represented by ontology Moreover, the authors propose a mixed reasoning mechanism to evaluate the ReiT policy. The access control policy including the context of the user and Web Services is evaluated by the reason or in addition, policy aware BOID agent to authorize the access control of the Web Service is presented. And the authors implemented the policy aware of BOID agent by extending the JADE platform.

III. PRIVACY AND SECURITY ISSUES

While the above mentioned technologies can help improve overall quality of health care delivery, the benefits of these technologies must be balanced with the privacy and security concerns of the user. Data from in-home sensors and medical records will be communicated electronically via the Internet and wireless transmissions. This increases the danger of compromising the security and privacy of individuals which we analyze in this section.

A. Data Access and Storage

There has long been concern over a patient's health record privacy and confidentiality [5]. Connecting personal health information to the Internet exposes this data to more hostile attacks compared to the paper-based medical records. Currently, patients have to physically go into a health care facility to get their medical record. Since the records are in paper format, this physically limits the number of people who see the record and how it gets transmitted. [6]However, once this information is available electronically, it opens the door for hackers and other malicious attackers to access the records as well as those who are authorized.

3.1Study of various attacks in Real Time Embedded Systems Denial of service and distributed denial of service attacks.

As shown in fig1 a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack)[7] is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Propagators of DoS attacks typically target sites or services hosted on high-profile Web servers such as banks, credit card payment gateways, and even root nameservers.

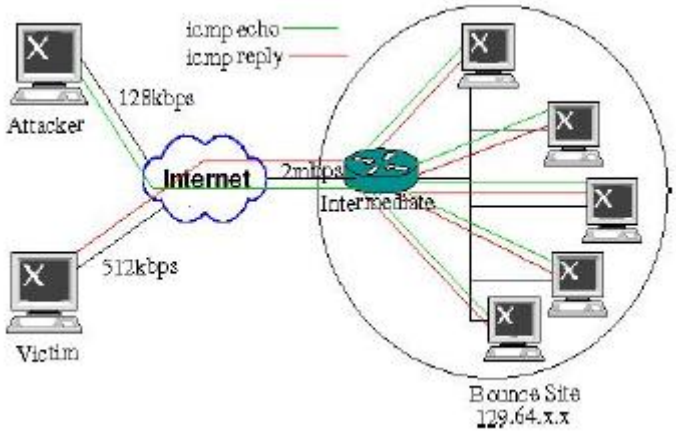

Fig1:Dos attack system

Both ICMP echo request and ICMP echo reply messages are used in Smurf Attack. A perpetrator sends a large amount of ICMP echo (ping) traffic to the IP broadcast addresses, all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses perform the IP broadcast to layer 2 broadcast functions most host on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. If the broadcast domain has N number of computers then for each echo request message sent to the broadcast domain, N number of echo reply messages are generated and sent not to the original sender but to the victim's computer (due to the spoofed source address in the ICMP echo request messages). In effect, the broadcast domain helps amplify and direct the DDoS attack traffic towards a victim computer. If more than one broadcast domains are involved then such DDoS attack traffic can be amplified even further and the victim computer is flooded with a large number of ICMP echo reply messages resulting in bandwidth exhaustion and also the resource exhaustion of the victim computer.

IV. ICMP CONNECTIVITY

The term is generally used with regards to computer networks, but is not limited to this field, For example, it is also used in reference to CPU resource management. One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. [8]In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.One step ahead, DDos does is capable of doing more harm. With this, attacker can use the victims system to infect other connected systems or send a spam. Attacker can find a weakness in the system and can inject a malware or software which can be remotely used by using this, now attacker can make the server "a slave" and send spams or get access to files using its permission. Thousands of system can be targeted from a single point.

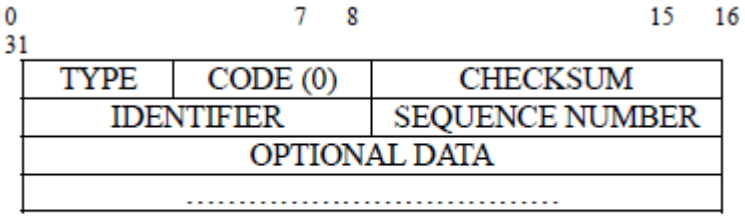

Fig2:ICMP Echo request/reply message format

The attacker sends a stream ICMP echo packets to the router at 128kbps. The attacker modifies the packets by changing the source IP address to be that of the victim's computer so replies to the echo packets will be sent to the address. [9]The destination address of the packets is a broadcast address of the so-called bounce site.DOS and DDOS can also happen in embedded systems since the malicious hacker can gain access to the embedded Web server and use all the server resources such as limited bandwidth which in turn leads to denial of service for legitimate embedded client from accessing the service

4.1THREAT FROM KEY LOGGING.

Keystroke logging (often called keylogging) is an action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware and software-based approaches to electromagnetic and acoustic analysis. The users in the embedded Web client must ensure that their keystroke logging must not be tracked by an imposter. The snooper can gain entry if he is able to track the key logging of the end user.

4.2 IP SPOOFING.

IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system or an embedded device.

4.3 BUFFER OVERFLOW

A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. [10]This may result in erratic program behavior, including memory access errors, incorrect results, program termination (a crash), or a breach of system security. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. They are thus the basis of many software vulnerabilities and can be maliciously exploited. Bounds checking can prevent buffer overflows. Programming languages commonly associated with buffer overflows include C and C++, which provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array which (the built-in buffer type) is within the boundaries of that array In embedded system this attack poses a greater threat since embedded systems will only allocate a small amount of memory. So any small type of this attack may lead to overflow of buffer at end user side and hence the system will crash

4.4 FORMAT STRING ATTACK.

Format string attacks are a class of software vulnerability. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write the number of bytes formatted to an address stored on the stack This type of attack is also common in embedded systems which causes the embedded systems to crash

4.5 SQL INJECTION ATTACK.

SQL injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. [11]It is an instance of a more general class of vulnerabilities that can occur whenever one programs or scripts the language that is embedded inside another. SQL injection attacks are also known as SQL insertion attacks.

V. EMBEDDED SECURITY SCAN DETECTOR POSSIBLE DEPLOYMENT

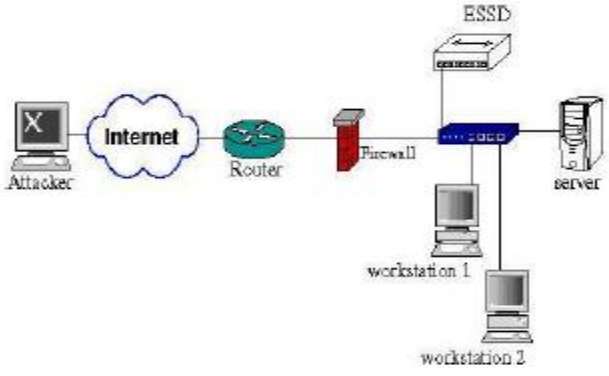

FIG3:Embedded Security Scan Detector

The system is called Embedded Security Scan Detector (ESSD) and its task is to ensure security through incorporation of Smurf Attack Detection. Figure 4 shows a possible deployment of the Embedded Security Scan Detector. Assuming the router and firewall permit ICMP echo requests and echo replies out of the network, and ESSD is connected with configured monitor switch port from [12]where this new system can detect abnormal behaviors and also the other systems are connected to the switch. The system is user programmable, meaning the user has the flexibility of choosing the ports that he/she would like to peep into looking for any possible malicious attack activity. The SBC which comply with the embedded PC standard, a commonly-used robotic development platform [9, 10], has a main board of approximately 4 by 4 inches that houses a processor, memory and the basic chipset needed to function as a standalone embedded computer capable of functioning with only a separate power supply and whatever outside input or output devices the application calls for. The embedded PC allows the use of an 802.11b (Wi-Fi) and wired Ethernet that provide high-speed two way communications link between the system and PC Database Server.

5.1 CROSS SITE SCRIPTING.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications that enables malicious attackers to inject client-side script into Web pages viewed by other users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on Websites were roughly 80% of all security vulnerabilities documented by Symantec as in 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site's owner.

5.2 VIRUS AND WORMS.

A virus is a program that can copy itself and infect a computer or any embedded device. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance a user can sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. [13]Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer. As stated above, the term "virus" is sometimes used as a ‘catch-all’ phrase to include all types of malware, even those that do not have the reproductive ability. Malware includes computer viruses, computer worms, Trojan horses, most rootkits, spyware, dishonest adware and other malicious and unwanted software, including true viruses. Viruses are sometimes confused with worms and Trojan horses, which are technically different. A worm can exploit security vulnerabilities to spread itself automatically to other computers through networks, while a Trojan horse is a program that appears harmless but hides malicious functions. Worms and Trojan horses, like viruses, may harm a computer system data or performance. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious or simply do nothing to call attention to themselves. Some viruses do nothing beyond reproducing themselves.

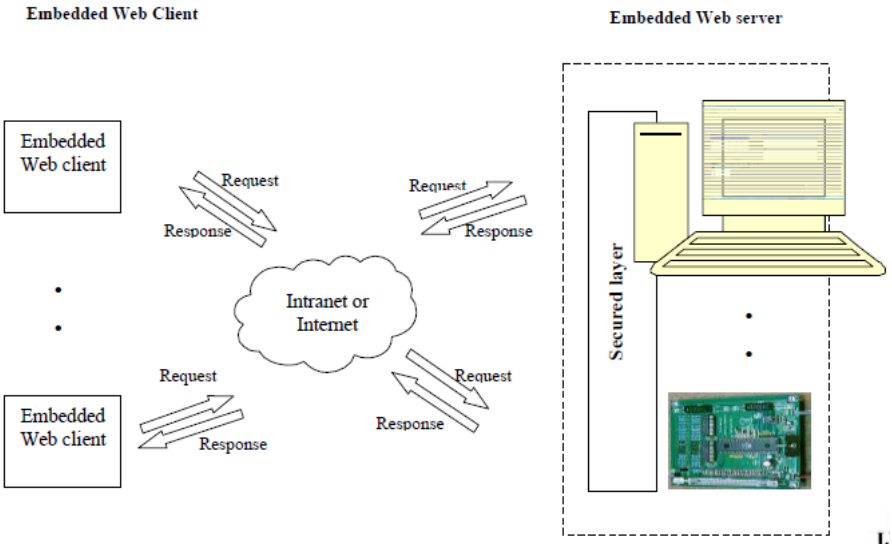

FIG4:EMBEDDED WEB CLIENT AND SERVER COM

VI. RESULT AND DISCUSSION

Embedded Security Scan Detector (ESSD) has been implemented on Linux 2.4.23 Single Board Computer (SBC) and programmed in C. Developing as a low-end new ESSD for to have the benefit that the system modules are natively more secure with substantially good system performance. In addition, a lot of legacy C library code can be easily ported. The entire test was conducted on the Single Board Computer (SBC). At first, we monitor and analyze ICMP traffic in the LAN because we wanted to know what ICMP messages go through the entire network interface, whether there is much more echo reply than echo request and also whether the reply message arrive within the short period of time or not. Then we wanted to know the overall picture of our lab LAN traffic information. So we run a web based Embedded Network Monitor System which has been developed in our lab for 24 hours in order to get traffic information. Figure 4 shows the detail statistical results about network traffic information. Figure 5 shows new system Embedded Security Scan Detector (ESSD) CPU utilization at the time of Smurf-based Attack Detection.

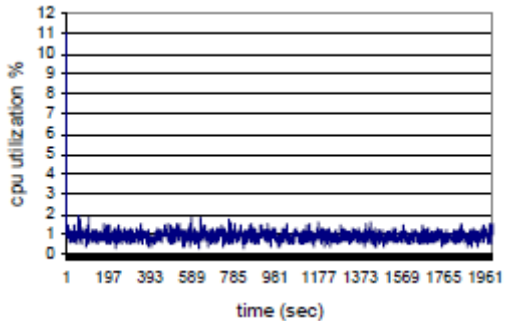

FIG5: Embedded Security Scan Detector (ESSD) CPU utilization

VII. CONCLUSION

This paper finally tune all the attacks related to embedded systems these attacks are related to denial of service to the Web client. Thus also a proposed architecture which is developed and implemented to prevent these type of attacks. This paper presents Embedded Security Scan Detector (ESSD) for DOS Attack Detection integrated into Low-end embedded Linux platform Single Board Computer (SBC). Based on testing performed, the developed ESSD is found to be performing at par with Ubuntu Linux Desktop which runs same application. Thus we can conclude that low-end embedded Linux platform which integrates open source TCP/IP network protocol is suitable for IPV4 application. Apart from that the inherited features of portability, low power, low cost and small size would make such product competitive.

REFERENCES

[1] J. Turley. The Essential Guide to Semiconductors. Prentice hall, 2003, Professional technical Reference, Upper Saddle River, NJ 07458, www.phptr.com

[2] D. Tennenhouse. " Embedding the Internet: Proactive Computing," Comm. Of the ACM, May, 2000

[3]. Lee Gerber, "Denial of Service Attacks Rip the Internet," IEEE Computer, April 2000

[4]. "Smurf IP Denial-of-Service Attacks," CERT® Advisory CA-1998-01, March 2000.http://www.cert.org/advisories/CA-1998-01.html

[5]. Siliva Farraposo, Laurent Gallon, Phillippe Owezarski, "Network Security and DoS Attacks," Feb – 2005. http://www.cert.org/reports/dist_workshop.pdf

[6] Dong Huang "Scematic Description of Web Service Security Constraints" Proceedings of the Second IEEE International Symposium on Service-Oriented System Engineering IEEE2006. http://WWW.ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?pu number=4027101

[7] Kevin D. Lux, Michael J. May, Nayan L. Bhattad, and Carl A. Gunter"WSEmail: Secure Internet Messaging Based on Web Services" Proceedings of the IEEE International Conference on Web Services IEEE2005. http://WWWieeexplore.ieee.org/iel5/10245/32665/01530785 .pdf?arnumber=1530785

[8] Jlan-xin li,Bin li,Liang li and Tong sheng che "An Agentbased Policy Aware Framework for Web Services Security" IFIP International Conference on Network and Parallel Computing – Workshops IEEE 2007 http://WWWieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 4351593

[9] George Yee and Larry Korba "Negotiated Security Policies for E-Services and Web Services" Proceedings of the IEEE International Conference on Web Services (I IEEE2005. http://WWWieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 1530852

[10] Massimiliano Rak, Valentina Casola, Nicola Mazzoccca Emilio Pasquale Mancini and Umberto Villano ' Optimizing Secure Web Services with MAWeS: a Case Study". http://WWWieeexplore.ieee.org/iel5/4543879/4550291/04550321.pdf

[11] Shiping Chen1, John Zic, Kezhe Tang, and David Lev "Performance Evaluation and Modeling of Web Services Security" International Conference on Web Services IEEE2007. http://WWWieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 4279628
[12] Michael Lesk, Martin R. Stytz and Roland L. Trope " providing Web service security in a federated environment" International conference on Privacy and Security IEEE 2007. http://WWWieeexplore.ieee.org/iel5/8013/4085579/0408559 9.pdf
[13] Yuan wo,, Bo-qin feng', Jin-Cang and Zun-Chao li "SXRSRPM: A Security Integrated Model for Web Services" Proceedings of the Third International Conference on Machine Learning and Cybernetics IEEE 2004. http://WWWieeexplore.ieee.org/xpls/abs_all.jsp?arnumber= 1378538

AUTHORS PROFILE

Prof. P. Rama Bayapa Reddy completed BE in computers from Marathwada University ,Aurangabad and M.Tech from JNTU, Anantapur. Now presently pursuing Ph.D from JNTUA, Anantapur. My interested Research area is internet controlled embedded systems.I conducted two national level seminars. I also conducted two workshops on Real Time Embedded Systems. Also I attended workshops conducted by JNTUK. I have total of 15 years of teaching experience. Right now I am working as Professor in Computer Science and Engineering in Dhruva institute of Engineering and Technology, Hyderabad.

Dr. K. Soundararajan received the B.E Degree in Electronics and Communications from S.V.U, Tirupati and M.Tech Degree in Instrumentation and control Engg. from J.N.T.U, Kakinada. He received Ph.D from University of Roorkee, Roorkee. He is having 32 years of teaching experience. He got the Best teacher award for the year 2006 from Andhra Pradesh Govt. and from Lead India2020 in 2005, President of India Award in Bharat Scouts & Guides in 1968, Best Paper Award in 1990–91 and 2000 from Institution of Engineers (India) for best technical paper published in Journal . He is an Expert Committee member, for different central Govt organizations, affiliation committee member for several colleges and different academic boards. He published 21 International Journals/Conferences and 27 national journals/conferences and he participated in 12 National seminars. He guided 9 Ph.Ds and 10 research scholars are working to obtain their PhD. He worked as principal of JNT university college of engineering Anantapur,A.P) and Rector of JNTU ANANTAPUR, Anantapur. Presently, he is working as Professor, Department of ECE, JNTUACE, of Jawaharlal Nehru Technological University College of Engineering, Anantapur, A.P,India.

Dr MHM Krishna Prasad, has completed B.Tech, M.Tech (CSE), JNTU, Hyderabad Ph.D., in Computer Science & Engineering from JNTU Hyderabad with specialization as Data Mining and successfully completed a two year MIUR fellowship at University of Udine, Italy. He has published no of papers in International and National Journals. Under his guidance multiple research scholars are doing research. Presently he is working as Associate Professor of CSE & Head, Dept. of Information Technology University College of Engineering JNTUK-Vizianagaram Campus, VIZIANAGARAM, A.P, India.