International Journal of Security and Its Applications
Vol. 10, No. 2 (2016), pp.375-384
http://dx.doi.org/10.14257/ijsia.2016.10.2.33

Network Security in Embedded System Using TLS

Vivek Negi, Himanshu Verma, Ipsita Singh, Aditya Vikram, Kanika Malik, Archana Singh, Gaurav Verma

Department of Electronics & Communication,
Jaypee University, A-10, Sector-62, Noida (U.P.), India
viveknegi99@gmail.com, himanshutechdn@gmail.com, ipsitasingh99@yahoo.in, adityavikram6289@gmail.com, kanikamalik44@gmail.com, archanasingh2424@gmail.com

Abstract

Security in terms of Networks have turn out to be more significant to Organizations, Military and personal computer user's. Since various kinds of threats are for data from sending it from sender side over internet till it reaches to receiver. Here we will focus on SSL it is a technique used to give client and server authentication, data confidentiality and data integrity. It transform our data into unintelligible form, data which we will be sending can be text or no text form, by encrypting our data we can save it from attacks like eavesdropping, in which interception of communication by unauthorized person, he can either listen or can add malicious information in our data which can lead to catastrophic results. This technique of secure data transmission is very useful in securing the integrity of data sent by the Unmanned Aerial Vehicles in military application to commercially used Electricity meter. Since the above mentioned devices uses microcontroller to send data through internet hence this data is always going to be susceptible to above mentioned threats so it is important to ensure that it doesn't fall in wrong hands, our objective is that our microcontroller sends the data to remote location has authenticity, confidentiality and integrity. First we will send some meaningful text already stored in controller of STM3240G Eval-board then that data will be sent to server. These encrypted packets will be sending to remote server through Ethernet. At the receiver end this data will be received and decrypted to get the original captured data.

Keywords*: Crypto System, SSL and TLS, Security, RTOS, ARM Cortex, Wire Shark*

1. Introduction

Cryptography is the skill which deals with learning of imposing furtive inscription such that information can be prearranged to avoid its content disclosure. The information which could be decoded by the people it is meant for. In the general term we are just securing the data. Certain algorithm is used in this phenomenon which we often named by cryptographic algorithm and termed as cipher and whole system is known as cryptosystem. Two ciphers which are related to cryptography are encipherment (also known as encryption) and decipherment (also known as decryption). Here cipher is used to describe different categories of algorithms in cryptography. For establishing a secure communication between sender-receiver ends, such pair needs one unique cipher which can serve millions of communicating pairs.

ISSN: 1738-9976 IJSIA

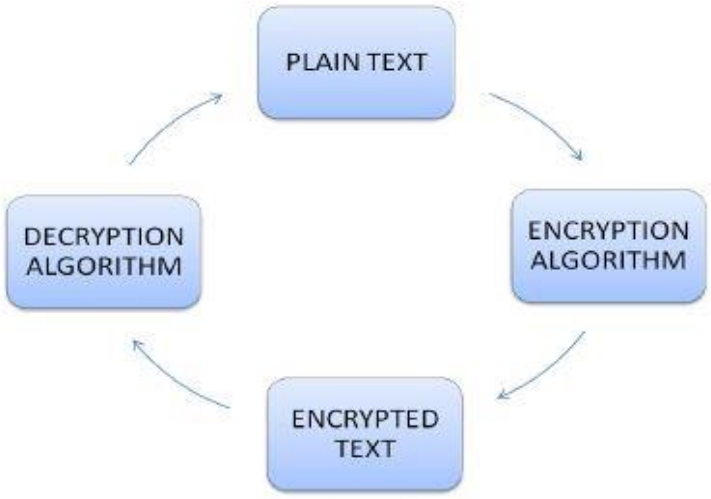

Figure 1. Crypto System

A. Goals of Security

For any data communication to be successful it must meet three objectives and these are Confidentiality, integrity and availability. If these requirements are not met then our data transfer will neither be secure nor successful.

1. Confidentiality

Securing the information is the foremost requirement so that hazardous actions which imperil the confidentiality of the information do not takes place. Such high level of confidentiality is required in military as well as in banking sector where user's account requires safety. Information has to be secured not only during its storage end but also through the transmission process.

2. Integrity

The term integrity means that changes which we require in data should be performed by official entities and through proper channel and hence continuous variations are not required in information. Veracity breach is not essentially caused by malicious action as an interruption in communication system may create undesired changes.

3. Availability

The information which has to be retrieved by officials, first of all it has to be available and secondly it has to be varied continuously in manner that information is accessible to official person otherwise such information is of no use. Such improper information is just as destructive for an organization as to be deficient of integrity and confidentiality.

B. Attacks Related to Data Security

The list of various attacks which can affect the confidentiality, integrity and availability of our data has been divided into three categories.

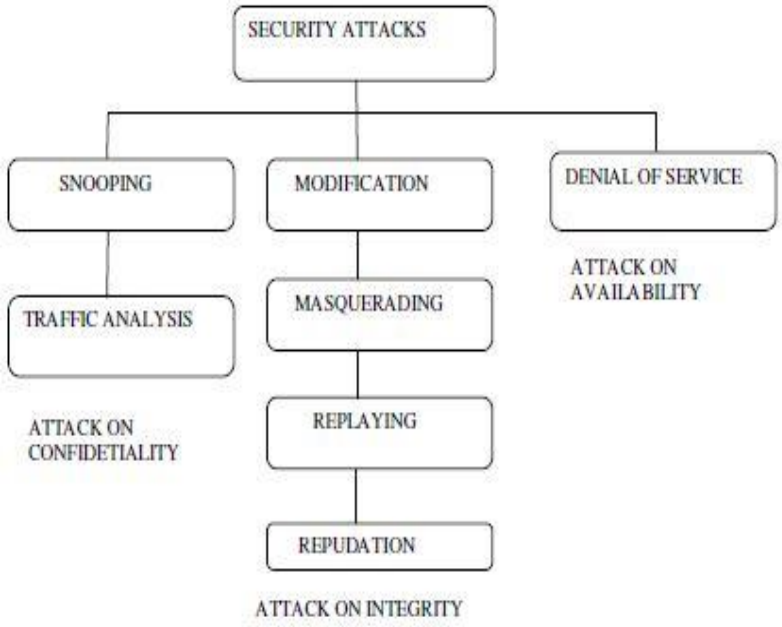

Figure 2. Taxonomy of Attacks on Data

C. Standard Security Mechanism and Access Control

ITU-T (X-800) has recommended some security mechanisms to provide the security services which is shown in fig. below. Access control uses methods to prove that a user has a access right to the data or resources owned by a system e.g. password or PINs

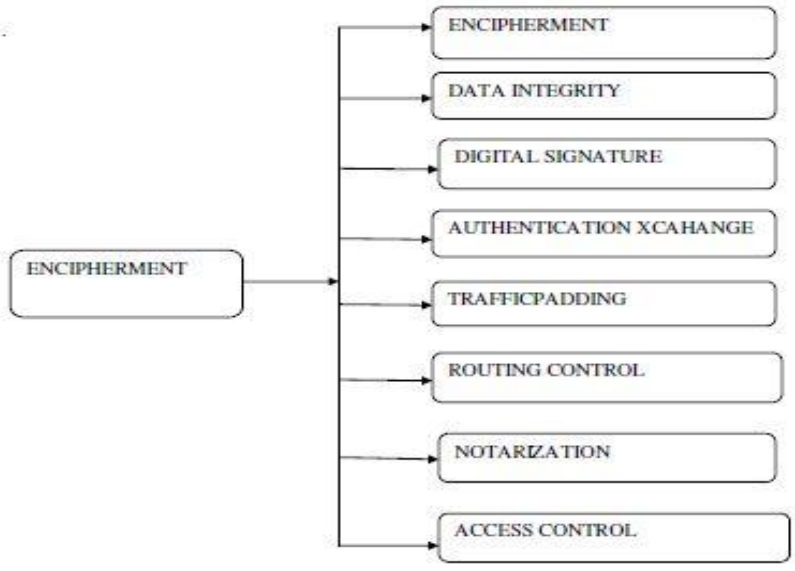

Figure 3. Standard Security Mechanism

D. Techniques Used in Cryptography

Broadly we divide cryptography techniques in two parts:

1. Symmetric-Key Cryptography

Secret-key cryptography is another term of symmetric key encryption cryptography technique. For both encrypting and decrypting data communal secret key is required. Algorithms which are used in such encryption technique are relatively very efficient in handing out large amounts of information than asymmetric encryption algorithms. Symmetric encryption algorithms are divided into two types one is block ciphers (block encryption) and other one is stream ciphers (bit-by-bit encryption).

2. Asymmetric-Key Cryptography

Asymmetric cryptography which is also termed as Public-key cryptography is division of cryptographic algorithms in which there are two set of keys, one of which is public and other one is private i.e. secret. However, two keys are mathematically linked to each other. When we talk about the function of these two keys then public key is used to confirm a digital signature whereas private key is used to establish a digital signature. Operations performed by these two keys is inverse of each other and therefore the term asymmetric is contrary to the term symmetric which depends on single key to perform the task.

2. Description of SSL and TLS

SSL protocols are ever-present security protocols which are taken into consideration in approximately every transaction pursued over internet. The function performed by these protocols is thoroughly meant for secure communication through a proper channel. SSL protocols are highly reliable on TCP protocols and after transforming such reliable transport protocols, a secure communication channel is established for important transactions. Applications and support given by SSL protocols is eternal overwhelming for different algorithms. Either secure communication over internet or any data transmission in company intranet both are genuinely supported by SSL. Once an SSL protocol is in process there is no need to worry about data safety or tampering of information. At a rapid pace these protocols are entering into the world of embedded systems but there is lot to work on because such complex protocols are too hot to be handled by microprocessors.

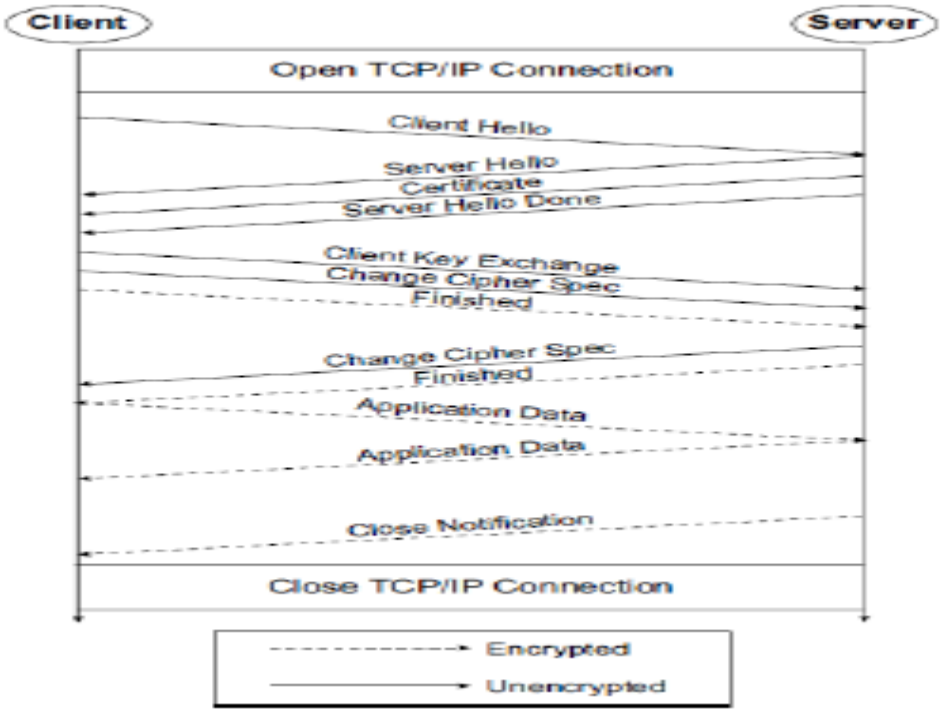

Figure 4. SSL Handshake Mechanism

In contradiction to SSL protocols, TLS protocols use different standardization methods for its implementations. As MD5 or SHA are standard supported by SSL protocols, HMAC is a standard which is accomplished by TLS protocols. To generate the output using TLS protocols one have to be aware form PRF (pseudo random function) where in SSL protocols we used Diffie-Hellman, RSA or Fortezza/DMS output functions to generate key material. Greatly said and explained thoroughly by Thomas that "every system at its building time has its own premaster secret and then secrets of master is created". The output generated through these standards clearly relies upon certain parameters and ciphers suite.

3. RTOS Overview

RTOS stands for Real Time Operating system which was urbanized by group of Real Time Engineers Ltd. Their versions are absolutely available free and therefore they are also termed as Free RTOS. Design of Free RTOS is very flexible for even very small applications of embedded systems and based upon this quality it permits different features and functions. Task handling and managing memory are prime functions of RTOS following by synchronizing different API levels, external hardware drivers and accessing a system file. Besides above features there are more characteristics such as large division of its C compilers coded in C language as well as, pre-emptive task handling, enormous sustain for 23 architectures in microcontrollers and 4.3k bytes of compilation on ARM7. As stated task handling is biggest supported feature so unlimited tasks can be processed at the same time and priority assigned to them also does not bother the hardware. Other than this function like Mutexes, counting semaphores, binary semaphores and queuing is also performed. Various interrupts can be handled at the same time, whatever may be its priority interrupts are automatically assigned according to it. The two terms interrupt

priorities and task priorities are relatively different and perform different functions and so should not be confused with it.

4. Hardware and Software Used

The evaluation board which we have used here is STM3240G generally worn for demonstration purposes. The board comes under the series of STM32F4 and comprises of STM32F407IGH6 high performance embedded ARM cortex (M4F) 32 bit microcontroller. This board contains full hardware features for containment of all peripherals (Ethernet, CAN, smartcard, MICRO-SD card, USART, IrDA, MEMS, EEPROM…etc) provided the feature of developing your own features. For specific application, Extension headers are provided to connect with wrapping boards and daughterboard. For Debugging and programming purposes in-circuit ST-LINK tool has been provided accessible for JTAG as well as SWD interface. One of the Software which we have used for our purpose is "Putty" easily available because of its free and open-source feature. Putty is a serial console application used for network file transfer due to its network supporting protocols such as SCP, rlogin, Telnet, SSH and raw socket connection. Putty was originated for Microsoft Windows and after that there are various version of this software is released for different operating systems. Version 0.59 is capable of connecting to serial port.

Figure 5. STM3240G Eval-board

The other software which we have used solely for our purpose is "Wire shark" which is also free and open source version are available. It serves many purposes like communication protocol development, network troubleshooting analysis and education. The real name of wire shark software is Ethereal which is a project and later on in May 2006 renamed to wire shark. It is also widely available for different platforms like Linux, OS X, Solaris, and BSD and for some other windows and UNIX systems. The cross compiler/IDE µVision4 is used which is a windows based platform tool contains C compiler, macro assembler and Hex file generator**.**

5. Results

Following sequence of image will show the flow of project and desired result achieved through this.

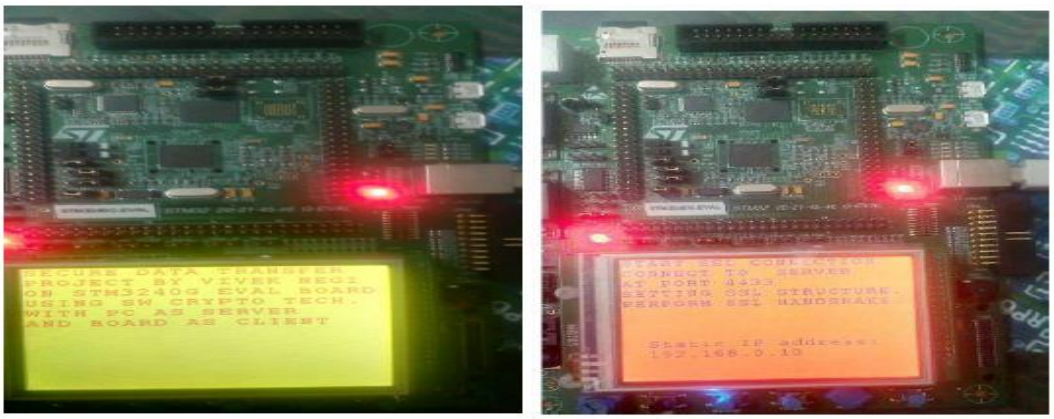

Fig6. Display and Setting up of Connection

At this point of time device hardware and Network interface is configured, SSL context is sent to server at port 4433 and now we are performing handshake with server this all can be viewed on Putty software terminal. Client IP address is 192.168.0.10 as shown in above image.

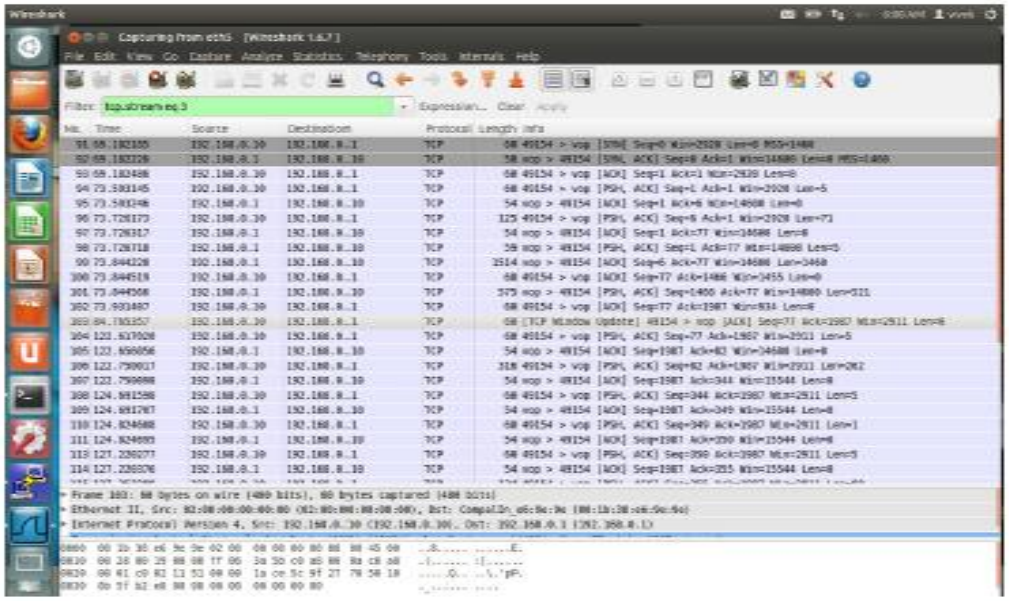

Figure 7. Client-server Communication on Wire Shark

Above figure shows the client server communication observed on Wire shark packet analyzer. Communication uses the TCP protocol in which patron IP address is "192.168.0.10" and server IP address is "'192.168.0.1." Sending and reception of packets during handshake protocol is shown with packet length at different instance of time.

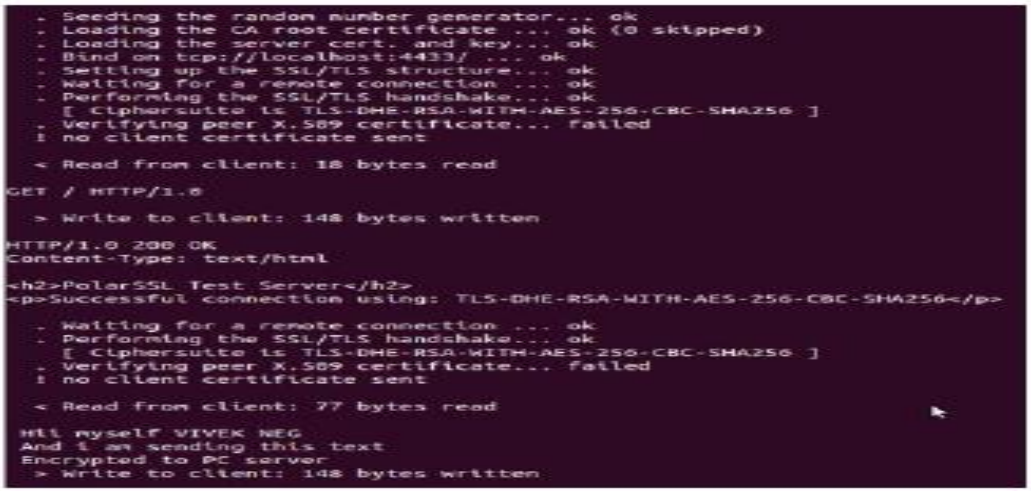

Figure 8. Reception and Decryption of Message by Server

The data sent by the client side encrypted is now decrypted at the server site; packet send is sent through secured channel hence its integrity is maintained.

Figure 9. Thread Termination

Finally thread created for communication is terminated, on pressing the reset button the request from the client will be sent again to the server.

6. Conclusion and Future Work

Data in the form of text has been successfully transmitted through the secure channel with proper encryption at the client site and decryption at the server site. The cipher suite used is a strong TLS suite which makes sure that the confidentiality and integrity of our data sent is maintained, hence the above application can be used to provide secure way of communication through embedded devices like sending meter reading from smart meter or remote entry configurations. This is a

complete new way of using the embedded devices in consumer market and defense sector and further improvement in this technology can make data transfer much more

faster and secure, as there is no specific cryptographic processor is used so we can make modifications in our algorithms according to advancement in technology, this makes software cryptographic approach more flexible and strong. By using this technique we can send the images captured by the camera using embedded device to the remote server with proper security and this can be useful in military application like drone monitoring country's border. Images sent by the drone could be of great importance and any tempering with them can lead to disastrous results. Since the size of such data is much bigger compared to the data sent by the today's embedded devices which can degrade performance in terms of speed but with the constant increment in controller's speed we can overcome this drawback.

References

[1] Mohini Chaudhari, Dr. Kanak Saxena "*Fast and Secure Data Transmission using Symmetric Encryption and Lossless Compression*" International Journal of Computer Science and Mobile Computing Vol.2 Issue. 2, February- 2013, pg. 58-63.
[2] Murali. B. A "*Linux Device Driver Coding for Pseudo Device*" International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005 National Conference on Architecture, Software system and Green computing.
[3] Sidra Malik "*A Novel Key-based Transposition Scheme for Text Encryption*" 2011 Frontiers of Information Technology.
[4] Robert franceschini and Amar mukherjee, "*Data compression using encrypted text*", Proceedings of Advanced Digital Libraries 1996 (ADL '96)0-8186-7402-4/96.
[5] Wen-Xiang Zhang,Si-You Xiao,Yi Zhang, "*Research on Image-text Encryption Techniques in Mobile Communications*", 2010 Second WRI Global Congress on Intelligent Systems, 978-0-7695-4304-8/10.
[6] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "*Text and Image Encryption Decryption Using Advanced Encryption Standard*", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014.
[7] Ching-Kun Chen and Chun-Liang Lin, "*Text Encryption Using ECG signals with Chaotic Logistic Map*", 2010 5th IEEE Conference on Industrial Electronics and Applications, 978-1- 4244-5046-6/10.
[8] Xing-Yuan Wang, Sheng-Xian Gu, "*New chaotic encryption algorithm based on chaotic sequence and plain text*", IET Inf. Secur., 2014, Vol. 8, Iss. 3, pp. 213–216 doi: 10.1049/ietifs. 2012.0279.
[9] Rohit Maheshwari and Sunil Pathak, "*A Proposed Secure Framework for Safe Data Transmission in Private Cloud*", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-1, April 2012.
[10] Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said and Halabi B Hasbullah, "*A Survey on Voice over IP over Wireless LANs*" , World Academy of Science, Engineering and Technology 71 2010.
[11] J.Balu and DR.S.Thirunirai Senthil, "*Secure Data Transmission Over Wimax Networks Using VPN Technology In Real Time Environment"*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 202-211.
[12] Asim Kadav and Michael M. Swift, "*Understanding Modern Device Drivers*" , ASPLOS'12, March 3−7, 2012, London, England, UK.Copyright c 2012 ACM 978-1-4503- 0759-8/12/03.
[13] Bruce Schneier, *Applied Cryptography*, 2nd edition. The standard layman's text on cryptographic algorithms and techniques.
[14] Eric Rescorla, *SSL and TLS, Designing and Building Secure Systems*. A book that specifically covers SSL and how to write an implementation. Includes a discussion of HTTPS.
[15] G. Verma et al*, "Wireless Position Tracking of a DTMF based Mobile Robot using GSM and GPS"* Indian Journal of Science and Technology", vol 8, issue 17, IPL0161,August 2015.
[16] G.Verma et al*, "Hardware Implementation of an Eco-friendly Electronic Voting Machine"* Indian Journal of Science and Technology", vol 8, issue 17, IPL088, August 2015.
[17] T. Gupta, G. Verma *"Area & Power Optimization of VPB Peripheral Memory for ARM7TDMI Based Microcontrollers"* in International Conference on Cognitive Computing and Information Processing (CCIP-2015) March 3-4, 2015 JSSATEN, Noida, India.
[18] T. Gupta, H. Verma, G. Verma, L. Sahoo *" A Portable & Cost Effective Human Computer Interface Device for Disabled*" in International Conference on Communication Systems and Network Technologies (CSNT-2015) April 4-6, 2015 organized by Machine Intelligence Research Labs, Gwalior, India.

