**SECURE WIRELESS DATA COMMUNICATION**



INTRODUCTION-:

 Wireless phones are very popular, and the number of people who use them is steadily growing. As of December 2009, there were over 285 million wireless subscribers in the U.S.  But even though wireless devices have many advantages, privacy is not one of them.

Depending on the kind of phone you use, others can listen to calls you make. Pagers can also be intercepted. And if your computer is connected to a wireless network ('Wi-Fi'), the data you transmit to other computers and printers might not be secure.

It pays to be aware of the privacy and fraud implications of using wireless devices. A few simple precautions will enable you to detect and prevent fraud as well as to safeguard the privacy of your communications.

A word about terminology: This guide uses the terms "analog" and "digital" when describing wireless communications. **Analog** cellular services have been available for 25 years and are now accessible across 95% of the U.S. They send a voice through the air using a continuous radio wave. **Digital** services, available since 1995, convert the signal into the ones and zeros of computer code. In contrast to analog signals which are continuous, digital transmissions are sent as discrete pulses of electricity. In cell phone networks, digital coverage is rapidly catching up to analog coverage and now accounts for more than 85% of the calls made. Digital calls are generally clearer and more secure than analog.

**BASIC CONCEPT-:**

  There are various ways to help protect your privacy when using Wi-Fi.  Begin with basic common sense.  Look around to see if anyone is surreptitiously trying to look at your computer.  Do not leave your computer unattended.  Never conduct unsecured transactions over unsecured Wi-Fi.  When entering sensitive information (such as your Social Security number, password, or credit card number), ensure that either the webpage encrypts the information or that your Wi-Fi connection is encrypted. Disable your wireless adapterif you are not using the Internet. Otherwise, you leave your computer open to vulnerabilities if it accidentally connects to the first available network.

**VPN (Virtual Private Network)-:**

This is the first line of defense against vulnerabilities created by Wi-Fi. A VPN provides encryption over an unencrypted Wi-Fi connection. This will help ensure that all web pages visited, log-on details, and contents of email messages remain encrypted.  This renders intercepted traffic useless to the hacker. You can obtain software to set up a VPN through your office or home computer, or you can use a commercial provider’s hosted VPN service.

. A BRIEF INTRODUCTION TO 8051 MICROCONTROLLER-:

When we have to learn about a new computer we have to familiarize about the machine capability we are using, and we can do it by studying the internal hardware design (devices architecture), and also to know about the size, number and the size of the registers.

         A microcontroller is a single chip that contains the processor (the CPU), non-volatile memory for the program (ROM or flash), volatile memory for input and output (RAM), a clock and an I/O control unit. Also called a "computer on a chip," billions of microcontroller units (MCUs) are embedded each year in a myriad of products from toys to appliances to automobiles. For example, a single vehicle can use 70 or more microcontrollers. The following picture describes a general block diagram of microcontroller.

**AT89S52:** The AT89S52 is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The device is manufactured using Atmel’s high-density nonvolatile memory technology and is compatible with the industry-standard 80C51 instruction set and pinout. The on-chip Flash allows the program memory to be reprogrammed in-system or by a conventional nonvolatile memory pro-grammer. By combining a versatile 8-bit CPU with in-system programmable Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcontroller, which provides a highly flexible and cost-effective solution to many, embedded control applications. The AT89S52 provides the following standard features: 8K bytes of Flash, 256 bytes of RAM, 32 I/O lines, Watchdog timer, two data pointers, three 16-bit timer/counters, a six-vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator, and clock circuitry. In addition, the AT89S52 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port, and interrupt system to continue functioning. The Power-down mode saves the RAM con-tents but freezes the oscillator, disabling all other chip functions until the next interrupt



The hardware is driven by a set of program instructions, or software. Once familiar with hardware and software, the user can then apply the microcontroller to the problems easily.

The pin diagram of the 8051 shows all of the input/output pins unique to microcontrollers:



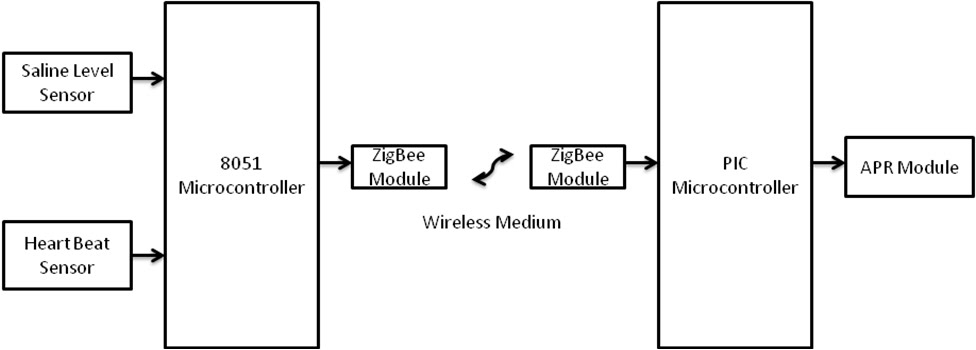
The following are some of the capabilities of 8051 microcontroller.

* Internal ROM and RAM
* I/O ports with programmable pins
* Timers and counters
* Serial data communication

The 8051 architecture consists of these specific features:

* + - 16 bit PC &data pointer (DPTR)
    - 8 bit program status word (PSW)
    - 8 bit stack pointer (SP)
    - Internal ROM 4k
    - Internal RAM of 128 bytes.
    - 4 register banks, each containing 8 registers
    - 80 bits of general purpose data memory
    - 32 input/output pins arranged as four 8 bit ports: P0-P3
    - Two 16 bit timer/counters: T0-T1
    - Two external and three internal interrupt sources Oscillator and clock circuits.

BLOCK DIAGRAM -:



CONCLUSION-:

Wireless networks have spawned a new past-time among hobbyists and corporate spies called war-driving. The data voyeur drives around a neighborhood or office district using a laptop and free software to locate unsecured wireless networks in the vicinity, usually within 100 yards of the source. The laptop captures the data that is transmitted to and from the network's computers and printers. The data could include anything from one's household finances to business secrets.

**References-:**

* **“8051 and embedded system” by Mazidi and Mazidi**
* **All datasheets from** [**www.datasheetcatalog.com**](http://www.datasheetcatalog.com)
* **About AT89s8252 from** [**www.atmel.com**](http://www.atmel.com)
* **And** [**www.triindia.co.in**](http://www.triindia.co.in)