International Conference on Latest Advancements & Future Trends In Engineering, Science & Management
Sambhram Institute of Technology, Bangalore (India)
03rd - 04th May 2019 www.conferenceworld.in
SAMBHRAM INSTITUTE OF TECHNOLOGY
ISBN : 978-93-87793-86-6

Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases

Ms. Sushma S,
Dept., CSE, Sambhram Institute of technology, Bangalore, India

Ms.Sushma Kurdekar,
Dept., CSE, Sambhram Institute of technology, Bangalore, India

Ms.Tanuja Kumari,
Dept., CSE, Sambhram Institute of technology, Bangalore, India.

Ms.Sushmitha M,
Dept., CSE, Sambhram Institute of technology, Bangalore, India

Mrs. Sohara Banu.A.R,
Dept., CSE, Sambhram Institute of technology, Bangalore, India

Abstract— *In Internet of Things (IoT) technology the health-care sector through remote, continuous, and non-invasive monitoring of patients. However, there are two main challenges faced by the IoT-enabled medical devices: energy- efficiency and security/privacy concerns. An ultra-low power and secure IoT sensing/pre-processing the prediction of ventricular arrhythmia using ECG signals. the proposed architecture is designed using an Application Specific Integrated Circuits design flow in 65-nm Low Power Enhanced technology. it consumes the power of 62.2% less than that of the state-of-the-art approaches, it occupying 16.0% smaller area. The proposed system uses ECG key that enables protection of communication channel and offers protection also at the hardware level that means protect from reverse engineering. The security infrastructure is kept at 9.5% for area and 0.7% for power.*

Keywords—Biomedical classifier, Design-for-trust, ECG, Hardware security, Internet of Things, Ventricular arrythmia.

1. INTRODUCTION

Developments in electronics and wireless communication technologies have spawned an era of Internet of things (IoT). Composed of a large number of simple interconnected components that employ massive communication to augment each other's functionality, IoT enabled devices and systems find applications across healthcare, smart buildings, and intelligent transport systems. In the healthcare sector, millions of IoT-enabled implantable medical devices (IMDs) and wearable devices are being deployed, which range from cardiac defibrillators and insulin pumps to ECG processors and fitness trackers Comprising typically 1) a sensing module, 2) a communication module, and 3) an application module, IoT- enabled solutions help tremendously in

improving patient care, enhancing the overall quality of life .These integrated platforms allow continuous aggregation and intelligent mining/pre-processing of health data that can be transmitted either periodically or judiciously based on the detection of certain events, over the network to medical facilities for further evaluation. Reliance on battery/harvested power and continual monitoring operation for extended lifetimes imposes strict power consumption constraints on IMDs/wearable devices. Thus, energy efficiency is a major concern in these devices.

2. USE OF INFRARED TECHNOLOGY

2.1 Infrared Technology

Infrared technology addresses a wide variety of wireless applications. The main areas are sensing and remote controls. In the electromagnetic spectrum, the infrared portion is divided into three regions: near infrared region, mid infrared region and far infrared region.

The wavelengths of these regions and their applications are shown below.

Near infrared region — 700 nm to 1400 nm — IR sensors, fiber optic

Mid infrared region — 1400 nm to 3000 nm — Heat sensing.

Far infrared region — 3000 nm to 1 mm — Thermal imaging.

The frequency range of infrared is higher than microwave and lesser than visible light.

For optical sensing and optical communication, photo optics technologies are used in the near infrared region as the light is less complex than RF when implemented as a source of signal. Optical wireless communication is done with IR data transmission for short range applications.

An infrared sensor emits and/or detects infrared radiation to sense its surroundings.

The working of any Infrared sensor is governed by three laws: Planck's Radiation law, Stephen – Boltzmann law and Wien's Displacement law.

2.2 Planck's Radiation law

Planck's law states that "every object emits radiation at a temperature not equal to 00K". Stephen – Boltzmann law states that "at all wavelengths, the total energy emitted by a black body is proportional to the fourth power of the absolute temperature". According to Wien's Displacement law, "the radiation curve of a black body for different temperatures will reach its peak at a wavelength inversely proportional to the temperature".

3. TYPES OF IR SENSORS

Infrared sensors can be passive or active. Passive infrared sensors are basically Infrared detectors. Passive infrared sensors do not use any infrared source and detects energy emitted by obstacles in the field of view. They are of two types: quantum and thermal. Thermal infrared sensors use infrared energy as the source of heat and are independent of wavelength. Thermocouples, pyroelectric detectors and bolometers are the common types of thermal infrared detectors. Keep your text and graphic files separate until after the text has been formatted and

styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Quantum type infrared detectors offer higher detection performance and are faster than thermal type infrared detectors. The photosensitivity of quantum type detectors is wavelength dependent. Quantum type detectors are further classified into two types: intrinsic and extrinsic types. Intrinsic type quantum detectors are photoconductive cells and photovoltaic cells.

Active infrared sensors consist of two elements: infrared source and infrared detector. Infrared sources include an LED or infrared laser diode. Infrared detectors include photodiodes or phototransistors. The energy emitted by the infrared source is reflected by an object and falls on the infrared detector.

3.1 What is an IR sensor?

An IR sensor is a device which detects IR radiation falling on it. There are numerous types of IR sensors that are built and can be built depending on the application. Proximity sensors (Used in Touch Screen phones and Edge Avoiding Robots), contrast sensors (Used in Line Following Robots) and obstruction counters/sensors (Used for counting goods and in Burglar Alarms) are some examples, which use IR sensors.

3.2 Working Mechanism

An IR sensor is basically a device which consists of a pair of an IR LED and a photodiode which are collectively called a photo-coupler or an opto-coupler. The IR LED emits IR radiation, reception and/or intensity of reception of which by the photodiode dictates the output of the sensor. Now, there are so many ways by which the radiation may or may not be able to reach the photodiode.

3.2.1 Direct incidence

We may hold the IR LED directly in front of the photodiode, such that almost all the radiation emitted, reaches the photodiode. This creates an invisible line of IR radiation between the IR LED and the photodiode. Now, if an opaque object is placed obstructing this line, the radiation will not reach the photodiode and will get either reflected or absorbed by the obstructing object. This mechanism is used in object counters and burglar alarms.

3.2.2 Indirect Incidence

High school physics taught us that black color absorbs all radiation, and the color white reflects all radiation. We use this very knowledge to build our IR sensor. If we place the IR LED and the photodiode side by side, close together, the radiation from the IR LED will get emitted straight in the direction to which the IR LED is pointing towards, and so is the photodiode, and hence there will be no incidence of the radiation on the photodiode. Please refer to the right part of the illustration given below for better understanding. But, if we place an opaque object in front the two, two cases occur:

3.2.3 Reflective Surface

If the object is reflective, (White or some other light color), then most of the radiation will get reflected by it, and will get incident on the photodiode. For further understanding, please refer to the left part of the illustration below.

3.2.4 Non-reflective Surface

If the object is non-reflective, (Black or some other dark color), then most of the radiation will get absorbed by it, and will not become incident on the photodiode. It is similar to there being no surface (object) at all, for the sensor, as in both the cases, it does not receive any radiation.

4. BACKGROUND AND RELATED WORK

4.1 Previous Work on ECG Processors

An ECG processor which has three stages known as preprocessing, feature extraction and classification, which proposed in [1]. All these three stages implemented in Quad Level Vector based algorithm [2]. To reduce the power consumption and maximize hardware utilization all functions were pipelined. Along with this clock gating and voltage scaling used parallel to reduce the energy wastes. The ECG processor has made using 0.18µm and consumed 6µW at 1.8V and 1.26µW at 0.7 V. Other system was implemented in three different chips in [3] for ECG classification. First chip consisted body-end circuits which was on-off keying transmitter and high-pass sigma delta modulator-based bio-signal processor (HPSDM-BSP). The second chip had DSP unit and receiver at receiving end. And third chip was classifier. DSP unit was used to adopt Discrete Wavelet Transform for ECG feature extraction and classification. The chip was made-up on 0.18µm CMOS technology and total consumed power was 5.967µW for DSP unit at 1.2V. The beat detection accuracy was 99.44% and ECG classification accuracy was 97.25%. The stated results only for detection of VA and not supposed for prediction.

4.2 Previous Work on Hardware Security: Logic Locking

According to us, there is no former work that can considers as securing the essential hardware for biomedical SoCs. The previous s work focuses on secure communication. Logic locking, we employed as a major part of hardware security. Who want to know detailed description on different DfTr techniques can refer survey paper [4] and [5].

Logic locking is DfTr technique which objective to protecting against IP privacy, hardware Trojans and overbuilding. It also focuses on reverse engineering attacks by secret key to locking a design. A set of XOR/XNORs gates referred as key gates to making enable additional logic and chip-locking features. Locked netlist produced by adding key gates to original netlist. The produced locked netlist will be passes through untrusted design phases which is shown in figure 3. But without knowledge on secret key locked netlist is not valuable.

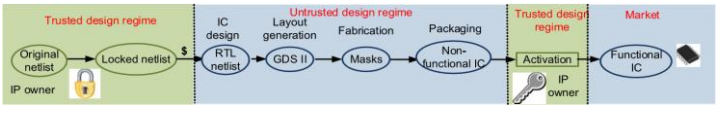
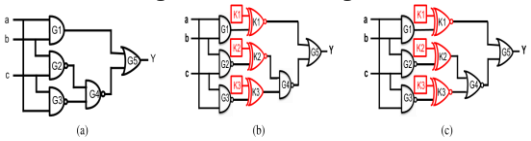


Fig. 1. Logic locking in the context of IC design flow. The design is in the locked form in the untrusted design.



(a) (b) (c)

Fig. 4. Logic locking using XOR/XNOR gates [20]. a) An example circuit: majority of three inputs. b) Circuit locked using XOR/XNOR key gates. The

ISBN : 978-93-87793-86-6

Fig 2 Logic locking using XOR/XNOR gates.(a) An example circuit: majority of three inputs. (b) circuit locked using XOR/XNOR key gates Correct key value is 110. c) Locked circuit with inverters immersed by the key gates. The correct key value is still 110.

Example The above figure 4(a) shows the example of majority circuits, 4(b) shows the locked version of majority circuits by using three XOR/XNOR key gates. Here by using the wire one input of every key gate is driven in original design, and another input of each key gate is considering as key input which is stowed in tamper-proof memory using key bit. Figure 4(c) shows as to increase the obfuscation complexity an inverters bubble pushed in the netlist. Without activated the locked IC cannot generate correct output. The activation is done by using correct key. Consider the figure 4(b), the correct output Y = 0 when applied correct key 110 for input 000. And when applied incorrect key for the same input producing wrong output Y=1.

How hardware trust issues address by logic locking?

Even if locked netlist steals by reverse engineering or it is obtained by reverse engineering, without knowledge on correct key netlist is not usable. Similarly counterfeiting attacks and logic locking thwarts piracy. Even fabricated chip functionality will not work appropriately without on knowledge of secret key. In the netlist insertion of Trojans will be prevented by logic locking. The insertion of Trojans in netlist prevented by making the netlist to harder for the attacker where to identify the safe zone for inserting Trojans will be tougher. Transition probability of signals will be alter by key gates in such a way that the transition probability will be unknown to attacker.

Types of Logic Locking:

1. Random Logic Locking: By inserting the XOR key gates at different locations in the netlist, Random Logic Locking locks the design. The example of locked netlist by inserting three key-gates K1, K2 and K3 using Random logic locking as shown in the figure 4(b).

2. Fault Analysis Based Logic Locking: The aim of Fault analysis-based logic locking to prevent usage of IC as black box. In FLL the correct output may produced by incorrect keys for some input pattern. It ensures maximum corruption for output when apply incorrect key. The hamming distance in between incorrect and correct output, applying incorrect keys measures as output corruption in terms of percentage.

3. Strong logic locking: It is a type of logic locking which inserts the key-gates in such a way that which maximize the interferences between prevents sensitization of key bits and key gates as individuals. With increased interference the attacker forces brute-force with exponentially increases the number of key combinations.

4. SAT Attack Resistant Logic Locking: Against logic locking, SAT attack is most powerful attacks. This attack fully based on concept of removing incorrect keys by perceptive input. By making ensure that input are narrow in effectiveness, SARLock produced resistance against the SAT attack. SARLock structure ensures that

each discriminating input patterns can remove maximum one incorrect key. To become more effective, SARLock have to joint with other logic locking method such as Fault analysis-based logic locking and Random logic locking. Here, we consider SARLock as surplus layer of security.

4.3 Previous Work on ECG Key Generation

Cryptographic algorithms is backbone of secure communication infrastructure which is depend on secret keys. These secret keys are usually generated by pseudorandom number generators (PRNGs).

These key need to satisfy the randomness properties which is specified by NIST. PRNGs first make to run complex processing algorithms on random seeds, to making them unrealistic for wearable devices and battery-operated devices. The physiological signals as ECG used to generate the secret key for that devices. ECG signals are not consistent always and it will be challenging to use in the direct biometric authentication. The keys as binary sequence generated built on the ECG signals which have better randomness properties and it also satisfy the NIST criteria. The earlier ECG based key generation based on different approaches which used inter-pulse interval which is also known as RR interval. These approaches along with the error correction circuitry also have high latency. The latest ECG based key generation accomplished by different ECG features and quantization of RR while passing NIST concepts. We will adopt the method which has all the seven features for key generation.

5. LITERATURE SURVEY

The purpose of the Literature Survey is to give the brief overview and also to establish complete information about the reference papers. The goal of Literature Survey is to completely specify the technical details related to the main project in a concise and unambiguous manner.

[1] H. Kim, R. F. Yazicioglu, T. Torfs, P. Merken, H.-J. Yoo, and C. Van Hoof, "A low power ECG signal processor for ambulatory arrhythmia monitoring system," in Proc. IEEE Symp. VLSI Circuits, Sep. 2010.

An ECG signal processor (ESP) is implemented for ambulatory arrhythmia monitoring systems. The ESP involves three heterogeneous processors and performs filtering, data compression, ECG classification, and encryption. A data reduction system, containing of skeleton and Huffman coding, which are used to memory access power and reduce the on-chip memory capacity. The ESP consumes 1.26-μW at 0.7V, while providing real time signal processing.

[2] H. Kim, R. F. Yazicioglu, P. Merken, C. Van Hoof, and H.-J. Yoo, "ECG signal compression and classification algorithm with quad level vector for ECG holter system," IEEE Trans. Inf. Technol. Biomed., Jan. 2010.

An ECG signal processing method with quad level vector (QLV) is projected for the ECG holter system. The QLV can used for both flows to achieve good performance with low-computation complexity. The compression algorithm is done by using ECG skeleton and Huffman coding. The accuracy performance of the R-peak detection is 100% without noise and 95.63% at the worst case with −10-dB SNR noise. The processing cost is reduced by 45.3% with the specified compression techniques.

[3] R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker you wear: A security analysis of wearable health trackers," in Proc. ACM Symp. Appl. Comput., 2016

Wearable tracking devices which was most popular due to valued services offered by them, monitoring human's health parameters and, usually it was assisting persons to take care of themselves. The results of the study shows that how these devices are susceptible to several attacks which can concessions users' data privacy and security, and finally call the tracker purveyors to raise the stakes against such attacks.

[4] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios," *Digit. Investigat.*, to be published.

Cardiac implantable medical devices forensics Cardiac Implantable Medical devices (IMD) are increasingly being used by patients to benefit from their therapeutic and life-saving functions. These medical devices are surgically implanted into patient's bodies and wirelessly configured by prescribing physicians and healthcare professionals using external programmers.

[5] G. Zheng *et al.*, "Multiple ECG fiducially points based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Informat.*,2015.

Heartbeats based Random binary sequences (RBSs) is the backbone of security aspects. The keys as binary sequence generated built on the ECG signals which have better randomness properties and it also satisfy the NIST criteria. The earlier ECG based key generation based on different approaches which used inter-pulse interval which is also known as RR interval. These approaches along with the error correction circuitry also have high latency.

[6] Y.-P. Chen *et al.*, "An injectable 64 nW ECG mixed-signal SoC in 65 nm for arrhythmia monitoring *IEEE J. Solid-State Circuits* jan, 2015

A syringe-implantable electrocardiography monitoring system is proposed. The proposed SoC is fabricated in 65 nm CMOS and consumes 64 nW while detecting atrial fibrillation arrhythmia and keeping the uneven waveform in memory in trials using an ECG simulator, and an isolated heart.

[7] AN 8.12 MW WAVELET DENOISING CHIP FOR PPG DETECTION AND PORTABLE HEART RATE MONITORING IN 0.18 MM CMOS," *IEEE TRANS. BIOMED. CIRCUITS SYST.*, JUN. 2012.

A low power wavelet denoising chip for photoplethysmography (PPG) detection and portable heart rate monitoring is presented. To remove noise and progress detection accuracy, Harr wavelet (HWT) is choosen as the processing tool. The proposed algorithms reduce the power consumptions of chip. The power consumption of used chip is only 8.12 μW in 1 V voltage supply.

[8] M. Yasin, B. Mazumdar, J. J. V. Rajendran, and O. Sinanoglu, "SARLock: SAT attack resistant logic locking," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust*, Apr. 2016

Logic locking is a protection technique which objective to protecting against IP privacy, hardware Trojans and overbuilding. It also focus on reverse engineering attacks by secret key to locking a design. The proposed method refers as SARLock which increase the number of input patterns to recover the secret key.

6. PROBLEM DEFINITION

The system consists of an silver chloride (Ag / Cl) sticking electrode or a sensor,. The second stage is an Instrumentation amplifier (IA), which has a high gain (1000) . The output of IA, is passed through the low pass filter with a cut off frequency of 150Hz. This block is used to convert the ECG signals to square waveform. Cathode Ray Oscilloscope is used to display the output waveform. Microcontroller is used to perform the counting of pulses. LCD is used to display the heart rate. It senses only heart beat rate not sense the respirator, body temperature and humidity. The health parameters of the patient are send through the Zigbee, Bluetooth Communication protocol. These protocols have short communication ranges to transmit the data. At any time the doctor can't able to see the health parameters of the patient.

7. PROPOSED SYSTEM

An ultra-low power and secure IoT sensing/preprocessing platform for prediction of ventricular arrhythmia using ECG signals. Our proposed solution is able to predict the on-set of the critical cardiovascular events up to 3 h in advance with 86% accuracy and also sensing body temperature, humidity and respiratory problems. Here four sensors are used for sensing temperature, humidity, heartbeat and respiratory.

Pic microcontroller collects the data from the sensors and sends the data through IOT. The protected data sent can be access anytime by the doctors by typing the corresponding exclusive IP address in any of the internet Browser at the end user device (eg. Laptop, Desktop, Tablet , Mobile phone).

The microcontroller is connected to IOT which provides information to doctor/caretaker when the heart rate is greater than 90 or less than 60 and when temperature is less than 20 or greater than 35.LCD is connected to microcontroller to display the transaction process and healthcare data. patient health status is continuously sent to doctor. Therefore, continuous monitoring of patient data is achieved.

7.1 Initialisation Phase

VA PROCESSOR ARCHITECTURE

The baseline VA processor presented in consists of three main stages: ECG pre-processing, feature extraction and classification. In the ECG pre-processing stage all the ECG wave features such as QRS complex, T-wave and P-wave are extracted. Prior to ECG delineation, filtering is performed because ECG could be corrupted by baseline drift, power line interference, and high frequency noise.

After filtering, QRS detection is performed based on the Pan and Tompkins technique. Along with the QRS peak detection, the QRS onset and offset are also delineated. Finally, T and P waves are delineated, and the corresponding fiducially points (P onset, P peak, P offset, T onset, T peak, and T offset) are extracted. Three major modifications were carried out to lower the power consumption: 1) Elimination of the SRAM block in QRS detection, and thus, reducing RAM requirements from 8KB down to 4KB. 2) Decreasing the operating frequency to 250 Hz equal to the ECG sampling frequency.3) The use of High Threshold Voltage (HVT) cells to reduce the leakage power.

ISBN : 978-93-87793-86-6

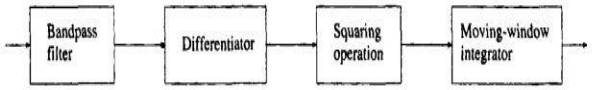
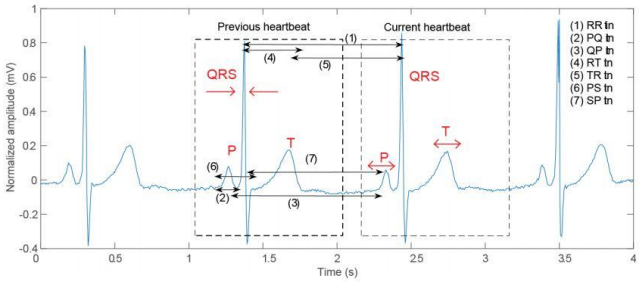


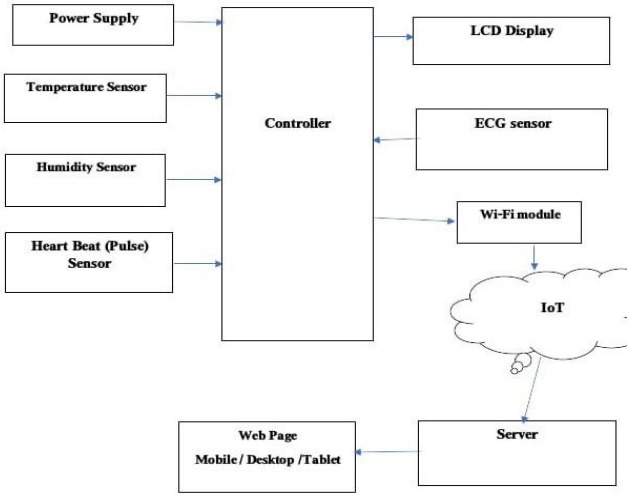
Fig 3 Block Diagram of Pan-Tompkins algorithm for QRS detection



Interval r	Reason for Wave generation	Amplitude	Time Interval	characteristics
p wave	Represents Atrial Depolarization	Normal amplitude is 1-1.5 mm	<0.12 sec	Small, rounded and upright
QRS complex	Represents Atrial Depolarization	Normal amplitude of R-wave is 8-12 mm	<0.04 to 0.10sec (QRS Interval	The first negative wave in the complex is the Q wave, the first positive wave in the complex is the R-wave and the first negative wave following the R-wave is the S-wave
T Wave	Represents ventricular repolarization	Normal amplitude is 2 – 5 mm	<0.04 to 0.10sec (QRS Interval	Same polarity as QRS complex usually correlates with polarity of Rwave
U Wave	Purkinje fiber repolarization	Not measured (low voltage)	<0.01sec	Usually of low voltage and same polarity as T wave when present

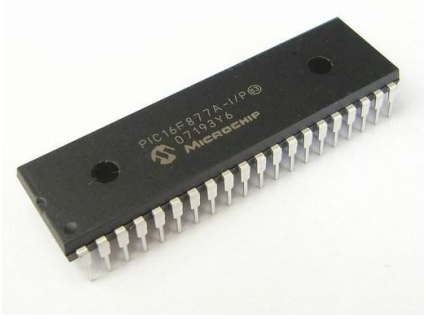
7.2 Architectural model

ISBN : 978-93-87793-86-6



Developments in electronics and wireless communication technologies have spawned an era of Internet of things (IoT). Composed of a large number of simple interconnected components that employ massive communication to augment each other's functionality, IoT enabled devices and systems find applications across healthcare, smart buildings, and intelligent transport systems. In the healthcare sector, millions of IoT-enabled implantable medical devices (IMDs) and wearable devices are being deployed, which range from cardiac defibrillators and insulin pumps to ECG processors and fitness trackers Comprising typically 1) a sensing module,2) a communication module, and 3) an application module, IoT- enabled solutions help tremendously in improving patient care, enhancing the overall quality of life. These integrated platforms allow continuous aggregation and intelligent mining/pre-processing of health data that can be transmitted either periodically or judiciously based on the detection of certain events, over the network to medical facilities for further evaluation. Reliance on battery/harvested power and continual monitoring operation for extended lifetimes imposes strict power consumption constraints on IMDs/wearable devices. Thus, energy efficiency is a major concern in these devices.

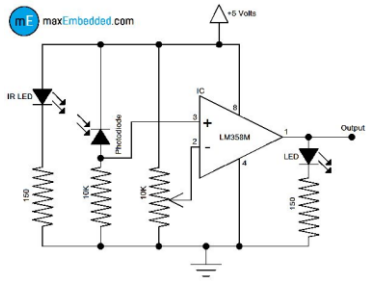
7.2.1 Micro controller



PIC16f877a finds its applications in a huge number of devices. It is used in remote sensors, security and safety devices, home automation and in many industrial instruments. An **EEPROM** is also featured in it which makes it possible to store some of the information permanently like transmitter codes and receiver frequencies and some other related data. The cost of this controller is low and its handling is also easy. Its flexible and can be used in areas where microcontrollers have never been used before as in microprocessor applications and timer functions etc.

1. It has smaller 35 instructions set.
2. It can operate up to 20MHz frequency.
3. The operating voltage is between 4.2 volt to 5.5 volts. If you provide it voltage more than 5.5 volts, it may get damaged permanently.
4. It does not have internal oscillator like other PIC18F46K22, PIC18F4550.
5. The maximum current each PORT can sink or source is around 100mA. Therefore, current limit for each GPIO pin of PIC16F877A is 10 milli ampere.
6. It is available in four IC packaging such as 40-pin PDIP 44-pin PLCC, 44-pin TQFP, 44-pin QFN.

7.2.2 Temperature Sensor



The LM35 series are precision integrated-circuit temperature devices with an output voltage linearly-proportional to the Centigrade temperature. The LM35 device has an advantage over linear temperature sensors calibrated in Kelvin, as the user is not required to subtract a large constant voltage from the output to obtain convenient Centigrade scaling. The LM35 device does not require any external calibration or trimming to provide typical accuracies of ±¼°C at room temperature and ±¾°C over a full −55°C to 150°C temperature range. Lower cost is assured by trimming and calibration at the water level. The low-output impedance, linear output, and precise inherent calibration of the LM35 device makes interfacing to readout or control circuitry especially easy. The device is used with single power supplies, or with plus and minus supplies. As the LM35 device draws only 60 µA from the supply, it has very low self-heating of less than 0.1°C in still air. The LM35 device is rated to operate over a −55°C to 150°C temperature range, while the LM35C device is rated for a −40°C to 110°C range (−10° with improved accuracy). The LM35-series devices are available packaged in hermetic TO transistor packages, while the LM35C, LM35CA, and LM35D devices are available in the plastic TO-92 transistor package. The LM35D device is available in an 8-lead surface-mount small-outline package and a plastic TO-220 package.

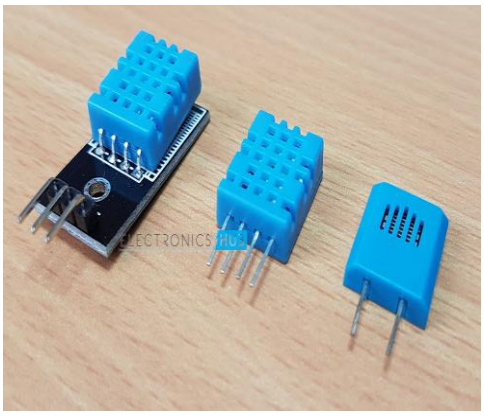
ISBN : 978-93-87793-86-6

Features

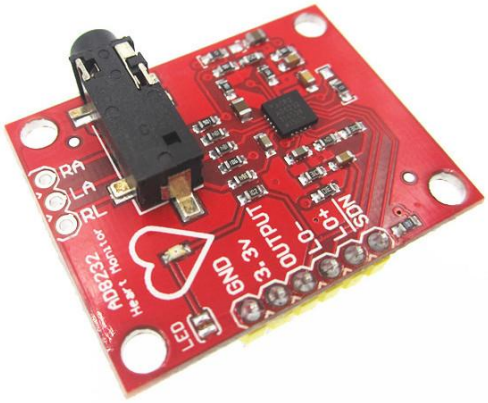
1. Calibrated Directly in Celsius (Centigrade)
2. Linear + 10-mV/°C Scale Factor
3. 0.5°C Ensured Accuracy (at 25°C)
4. Rated for Full −55°C to 150°C Range
5. Suitable for Remote Applications
6. Low-Cost Due to Wafer-Level Trimming
7. Operates From 4 V to 30 V
8. Less Than 60-µA Current Drain
9. Low Self-Heating, 0.08°C in Still Air
10. Non-Linearity Only ±¼°C Typical
11. Low-Impedance Output, 0.1 Ω for 1-mA Load

7.2.3 Humidity Sensor

Humidity is defined as the amount of water present in the surrounding air. This water content in the air is a key factor in the wellness of mankind. For example, we will feel comfortable even if the temperature is 0C with less humidity i.e. the air is dry. But if the temperature is 100C and the humidity is high i.e. the water content of air is high, then we will feel quite uncomfortable. Humidity is also a major factor for operating sensitive equipment like electronics, industrial equipment, electrostatic sensitive devices and high voltage devices etc. Such sensitive equipment must be operated in a humidity environment that is suitable for the device. Hence, sensing, measuring, monitoring and controlling humidity is a very important task.



ISBN : 978-93-87793-86-6

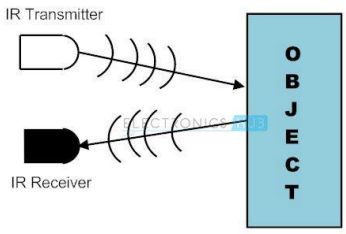


7.2.4 ECG and PULSE rate sensor

This sensor is a cost-effective board used to measure the electrical activity of the heart. This electrical activity can be charted as an ECG or Electrocardiogram and output as an analog reading. ECGs can be extremely noisy, the AD8232 Single Lead Heart Rate Monitor acts as an op amp to help obtain a clear signal from the PR and QT Intervals easily.

The AD8232 is an integrated signal conditioning block for ECG and other biopotential measurement applications. It is designed to extract, amplify, and filter small biopotential signals in the presence of noisy conditions, such as those created by motion or remote electrode placement. The AD8232 module breaks out nine connections from the IC that you can solder pins, wires, or other connectors to. SDN, LO+, LO-, OUTPUT, 3.3V, GND provide essential pins for operating this monitor with an Arduino or other development board. Also provided on this board are RA (Right Arm), LA (Left Arm), and RL (Right Leg) pins to attach and use your own custom sensors. Additionally, there is an LED indicator light that will pulsate to the rhythm of a heartbeat.

Note: This product is NOT a medical device and is not intended to be used as such or as an accessory to such nor diagnose or treat any conditions.



Features: Operating Voltage - 3.3V**,** Analog Output**,** Leads-Off Detection**,** Shutdown Pin**,** LED Indicator**,** 3.5mm Jack for Biomedical Pad Connection or Use 3 pin header.

7.2.5 IR Receiver Modules for Remote Control Systems

Infrared sensors can be passive or active. Passive infrared sensors are basically Infrared detectors. Passive infrared sensors do not use any infrared source and detects energy emitted by obstacles in the field of view.

ISBN : 978-93-87793-86-6

They are of two types: quantum and thermal. Thermal infrared sensors use infrared energy as the source of heat and are independent of wavelength. Thermocouples, pyroelectric detectors and bolometers are the common types of thermal infrared detectors.

Quantum type infrared detectors offer higher detection performance and are faster than thermal type infrared detectors. The photosensitivity of quantum type detectors is wavelength dependent. Quantum type detectors are further classified into two types: intrinsic and extrinsic types. Intrinsic type quantum detectors are photoconductive cells and photovoltaic cells.Active infrared sensors consist of two elements: infrared source and infrared detector. Infrared sources include a LED or infrared laser diode. Infrared detectors include photodiodes or phototransistors. The energy emitted by the infrared source is reflected by an object and falls on the infrared detector.

8 . SET OF PARAMETERS

8.1 DHT11

Operating Voltage ranges from 3.5V to 5.5V. Operating current is 0.3mA (measuring) 60u(standby). Output will be in Serial data format. Humidity Ranges from 20% to 90%. Resolution of Humidity is 16-bit. Accuracy is ±1°C and ±1%.

8.2.LM35

Calibrated directly in ^{o} Celsius (Centigrade). Linear + 10.0 mV/^{o}C scale factor. 0.5^{o}C accuracy guarantee able (at +25^{o}C). Rated for full −55^{o} to +150^{o}C range. It is suitable for remote applications. Low cost due to wafer-level trimming. Operates from 4 to 30 volts. Less than 60 µA current drain.

8.3.ECGsensor

Gain is 1100. Ranges from ±1.5mV (with VCC = 3.3V). Bandwidth is between 0.5-40Hz. Current Consumed by ECG sensor is ~4mA. Input Impedance is 100GOhm. CMRR is 110dB. Electrodes used are 3 or 2 (virtual REF).

8.4.LCD16*2display

A 16x2 LCD means it can display 16 characters per line and there are 2 such lines. In this LCD each character is displayed in 5x7 pixel matrix. This LCD has two registers, namely, Command and Data.

8.5.Esp8266(Wi-Fimodule)

Operating Voltage is 3.0 ~ 3.6V. Average Operating Current used is 80mA. Tensilica Xtensa LX106 32 bit RISC CPU running at 80 MHz. 16 GPIO Input Pins.SPI(Serial Peripheral Interface). I^2C(Inter-Integrated Circuit) used for software implementation. I^2S(Inter-IC sound) interfaces with DMA (sharing pins with GPIO). UART on dedicated pins – 2x TX and 1x RX. 1x 10bit ADC. Operating Temperature is -40°C ~ 125°C. Frequency Range is 2400 ~ 2483.5MHz. Memory used 32 KiB instruction RAM,32 KiB instruction cache RAM, 80 KiB user-data RAM,16 KiB ETS system-data RAM.

8.6. THRESHOLD TABLE

Sensors	Threshold
DHT11	30% - 60%
LM 35	< 20F and >35F
ECG sensor	< 60 and >90

9. CONCLUSION AND FUTURE ENHANCEMENT

We present an ultra-low power, secure, fully integrated IoT platform for prediction of ventricular arrhythmia using ECG signals. The proposed architecture was implemented using an ASIC design flow in 65nm LPe technology. The proposed VA processor achieves a reduction of 62.2% in power consumption and a 16.0% reduction in area when compared to similar state-of-the-art processors. This reduction is accomplished by processing the incoming ECG signal directly, hence, reducing the size of the required RAM for ECG signal processingfrom8KB to 4KB. Moreover, operating on the ECG signal directly enables the proposed VA processor to operate at the same frequency as the sampling frequency of 250Hz, further reducing dynamic power consumption. The proposed processor re-uses the ECG features used during classification to generate a key for securing the proposed IoT platform against telemetry-based and hardware-based attacks. The power and area overhead of the overall security infrastructure are 0.7% and 9.5%, respectively, with no impact on the design speed. While this paper presents a case-study for a specific biomedical SoC, the methodology to identify security objectives and map them to defense layers is generic. With some customization, the proposed methodology can be easily adopted for other resource-constrained, security-critical biomedical platforms as well as other types of IoT devices.

Two main challenges faced by the IoT-enabled medical devices: energy- efficiency and security/privacy concerns.

Existing systems sense only heart beat rate not sense the respiratory, body temperature and humidity.

Remote monitoring requires patient data record automatically sent to the doctor.

Future Enhancement

While we presented an IoT platform with several advantages over the state-of-art solutions, there are opportunities for future improvements that include a low-powered wireless transceiver module to transmit the biomedical signals. Integrate multiple biomedical signals with the ECG, such as blood glucose, electroencephalograph, and electromyography. Encrypt and authenticate the communication using the ECG-generated key The current system enables this support but uses the key only to unlock the locked processor Enhance the protection against the insertion of different classes of hardware Trojans, especially those that are easy to insert and difficult to detect, such as time bombs. Employ improved filtering techniques to remove any

type of noise that could be coupled with the ECG signal and further improve the prediction accuracy. Add protection against other forms of hardware attacks such as side-channel attacks on cryptographic algorithms.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] M. Hassanalieragh et al., "Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges," in Proc. IEEE Int. Conf. Services Comput., Sep. 2015, pp. 285–292.

[3] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," IEEE Pervasive Comput., vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[4] J. Wei, "How wearables intersect with the cloud and the Internet of Things: Considerations for the developers of wearables," IEEE Consum. Electron. Mag., vol. 3, no. 3, pp. 53–56, Mar. 2014.

[5] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in Proc. Black Hat Conf. Presentation Slides, 2011. [Online]. Available: https://media.blackhat.com/bhus11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf.

[6] H. Kim, R. F. Yazicioglu, T. Torfs, P. Merken, H.-J. Yoo, and C. Van Hoof, "A low power ECG signal processor for ambulatory arrhythmia monitoring system," in Proc. IEEE Symp. VLSI Circuits, Sep. 2010.

[7] H. Kim, R. F. Yazicioglu, P. Merken, C. Van Hoof, and H.-J. Yoo, "ECG signal compression and classification algorithm with quad level vector for ECG holter system," IEEE Trans. Inf. Technol. Biomed., Jan. 2010.

[8] R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker you wear: A security analysis of wearable health trackers," in Proc. ACM Symp. Appl. Comput., 2016

[9] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Cardiac implantable medical devices forensics: Postmortem analysis of lethal attacks scenarios," *Digit. Investigat.*, to be published.

[10] G. Zheng *et al.*, "Multiple ECG fiducially points based random binary sequence generation for securing wireless body area networks," *IEEE J. Biomed. Health Informat.*,2015.