RESEARCHERID
THOMSON REUTERS

[*Mounica* et al., 4(6): June, 2017*] ISSN: 234-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

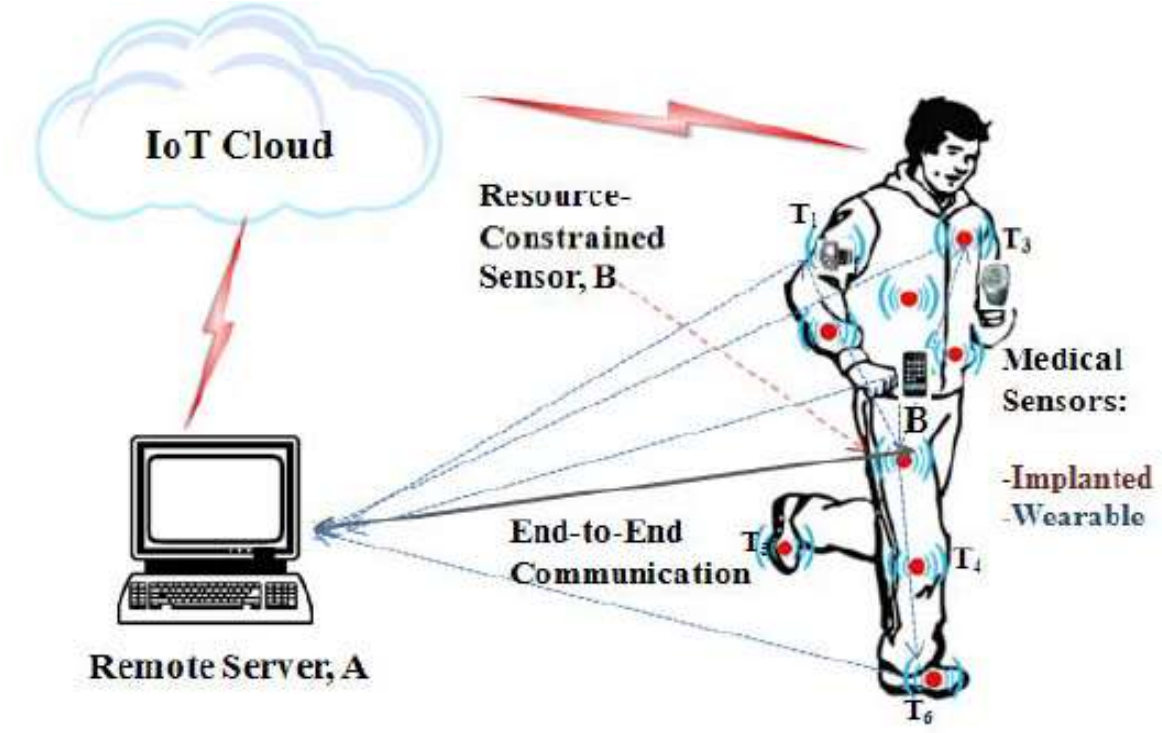
SECURED HEALTH RECORD MAINTENANCE AND HOUSE-HOLD DEVICE CONTROL OPERATIONS USING IOT

Mrs. Mounica B[*1], Aditya D Y[2] & Ajey Dinakar[3]
[*1]Assistant Professor, Department of Information Science, New Horizon College of Engineering, Bengaluru, India.
[2]Student, Department of Information Science, New Horizon College of Engineering, Bengaluru, India.
DOI: 10.5281/zenodo.163587

Keywords: Internet of Things, Healthcare, microcontroller, sensors, Wi-Fi/Bluetooth, Home automation.

Abstract
A Secured sensor based clever checking framework has swung to be incredibly outstanding in various applications, for instance, restorative, redirection, security, and business fields. A development in complete people close by an important developing part is driving quick ascents in social insurance costs. The social insurance framework is encountering an adjustment in which persevering seeing of patients is possible even without hospitalization. Pushed Sensors recognize unusual or unforeseen conditions by checking physiological parameters close by various signs. In this way, fundamental help can be given in times of urgent need. This Android based application is valuable for watching and controlling the family electronic contraptions with UART tradition. The customer can give orders from their flexible application to kill on or turn the electronic devices in light of their needs. This framework uses viable sensors and IoT based strategies that screen improvements and current health position of human. By using the IoT office these purposes of intrigue will be encoded and secured into the Cloud Server, subsequently of this any different individuals can view and screen the health records of patient wherever in the globe and a comparable framework can offer decisions to customers to control the family electronic devices through their Android convenient application.

Introduction
The Internet of Things (IoT) is an aggregate term for any of the many systems of sensors, actuators, processors, and PCs associated with the Internet. Healthcare applications for the IoT can possibly convey thorough patient care in different settings, including intense (in-doctor's facility), long haul (nursing homes), and group based (commonly, in-home). IoT can possibly precisely track individuals, hardware, examples, supplies, or even administration creatures and investigate the information caught. With patients joined to sensors to gauge fundamental signs and other biometric data, issues could be all the more quickly analyzed, a superior nature of care given, and assets utilized all the more effectively.



Existing Systems

Existing systems in healthcare and home automation can be to a great degree valuable in giving exact and dependable data on individuals' exercises and practices, along these lines guaranteeing a sheltered and sound living condition. . It might be that the shrewd sensors innovation will reform our life, social connection and exercises especially similarly that PCs have done a couple of decades back. Be that as it may, similar to all frameworks, the as of now existing frameworks have a few confinements and difficulties that should be tended to.

The present frameworks portray the arrangement of an essential, negligible exertion Microcontroller based heart rate with LCD yield. Heart rate of the subject is measured from the thumb finger using IRD (Infrared Device sensors and the rate is then touched base at the midpoint of and appeared on a substance based LCD). The device LCD demonstrating the heart beat rat and counting values through sending thumps from the sensor.

Limitations

- Data loss while converting analog to Digital.
- Accuracy is less.
- Delay in Real time Data transmission.
- Security Problem Causes while communication with Server.
- No powerful Cryptographic Procedures.
- Not an integration of multiple applications in same scenario.
- No temperature estimation.
- Remote observing is unrealistic.

The inclusion of sensors was a progressive step in healthcare frameworks. The sensors helped checking the pulse rate of the patient, temperature and mugginess of the patient's room. The worry in this sort of strategies was the overwhelming cryptographic functions that ended up being exorbitant or rather non-effective on the asset compelled hubs. The encryption can't be evacuated since the information is exceedingly private. In this

way, there should be some technique to offload these substantial cryptographic functions onto the less asset compelled sensor hubs so that the asset obliged hubs can perform proficiently with a specific end goal to screen healthcare information. The proficient usage of the vitality is basically required because of expanding interest in vitality utilization. In any case, there is a requirement for a solitary application that would deal with such different situations effectively.

Proposed System

Motivation

The primary motto of this framework is to screen the health records of the patients and controlling the family devices by means of Android Application and keep up the subtle elements into the server by means of Internet of Things with proficient cryptographic process.

The proposed framework examines about building up a successful framework for healthcare checking and home automation. In this framework we plan to have an equipment unit and also an android application.

Hardware Kit

The hardware kit proposed incorporates a pulse sensor that when put on the patient's finger, numbers the heart pulsates. The following segment in the kit is accelerometer, which monitors the patient's developments. Temperature and humidity sensors are likewise incorporated into request to gauge temperature and humidity of the patient's room separately. A Bluetooth device is important to associate the whole kit to the client's android device. A 2-channel hand-off is likewise actualized. A DC fan and an AC bulb are likewise included on the kit. Every one of these parts are controlled by a focal microcontroller chip. The readings gathered by the kit and furthermore the fan and light are all together taken care of by the android application. The readings can likewise be appeared on a webpage.

Android Application

The android application is utilized by the doctors and patient's relatives or companions. The client needs to associate with the hardware kit depicted above by utilizing the Bluetooth association. The points of interest of the patient are then to be enlisted in the application. In the event that there is any irregularity in the patient's sensor information, the disturbing notice is sent to his/her relatives or companions and the specialist. Likewise the working of fan and light actualized in the hardware kit can be controlled by the proposed android application.

The framework guarantees the accompanying:

1. Records will be proficiently and precisely put away in the server. It will require least time for the general population to get the disturbing message.
2. Minimal wastage of vitality if there should arise an occurrence of savvy home computerization by controlling the working of light and fans viably through the android application.

Enhancements

- Compact size
- Multiple Sensors are used.
- Monitor the patient's room temperature, room humidity level, heart rate and position of the patient.
- Integrating Health record monitoring with Electronic Device Handling system is useful to all users to operate the devices from the place itself not even to move for device on/off operations.

Hardware Description

ATmega 328

The ATmega328P gives the accompanying components: 32K bytes of In-System Programmable Flash with Read-While-Write abilities, 1K bytes EEPROM, 2K bytes SRAM, 23 universally useful I/O lines, 32 broadly useful working registers, three adaptable Timer/Counters with think about modes, inner and outside intrud es on,

a serial programmable USART, a byte-arranged 2-wire Serial Interface, a SPI serial port, a 6-channel 10-bit ADC (8 directs in TQFP and QFN/MLF bundles), a programmable Watchdog Timer with inside Oscillator, and five software selectable power sparing modes. The Idle mode stops the CPU while permitting the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and intrude on framework to keep working. The Power-down mode spares the enroll substance however solidifies the Oscillator, incapacitating all other chip functions until the following hinder or hardware reset. In Power-spare mode, the offbeat clock keeps on running, enabling the client to keep up a clock base while whatever is left of the device is resting. The ADC Noise Reduction mode stops the CPU and all I/O modules aside from nonconcurrent clock and ADC, to limit exchanging clamor amid ADC changes. In Standby mode, the precious stone/resonator Oscillator is running while whatever remains of the device is resting.

This permits quick start-up consolidated with low power utilization. The device is fabricated utilizing Atmel's high thickness non-unpredictable memory innovation. The On-chip ISP Flash enables the program memory to be reconstructed In-System through a SPI serial interface, by a traditional non-unstable memory software engineer, or by an On-chip Boot program running on the AVR center. The Boot program can utilize any interface to download the application program in the Application Flash memory. Software in the Boot Flash segment will keep on running while the Application Flash segment is refreshed, giving genuine Read-While-Write operation. By consolidating a 8-bit RISC CPU with In-System Self-Programmable Flash on a solid chip, the Atmel ATmega328P is an intense microcontroller that gives a very adaptable and practical answer for some implanted control applications. The ATmega328P AVR is bolstered with a full suite of program and framework advancement instruments including: C Compilers, Macro Assemblers, program Debugger/Simulators, In-Circuit Emulators, and Evaluation kits.

DHT11:

DHT11 Temperature and Humidity Sensor highlights a temperature and humidity sensor complex with an calibrated digital signal output. By utilizing the select advanced flag procurement system and temperature and humidity detecting innovation, it guarantees high unwavering quality and fantastic long haul strength. This sensor incorporates a resistive-sort humidity estimation segment and a NTC temperature estimation part, and associates with a superior 8-bit microcontroller, offering amazing quality, quick reaction, hostile to obstruction capacity and cost-adequacy. At the point when MCU sends a begin flag, DHT11 changes from the low-control utilization mode to the running-mode, sitting tight for MCU finishing the begin flag. When it is finished, DHT11 sends a reaction flag of 40-bit information that incorporate the relative humidity and temperature data to MCU. Clients can gather (read) a few information. Without the begin motion from MCU, DHT11 won't give the reaction flag to MCU. When information is gathered, DHT11 will change to the low power-utilization mode until it gets begin motion from MCU once more.

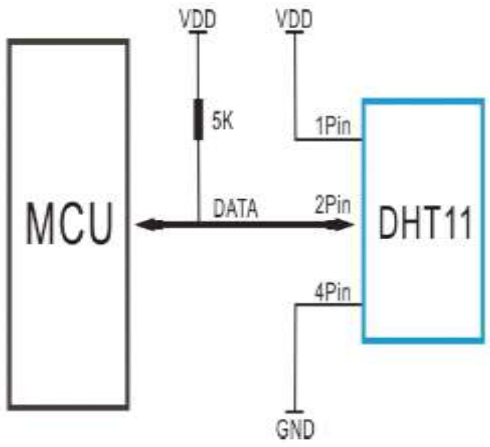


Fig. DHT11 Connectivity

Microcontroller

The AVR core combines a rich instruction set with 32 universally useful working registers. All the 32 registers are straightforwardly associated with the Arithmetic Logic Unit (ALU), enabling two free registers to be gotten to in one single guideline executed in one clock cycle. The subsequent design is more code productive while accomplishing throughputs up to ten times speedier than ordinary CISC microcontrollers. The ATmega328 gives the accompanying components: 32Kbytes of In-System Programmable Flash with Read-While-Write capabilities,1Kbytes EEPROM, 2Kbytes SRAM, 23 broadly useful I/O lines, 32 universally useful working registers, three adaptable Timer/Counters with look at modes, inside and outer interrupts, a serial programmable USART, a byte-arranged 2-wire Serial Interface, a SPI serial port, a 6-channel 10-bit ADC (8 directs in TQFP and QFN/MLF bundles), a programmable Watchdog Timer with inner Oscillator, and five software selectable power sparing modes.

The Idle mode stops the CPU while permitting the SRAM, Timer/Counters, USART, 2-wire Serial Interface, SPI port, and interrupt framework to keep working. The Power-down mode spares the enroll substance yet freezes the Oscillator, disabling all other chip functions until the following interrupt or hardware reset. In Power-spare mode, the asynchronous clock keeps on running, enabling the client to maintain a clock base while whatever is left of the device is sleeping. The ADC Noise Reduction mode stops the CPU and all I/O modules with the exception of asynchronous clock and ADC, to limit exchanging commotion amid ADC changes. In Standby mode, the precious stone/resonator Oscillator is running while whatever remains of the device is sleeping. This permits quick start-up consolidated with low power utilization.

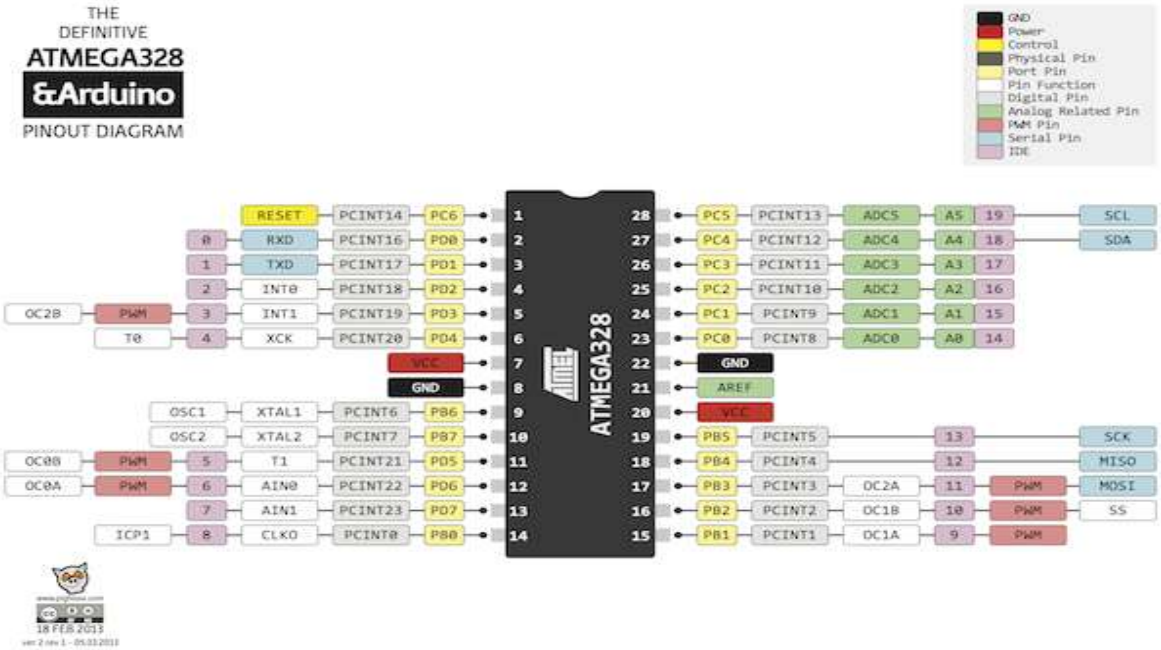


Image for Microcontroller ATMEGA328P with Pin Configuration

Arduino Board

Arduino is a group of single-board microcontrollers, pointed toward building intuitive items or situations in a simple way. The hardware comprises of open-source board plans in light of different 8-bit Atmel AVR microcontrollers or 32-bit Atmel ARM processors. The frameworks give sets of advanced and simple I/O sticks that can be interfaced to different augmentation sheets and different circuits. A few models additionally include a USB interface for stacking code from PCs. The primary Arduino was presented in 2005. Its architects tried to give a modest and simple route for specialists, understudies, and professionals to make devices that cooperate

with their condition utilizing sensors and actuators. Normal cases for learner specialists incorporate straightforward robots, indoor regulators and movement finders. Arduino sheets accompanied a straightforward incorporated improvement condition (IDE) that keeps running on normal PCs and enables clients to compose programs for Arduino utilizing C or C++.

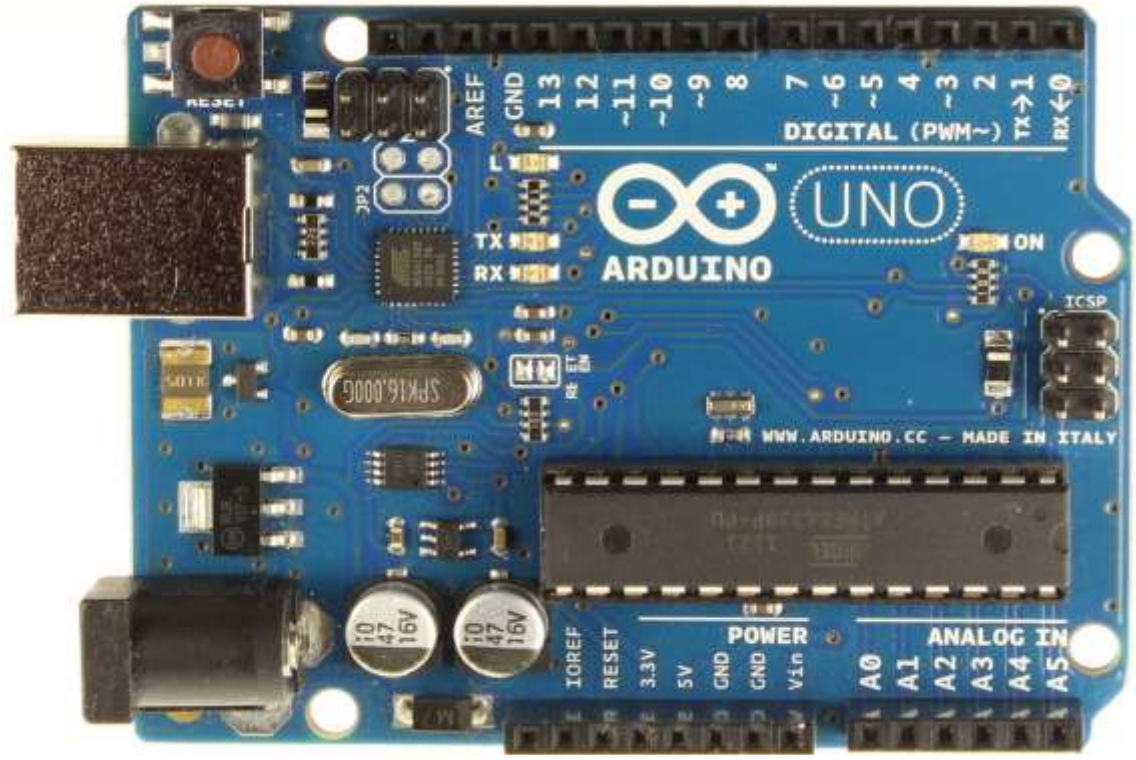


Image for Arduino Uno Board

LCD Display
Liquid Crystal Display which is generally known as Alphanumeric Display can show Alphabets, Numbers and additionally special symbols along with alphabets. Graphics display has embedded controller for controlling different modes. Controller acknowledges commands and information bytes from micro controller.

Bluetooth

Description: HC-05 is a class-2 bluetoothmodule with Serial Port Profile, which can design as either Master or slave. a Drop-in trade for wired serial connections, straightforward use. You can utilize it essentially for a serial port substitution to build up association between MCU, PC to your embedded project and so forth.
Software

Arduino Ide

Introduction

- Arduino is an open source computer hardware and software organization, venture and client group that outlines and makes kits for building advanced devices and intelligent articles that can detect and control the physical world. Arduino loads up might be bought preassembled, or as do it without anyone's help kits; in the meantime, the hardware outline data is accessible for the individuals who might want to amass an Arduino from scratch. The venture depends on a group of microcontroller

board plans made essentially by Smart Projects in Italy, and furthermore by a few different sellers, utilizing different 8bit Atmel AVR microcontrollers or 32bit Atmel ARM processors. These frameworks give sets of computerized and simple I/O sticks that can be interfaced to different expansion sheets and different circuits. The sheets highlight serial interchanges interfaces, including USB on a few models, for stacking programs from PCs. For programming the microcontrollers, the Arduino platform gives an integrated development environment (IDE) in view of the Processing venture, which incorporates bolster for C and C++ programming languages.

- The Arduino integrated development environment (IDE) is a cross platform application written in Java, and gets from the IDE for the Processing programming language and the Wiring ventures. It is intended to acquaint programming with craftsmen and different newcomers new to software development. It incorporates a code proofreader with components, for example, language structure highlighting, brace matching, and automatic indentation, and is additionally fit for assembling and transferring programs to the board with a solitary snap. A program or code composed for Arduino is known as a portray. Arduino programs are composed in C or C++. The Arduino IDE accompanies a software library called "Wiring" from the first Wiring venture, which makes numerous regular info/yield operations substantially less demanding. Clients just need characterize two functions to make a runnable cyclic executive program:
- **setup():** a function run once at the start of a program that can initialize settings
- **loop():** a function called repeatedly until the board powers off.

The EAGLE Schematic & PCB Layout Editor

This tutorial leads you through the means important to make a basic two-sided PCB utilizing EAGLE. This is really great however in view of the command-line interface to EAGLE. It is less demanding when figuring out how to utilize the simplified GUI, which we follow in this instructional exercise. This guide accept that you are planning a two-sided PCB with plated-through openings (PTH), the ordinary case, and upheld by the freeware adaptation of EAGLE giving your board is no bigger than 100mmX80mm. In the event that you need to download the freeware EAGLE to your own particular PC this is simple. Search for the most recent freeware rendition for your working framework and language (e.g. bird win-5.2.exe for windows XP and English). When you initially run the application, after establishment, tap the "keep running as freeware" catch. Bird can likewise be utilized to outline multi-layer and single-sided PCBs, non-PTH PCBs, and so on. It can likewise be effortlessly adjusted to deliver boards with coarser features, suitable for low quality optical procedures and manual manufacture:

In order to design a PCB, you need to complete the following steps:

1. Create a schematic sheet & add components
2. Add nets to the schematic (connect components)
3. Check schematic (Electrical Rule Check or ERC)
4. Create a board outline
5. Position components on the board
6. Route tracks between the components
7. Check board (Design Rule Check or DRC)
8. Pour copper to fill empty spaces on the board
9. (Optional) Add text legends to PCB layout
10. Perform Final Checks

In EAGLE the schematic design takes more often than not. The PCB format itself, steps 4-9, utilizes the magnificent implicit auto-router, and can be brisk if design is great, or inconceivable if design is awful. On the off chance that you set aside opportunity to reposition the parts painstakingly you will decrease the normal length of tracks, and improve high-recurrence execution from the board, and in addition guaranteeing that even thick formats can auto-route completely.

System Design

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development.

Modules

Key Agreement and Distribution Requirements

For key agreement protocol and authentication technique utilized inside the protocol itself, ordinarily asymmetric keys are utilized. As symmetric key based protocols require key refresh after a specific time, so they are bad contender for key agreement and distribution protocols. Also, symmetric key based security protocols ask for pre-distribution prepare; a mind boggling setup [4]. At the point when sensors have compelled resources, exceptional consideration is needed a protected E2E channel considering the capacities of the both finishes.

Accelerometers and Acceleration Measurement

As depicted before that the overwhelming computational errands of asymmetric key agreement and distribution is registered by offloading them to the neighboring hubs with enough resources. Choice of these neighboring hubs is made by confirming whether they are introduced or worn-on the body. These sensor hubs are accepted to have an additional tri-hub accelerometer going with, of an indistinguishable sort from cell phone (door) has integrated to think about information straightforwardly to find connections. Since accelerometers are small, shabby and require little vitality to work, this is a sensible presumption and achievable to actualize. Only for a case, the freescale MMA845xQ line of accelerometers expenses about a few dollars and expend "1.8 miniaturized scale amps in standby mode and as low as 6 smaller scale amps in dynamic mode" [11], [2]. Though accelerometers utilized in our work are LIS3DSH, (created by Mouser Electronics) utilized as a part of Broadcom WICED Sense Bluetooth keen sensor development kit, Figure 1.

They have comparative cost as freescale MMA845xQ line of accelerometers. LIS3DSH accelerometer is a ultra-low-control elite three-pivot linear accelerometer having a place with the "nano" family with an installed state machine that can be programmed to actualize self-ruling applications. It has powerfully selectable full sizes of ±2g/±4g/±6g/±8g/±16g and is fit for measuring increasing speeds with yield information rates from 3.125 Hz to 1.6 kHz [10].

Accelerometers recognize constrain acting the other way to the relocation vector and measured speeding up should be remedied for the gravitational impact. The crude information from cell phone and sensors' accelerometers is changed over to discernable information through adjustment. Accelerometer's crude information is given in neighborhood device arranges; tomahawks introductions change if the device introduction is lost. Like if the device is turned on its side, the Z-pivot at no time in the future focuses upwards; rather it is additionally pivoted, Figure 1(c). While the speeding up vectors can be utilized to decide the roll and pitch edges, these qualities may not be proper for ongoing estimations. So the presumption is made that introduction of the cell phone is not changed as for position of the sensor introduced on the body. Consequently, the changes are not required to think about information for connections. Additionally the speeding up estimations are thought to be standardized, the device measured gravity with a unit esteem.

Authentication and Correlation of Data

As our approach relies on upon recognizable acceleration events, the calculation performs authentication if the client is moving. Likewise information for a brief term makes may prompt mistaken outcomes (false positives and false negatives). The cell phone functioning as portal records information from sensors' accelerometers to start the authentication procedure of neighboring sensor.In the event that if any sensor is expelled from the body, it loses the status of validated put stock in sensor. This trust authentication strategy is depicted beneath from the cell phone insightful.

Network Model

In the body area organize health observing situation outlined in Figure 2, it comprises of heterogeneous resources medicinal sensors going with tri-hub accelerometers embedded and worn-on the body of individual alongside a cell phone functioning as portal (or base station). Among this sensors introduced on body and other gear (computers, advanced cells, iPads and sensor devices, observation sensors working in the region healing facility or home environment), embedded sensors on human body are profoundly resource obliged hubs and may be situated in un-open places inside body too (i.e., supplanting batteries is incomprehensible, needs surgery). Along these lines, our concentration is to safeguard their vitality resources and is basically vital with the condition to have an E2E secure correspondence to secure their information. These sensors and devices are ordered into various classifications as takes after:

1. Highly resource-constrained nodes, unable to perform asymmetric operations such as implanted sensors.
2. Less resource constrained sensors, able to perform asymmetric operations required by the key agreement protocol having accelerometers integrated with them including the smartphone working as a gateway.
3. Devices or sensors with no constrains on resources (energy, computing power or storage capabilities) such as remote servers, workstations or laptops etc. If the remote server A wants to communicate with highly resource-constrained sensor B having no prior shared key or secured connection to get some data, an E2E key distribution protocol is needed to establish a secure channel between them for further communications. B delegates its expensive cryptographic tasks required for asymmetric key agreement to its neighboring trusted sensors installed on the body for assistance.

Selection of Assisting Nodes

Selection of helping trusted sensors in B's vicinity is made by seeing if they are introduced on the body. On the off chance that any such sensor hub's accelerometer information is not associated with the Smartphone's accelerometer information; suggests that this particular sensor is not trustful and is not included in allotting any undertaking to contribute in key agreement mechanism. As sensors can't be introduced without the permission and knowledge of individual so are viewed as dependable at first. Besides, if any such neighboring hub is traded off, its mutual pair-wise key with the sensor hub and entryway is denied compelling it to instate rekeying process. The proposed protocol in this way precludes the disclosure danger and keeps working regardless of the possibility that a neighboring sensor ends up plainly inaccessible.

Assumptions

1. Each sensor node has a pair-wise secret key with its neighboring nodes/trusted devices as K1r, K2r, K3r,…Knr after the initialization phase through a process of bootstrapping using a trusted key management server.
2. The resource-constrained sensor nodes are available to discover a set of trusted high-resources sensor nodes in their neighborhood by finding the data correlations through accelerometers data (provided by gateway).

Conclusion

- This paper shows the various solutions for healthcare systems and smart home automation.
- The powerful encryption methods have been discussed.
- The encryption methods have been implemented on the resource constrained sensors effectively by offloading them on the trusted nodes.
- The need of patient's caretaker to be always present near the patient to monitor them has been resolved.
- The mobile phone application holder can control the household device operations from a distance which provides flexibility for his movements or the user can carry on with his work and operate the device operations from his workplace.
- The whole system deals with security of the healthcare data and smart home automation which deals with conserving energy.

References

[1] D. E Vans, The Internet of Things: How the Next Evolution of the Internet is Changing Everything, Cisco Internet Business Solutions Group (IBSG), 2011.
[2] J L. Atzori, A. Lera, G. Morabioto, The internet of things: a survey, Comput. Netw. 54(15) (2010) 2787–2805.
[3] T. Kivinen, "Minimal IKEv2," draft-kivinen-ipsecme-ikev2-minimal-01 (WiP), IETF, 2012.
[4] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Lightweight collaborative key establishment scheme for the Internet of Things," Computer Networks, vol. 64, no. 0, pp. 273 – 295, 2014.
[5] S. Raza, S Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig. "Securing communication in 6LoWPAN with compressed IPsec". In: International conference on distributed computing in sensor systems and workshops (DCOSS). IEEE; 2011. p. 1–8.
[6] R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, "Tailoring End-to-End IP Security Protocols to the Internet of Things," in Proc. of IEEE ICNP, 2013.
[7] S. Santesson and H. Tschofenig, "Transport Layer Security (TLS) Cached Information Extension," draft-ietf-tls-cached-info-16 (WiP), IETF, 2014.
[8] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, IETF, 2012.
[9] A. J. Menezes , S. A. Vanstone , P. C. Van Oorschot, Handbook of Applied Cryptography, CRC Press, Inc., Boca Raton, FL, 1996.
[10] Mouser Electronics STMicroelectronics LIS3DSH accelerometers specification.
[11] Freescale Semiconductor. FreescaleXtrinsic accelerometers optimize resolution and battery life in consumer devices, September 2010.
[12] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (1976) 644–654.
[13] R. Moskowitz and R. Hummen, "HIP Diet EXchange (DEX)," draftmoskowitz-hip-dex-01 (WiP), IETF, 2012.
[14] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723, 2013.
[15] C. T. Cornelius, D. F. Kotz, Recognizing whether sensors are on the same body, Pervasive and Mobile Computing, Volume 8, Issue 6, December 2012, Pages 822–836