

SMART SECURITY DEVICE FOR WOMEN SAFETY

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Engineering degree in Electronics and Communication Engineering

By

PANNEM LEELA KRISHNA KRISHNA SAI(37130298)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

APRIL 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119

www.sathyabama.ac.in



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **PANNEM LEELA KRISHNA SAI(37130298)** who carried out the project entitled **"SMART SECURITY DEVICE FOR WOMEN SAFETY"** under our supervision from December 2020 to April 2021.

Internal Guide

MS. D. JAMUNA RANI M.E., (Ph.D.,)

Head of the Department

Dr. T. RAVI M.E., Ph.D.

Submitted for Viva voice Examination held on _____

INTERNAL EXAMINER

EXTERNAL EXAMINER

DECLARATION

I **PANNEM LEELA KRISHNA SAI (37130298)** hereby declare that the Project Report entitled **SMART SECURITY DEVICE FOR WOMEN SAFETY** done by us under the guidance of **MS. D. JAMUNA RANI M.E., (Ph.D.,)** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **ELECTRONICS AND COMMUNICATION ENGINEERING.**

DATE : 19/04/2021

PLACE:

PANNEM LEELA KRISHNA SAI (37130298)

SIGNATURE OF CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. We are grateful to them.

I convey my thanks to **Dr. N. M. NANDHITHA, M.E., Ph.D.**, Dean School of Electrical and Electronics and **Dr. T. RAVI, M.E., Ph.D.**, Head of the Department of Electronics and Communication Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **MS. D. JAMUNA RANI, M.E., (Ph.D.)** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of our project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the Department of Electronics and Communication Engineering who were helpful in many ways for the completion of the project.

ABSTRACT

The software or application has access to GPS and Messaging services which is pre-programmed in such a way that whenever it receives emergency signal, it can send help request along with the location co-ordinates to the nearest Police station, relatives and the people in the near radius who have application. This action enables help instantaneously from the Police as well as Public in the near radius who can reach the victim with great accuracy. Today in the current global scenario, the prime question in every girl's mind, considering the ever rising increase of issues on women harassment in recent past is mostly about her safety and security. The only thought haunting every girl is when they will be able to move freely on the streets even in odd hours without worrying about their security. This paper suggests a new perspective to use technology for women safety. Indian Women Are Harassed, Raped, Killed Every Day!!” That's a way beyond HUGE number! We propose an idea which changes the way everyone thinks about women safety.

A day when media broadcasts more of women's achievements rather than harassment, it's a feat achieved! Since we (humans) can't respond aptly in critical situations, the need for a device which automatically senses and rescues the victim is the venture of our idea in this paper. We propose to have a device which is the integration of multiple devices, hardware comprises of a wearable “Smart band” which continuously communicates with Smart phone that has access to the internet. The application is programmed and loaded with all the required data which includes Human Behaviour and reactions to different situations like anger, fear and anxiety. This generates a signal which is transmitted to the smart phone

CHAPTER	TABLE OF CONTENT	PAGE NUMBER
	ABSTRACT	v
1	INTRODUCTION	1
2	LITERATURE SURVEY	3
3	SYSTEM DESIGN	4
	3.1 Internet of Things	4
	3.2 Existing Process	5
	3.3 Applications	6
	3.4 Media	7
	3.5 Manufacturing Network	8
	3.6 Energy Management	9
	3.7 Unique Address-ability Of Things	11
4	TREND AND CHARACTERISTICS	12
	4.1 Intelligence	12
	4.2 Architecture	12
	4.3 Network Architecture	13
	4.4 Complexity	13
	4.5 Space Considerations	13
5	ENABLING TECHNOLOGIES FOR IOT	15
	5.1 Short range wireless	15
	5.3 Medium Range Wireless	15
6	CRITICISM AND CONTROVERSIES	16
	6.1 Platform Fragmentation	16
	6.2 Privacy,autonomy & control	16

	6.3	Data Storage and Analytics	18
	6.4	Security	18
	6.5	Environmental Sustainability Impact	20
	6.6	International Obsolescence of Devices	20
7		IOT ADOPTION BARRIERS	22
	7.1	Complexity and unclear value	22
	7.2	Privacy and Security Concerns	22
	7.3	Traditional governance Structures	23
8		FLOW CHART	24
	8.1	Node MCU	25
	8.2	ESP8266 Arduino Core	25
	8.3	Node MCU Development Board	26
9		SENSORS AND ITS WORKING	27
	9.1	Tilt Sensor	27
	9.2	Specification Of Tilt Sensors	28
	9.3	Working Principle	29
	9.4	Heartbeat Sensor	29
	9.5	Principle of Heartbeat Sensor	30
	9.6	Working of Heartbeat Sensor	30
	9.7	Vibration Sensor	32
	9.8	Working of Vibration Sensor	33
	9.9	Parts for Design	36
	9.10	Pressure Sensor	37
10		ARDUINO IDE SOFTWARE	39
11		CONCLUSION	40
12		REFERENCES	41

LIST OF FIGURES

FIG .NO	CONTENT	PAGE NO.
8.1	BLOCK DIAGRAM	24
8.2	ESP8266	26
8.3	NODE MCU	26
9.1	TILT SENSOR	27
9.2	CIRCUIT DIAGRAM	30
9.3	HEART RATE SENSOR	31
9.4	LED	31
9.5	CIRCUIT DIAGRAM	32
9.6	PRESSURE FORCE DIAGRAM	34
9.7	CIRCUIT DIAGRAM	35
9.8	GRAPH	35
9.9	LDTO POLYMER	36
9.10	GRAPH	36
9.11	USB	37
9.12	PRESSURE SENSOR	38

CHAPTER 1

INTRODUCTION

This paper focuses on a security system that is designed merely to serve the purpose of providing security to women so that they never feel helpless while facing such social challenges. An advanced system can be built that can detect the location and health condition of person that will enable us to take action accordingly based on electronic gadgets like GPS receiver, body temperature sensor, GSM, Pulse rate sensor. We can make use of number of sensors to precisely detect the real time situation of the women in critical abusive situations. The heartbeat of a person in such situations is normally higher which helps make decisions along with other sensors like motion sensors to detect the abnormal motion of the women while she is victimized. The idea to develop a smart device for women is that it's completely comfortable and easy to use a compared with already existing women security solutions such as a separate garment, bulky belts and infamous mobile apps that are just very abstract and obsolete. The Smart band integrated with Smart phone has an added advantage so as to reduce the cost of the device and also in reduced size. The GPS and the GSM can be used of a smart phone. This also enables in reduced power use and that the watch can be installed with Bluetooth 4.0 BLE (Bluetooth Low Energy) which comes in handy for several days on a single shot of charge.

Development of the Internet of Things (IoT) is going on quicker, it is uniting a colossal number of points of interest, including devices, people and spots, to pass on and offer information, enhancing business quality and high ground and making new business opportunities. It is presently just a matter of time to see that the virtual and veritable match in a more cutting edge structure. Lately there has been a significant move in the IoT which moved from a unified structure to a perplexing network of decentralized smart devices.

This movement expanded networking and cloud enablement of a wide range of physical devices from machines through autos to home apparatuses. Through this change everything around us will be coordinated towards viable working, controlling, checking, reporting and data storing powered by smart chips. These will doubtlessly going to make our life super straightforwardness. As IoT is based on a wide range of semiconductor technologies, including power management devices, sensors and microchips execution so security prerequisites change extensively starting with one application then onto the next. The way that the accomplishment of smart homes, connected autos and Industry 4.0 production lines depend all that much on client certainty, simple to-utilize, and safeguard security

capacities. The more prominent the volume of delicate information exchange over the IoT is occurring the more noteworthy the danger of information and data fraud, device control, information adulteration, IP robbery and much server/system control. In this paper the talk will be on what is going ahead to make the IoT secured, what are the measures so far taken in development of dependable framework and what is the imminent answers for IoT in the setting of secured utilization of IoT devices in our regular life.

This is a security system that is designed to providing security to women so that they never feel helpless while facing such critical situations. An advanced system can be built that can detect the location and health condition of women that will enable us to take action accordingly.

We can make use of number of sensors to precisely detect the real time situation of the women in critical situations. The temperature of a women in such situations is normally higher which helps to make decisions. This paper focuses on a security system that is designed merely to serve the purpose of providing security to women so that they never feel helpless while facing such social challenges. An advanced system can be built that can detect the location and health condition of person that will enable us to take action accordingly based on electronic gadgets like IOT, body temperature sensor , GSM, Pulse rate sensor, buzzer and node MCU. We can make use of number of sensors to precisely detect the real time situation of the women in critical abusive situations. The heartbeat of a person in such situations is normally higher which helps make decisions along with other sensors like motion sensors to detect the abnormal motion of the women while she is victimized. The idea to develop a smart device for women is that it's completely comfortable and easy to use as compared with already existing women security solutions such as a separate garment, bulky belts and infamous mobile apps that are just very abstract and obsolete.

CHAPTER 2

LITERATURE SURVEY

Y. P. Singh Presented a paper on Comparative and Critical technical study of the privacy. Security and privacy are now critical factors in the successful introduction and acceptance of the Internet of Things. In the current situation, the important goal is to provide security to women from issues of women harassment. The only thought haunting every girl is when they will be able to move freely on the streets even at any time without worrying about their security. This paper suggests a new idea to use technology for women safety.

Hock Beng Lim, “A Soldier Health Monitoring System for Military Applications,” International Conference on Body Sensor Networks. ,this statistics released by the Country's National Crime Records Bureau(NCRB) had revealed” That’s a HUGE number! We propose an idea which changes the way everyone thinks about women safety. We propose to have a device which is the integration of multiple devices, hardware comprises of a wearable “Smart band” which continuously communicates with Smart phone that has access to the internet.

Mithun Petal. discussed Patient Monitoring System using the generates a signal which is transmitted to the smart phone. The application has access to GPS and Messaging services which is pre-programmed in such a way that whenever it receives emergency signal, it can send help request along with the location co-ordinates to the nearest Police station, relatives. This action enables help instantaneously from the Police.

M.Goyal published a paper on New Epoch of Wireless Communication. In this paper the system intends to a wireless technique in the form of embedded device namely Raspberry Pi for women that will serve the purpose of alerts and way of communicating with secure channels and it captures the image using R-pi camera. There are many android applications for women safety but they as not as much as efficient. So to solve this issue of women safety we developed a prototype which is easy to use and which is efficient to provide help to that victim. so when the victim press kits button, our application will capture the photo, collect users information

CHAPTER-3

SYSTEM DESIGN

3.1 INTERNET OF THINGS:

The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" and for these purposes a "thing" is "an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks".

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications.

The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a smart grid, and expanding to areas such as smart cities. "Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring, or field

operation devices that assist firefighters in search and rescue operations. Legal scholars suggest regarding "Things" as an "inextricable mixture of hardware, software, data and service". These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include home automation (also known as smart home devices) such as the control and automation of lighting, heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring. As well as the expansion of Internet-connected automation into a plethora of new application areas, IoT is also expected to generate large amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process such data more effectively. IoT is one of the platforms of today's Smart City, and Smart Energy Management Systems.

3.2 Existing Process

As of 2016, the vision of the Internet of things has evolved due to a convergence of multiple technologies, including ubiquitous wireless communication, real-time analytics, machine learning, commodity sensors, and embedded systems. This means that the traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things (IoT). The concept of a network of smart devices was discussed as early as 1982, with a modified Coke machine at Carnegie Mellon University becoming the first Internet-connected appliance, able to report its inventory and whether newly loaded drinks were cold. Mark Weiser's seminal 1991 paper on ubiquitous computing,

"The Computer of the 21st Century", as well as academic venues such as UbiComp and PerCom produced the contemporary vision of IoT. In 1994 Reza Raji described the concept in IEEE Spectrum as "[moving] small packets of data to a large set of nodes, so as to integrate and automate everything from home appliances to entire factories". Between 1993 and 1996 several companies proposed solutions like Microsoft's at Work or Novell's NEST. However, only in 1999 did the field start gathering momentum. Bill Joy envisioned Device to Device (D2D) communication as part of his "Six Webs" framework, presented at the World Economic Forum at Davos in 1999. The concept of the Internet of things became popular in 1999, through the Auto-ID Centre at MIT and related market-analysis publications.

3.3 Applications

According to Gartner, Inc. (a technology research and advisory corporation), there will be nearly 20.8 billion devices on the Internet of things by 2020. ABI Research estimates that more than 30 billion devices will be wirelessly connected to the Internet of things by 2020. As per a 2014 survey and study done by Pew Research Internet Project, a large majority of the technology experts and engaged Internet users who responded—83 percent—agreed with the notion that the Internet/Cloud of Things, embedded and wearable computing (and the corresponding dynamic systems) will have widespread and beneficial effects by 2025. As such, it is clear that the IoT will consist of a very large number of devices being connected to the Internet. In an active move to accommodate new and emerging technological innovation, the UK Government, in their 2015 budget, allocated £40,000,000 towards research into the Internet of things. The former British Chancellor of the Exchequer George Osborne, posited that the Internet of things is the next stage of the information revolution and referenced the inter-connectivity of everything from urban transport to medical devices to household appliances.

The ability to network embedded devices with limited CPU, memory and power resources means that IoT finds applications in nearly every field. Such systems could be in charge of collecting information in settings ranging from natural ecosystems to buildings and factories, thereby finding applications in fields of environmental sensing and urban planning. On the other hand, IoT systems could also be responsible for performing actions, not just sensing things. Intelligent shopping systems, for example, could monitor specific users' purchasing habits in a store by tracking their specific mobile phones. These users could then be provided with special offers on their favourite products, or even location of items that they need, which their fridge has automatically conveyed to the phone. Additional examples of sensing and actuating are reflected in applications that deal with heat, water, electricity and energy management, as well as cruise-assisting transportation systems.

Other applications that the Internet of things can provide is enabling extended home security features and home automation. The concept of an "Internet of living things" has been proposed to describe networks of biological sensors that could use cloud-based analyses to allow users to study DNA or other molecules. However, the application of the IoT is not only restricted to these areas. Other specialized use cases of the IoT may also exist. An overview of some of the most prominent application areas is provided here.

3.4 Media

In order to hone the manner in which things, media and big data are interconnected, it is first necessary to provide some context into the mechanism used for media process. It has been suggested by Nick Couldry and Joseph Turow that practitioners in media approach big data as many actionable points of information about millions of individuals. The industry appears to be moving away from the traditional approach of using specific media environments such as newspapers, magazines, or television shows and instead tap into consumers with technologies that reach targeted people at optimal times in optimal locations. The ultimate aim is of course to serve, or convey, a message or content that is (statistically speaking) in line with the consumer's mind-set.

For example, publishing environments are increasingly tailoring the messages (advertisements) and content (articles) to appeal to consumers that have been exclusively gleaned through various data-mining activities. The media industries process big data in a dual, interconnected manner: Targeting of consumers (for advertising by marketers) Data-capture Thus, the Internet of things creates an opportunity to measure, collect and analyse an ever-increasing variety of behavioural statistics. Cross-correlation of this data could revolutionise the targeted marketing of products and services. For example, as noted by Danny Meadows-Klue, the combination of analytics for conversion tracking with behavioural targeting has unlocked a new level of precision that enables display advertising to be focused on the devices of people with relevant interests.

Big data and the IoT work in conjunction. From a media perspective, data is the key derivative of device interconnectivity, whilst being pivotal in allowing clearer accuracy in targeting. The Internet of things therefore transforms the media industry, companies and even governments, opening up a new era of economic growth and competitiveness. The wealth of data generated by this industry (i.e. big data) will allow practitioners in advertising and media to gain an elaborate layer on the present targeting mechanisms used by the industry.

Environmental monitoring applications of the IoT typically use sensors to assist in environmental protection by monitoring air or water quality, atmospheric or soil conditions, and can even include areas like monitoring the movements of wildlife and their habitats. Development of resource constrained devices connected to the Internet also means that other applications like earthquake or tsunami early-warning systems can also be used by emergency services to provide more effective aid. IoT devices in this application typically

span a large geographic area and can also be mobile. It has been argued that the standardization IoT brings to wireless sensing will revolutionize this area.

Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms is a key application of the IoT. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It can also be used for scheduling repair and maintenance activities in an efficient manner, by coordinating tasks between different service providers and users of these facilities. IoT devices can also be used to control critical infrastructure like bridges to provide access to ships. Usage of IoT devices for monitoring and operating infrastructure is likely to improve incident management and emergency response coordination, and quality of service, up-times and reduce costs of operation in all infrastructure related areas. Even areas such as waste management can benefit from automation and optimization that could be brought in by the IoT.

3.5 Manufacturing Network

Control and management of manufacturing equipment, asset and situation management, or manufacturing process control bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks, by networking machinery, sensors and control systems together. Digital control systems to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT.

But it also extends itself to asset management via predictive maintenance, statistical evaluation, and measurements to maximize reliability. Smart industrial management systems can also be integrated with the Smart Grid, thereby enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors. The National Science Foundation established an Industry/University Cooperative Research Center on intelligent maintenance systems (IMS) in 2001 with a research focus to use IoT-based predictive analytics technologies to monitor connected machines and to predict machine degradation, and further to prevent potential failures. The vision to achieve near-zero breakdown using IoT-based predictive analytics led the future development of e-manufacturing and

maintenance activities. The term IIoT (Industrial Internet of Things) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT. IIoT in manufacturing could generate so much business value that it will eventually lead to the fourth industrial revolution, so the so-called Industry 4.0.

It is estimated that in the future, successful companies will be able to increase their revenue through Internet of things by creating new business models and improve productivity, exploit analytics for innovation, and transform workforce. The potential of growth by implementing IIoT will generate \$12 trillion of global GDP by 2030 while connectivity and data acquisition are imperative for IIoT, they should not be the purpose, rather the foundation and path to something bigger. Among all the technologies, predictive maintenance is probably a relatively "easier win" since it is applicable to existing assets and management systems. The objective of intelligent maintenance systems is to reduce unexpected downtime and increase productivity. And to realize that alone would generate around up to 30% over total maintenance costs. Industrial big data analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data. Cyber-physical systems (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes. An IoT-enabled intelligent system of such cases has been demonstrated by the NSF Industry/University Collaborative Research Center for Intelligent Maintenance Systems (IMS) at University of Cincinnati on a band saw machine in IMTS 2014 in Chicago. Band saw machines are not necessarily expensive, but the band saw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics.

3.6 Energy management

Integration of sensing and actuation systems, connected to the Internet, is likely to optimize energy consumption as a whole. It is expected that IoT devices will be integrated into all forms of energy consuming devices (switches, power outlets, bulbs, televisions, etc.) and be able to communicate with the utility supply company in order to effectively balance power generation and energy usage. Such devices would also offer the opportunity for users to remotely control their devices, or centrally manage them via a cloud based interface, and

enable advanced functions like scheduling (e.g., remotely powering on or off heating systems, controlling ovens, changing lighting conditions etc.). Besides home based energy management, the IoT is especially relevant to the Smart Grid since it provides systems to gather and act on energy and power-related information in an automated fashion with the goal to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity. Using advanced metering infrastructure (AMI) devices connected to the Internet backbone, electric utilities can not only collect data from end-user connections, but also manage other distribution automation devices like transformers and reclosers.

IoT devices can be used to enable remote health monitoring and emergency notification systems. These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers, Fitbit electronic wristbands, or advanced hearing aids. Some hospitals have begun implementing "smart beds" that can detect when they are occupied and when a patient is attempting to get up. It can also adjust itself to ensure appropriate pressure and support is applied to the patient without the manual interaction of nurses. Specialized sensors can also be equipped within living spaces to monitor the health and general well-being of senior citizens, while also ensuring that proper treatment is being administered and assisting people regain lost mobility via therapy as well. Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. More and more end-to-end health monitoring IoT platforms are coming up for antenatal and chronic patients, helping one manage health vitals and recurring medication requirements.

IoT devices can be used to monitor and control the mechanical, electrical and electronic systems used in various types of buildings (e.g., public and private, industrial, institutions, or residential) in home automation and building automation systems. In this context, three main areas are being covered in literature: The integration of the internet with building energy management systems in order to create energy efficient and IOT driven "smart buildings". The possible means of real-time monitoring for reducing energy consumption and monitoring occupant behaviours. The integration of smart devices in the built environment and how they might be used in future applications.

The IoT can assist in integration of communications, control, and information processing across various transportation systems. Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user).

Dynamic interaction between these components of a transport system enables inter and intra vehicular communication, smart traffic control, smart parking, electronic toll collection systems, logistic and fleet management, vehicle control, and safety and road assistance.

A growing portion of IoT devices are created for consumer use. Examples of consumer applications include connected car, entertainment, residences and smart homes, wearable technology, quantified self, connected health, and smart retail. Consumer IoT provides new opportunities for user experience and interfaces. Some consumer applications have been criticized for their lack of redundancy and their inconsistency, leading to a popular parody known as the “Internet of Shit.”

3.7 Unique addressability of things

The original idea of the Auto-ID Center is based on RFID-tags and unique identification through the Electronic Product Code however this has evolved into objects having an IP address or URI. An alternative view, from the world of the Semantic Web focuses instead on making all things (not just those electronic, smart, or RFID-enabled) addressable by the existing naming protocols, such as URI. The objects themselves do not converse, but they may now be referred to by other agents, such as powerful centralized servers acting for their human owners.

Integration with the Internet implies that devices will use an IP address as a unique identifier. Due to the limited address space of IPv4 (which allows for 4.3 billion unique addresses), objects in the IoT will have to use the next generation of the Internet protocol (IPv6) to scale to the extremely large address space required. Internet of things devices additionally will benefit from the stateless address auto-configuration present in IPv6, as it reduces the configuration overhead on the hosts, and the IETF 6LoWPAN header compression. To a large extent, the future of the Internet of things will not be possible without the support of IPv6; and consequently the global adoption of IPv6 in the coming years will be critical for the successful development of the IoT in the future. A combination of these ideas can be found in the current GS1/EPCglobal EPC Information Services (EPCIS) specifications. This system is being used to identify objects in industries ranging from aerospace to fast moving consumer products and transportation logistics.

CHAPTER 4

TRENDS AND CHARACTERISTICS

4.1 Intelligence

Ambient intelligence and autonomous control are not part of the original concept of the Internet of things. Ambient intelligence and autonomous control do not necessarily require Internet structures, either. However, there is a shift in research to integrate the concepts of the Internet of things and autonomous control, with initial outcomes towards this direction considering objects as the driving force for autonomous IoT. In the future the Internet of things may be a non-deterministic and open network in which auto-organized or intelligent entities (Web services, SOA components), virtual objects (avatars) will be interoperable and able to act independently (pursuing their own objectives or shared ones) depending on the context, circumstances or environments. Autonomous behavior through the collection and reasoning of context information as well as the objects ability to detect changes in the environment, faults affecting sensors and introduce suitable mitigation measures constitute a major research trend, clearly needed to provide credibility to the IoT technology. Modern IoT products and solutions in the marketplace use a variety of different technologies to support such context-aware automation but more sophisticated forms of intelligence are requested to permit sensor units to be deployed in real environments.

4.2 Architecture

The system will likely be an example of event-driven architecture, bottom-up made (based on the context of processes and operations, in real-time) and will consider any subsidiary level. Therefore, model driven and functional approaches will coexist with new ones able to treat exceptions and unusual evolution of processes (multi-agent systems, B-ADSc, etc.). In an Internet of things, the meaning of an event will not necessarily be based on a deterministic or syntactic model but would instead be based on the context of the event itself: this will also be a semantic web. Consequently, it will not necessarily need common standards that would not be able to address every context or use: some actors (services, components, avatars) will accordingly be self-referenced and, if ever needed, adaptive to existing common standards (predicting everything would be no more than defining a "global finality" for everything that is just not possible with any of the current top-down approaches and standardizations). Building on top of the Internet of things, the web of things is an

architecture for the application layer of the Internet of things looking at the convergence of data from IoT devices into Web applications to create innovative use-cases. In order to program and control the flow of information in the Internet of things, a predicted architectural direction is being called BPM Everywhere which is a blending of traditional process management with process mining and special capabilities to automate the control of large numbers of coordinated devices.

4.3 Network architecture

The Internet of things requires huge scalability in the network space to handle the surge of devices. IETF 6LoWPAN would be used to connect devices to IP networks. With billions of devices being added to the Internet space, IPv6 will play a major role in handling the network layer scalability. IETF's Constrained Application Protocol, ZeroMQ, and MQTT would provide lightweight data transport. "MQ" in "MQTT" came from IBM's MQ Series message queuing product line. Fog computing is a viable alternative to prevent such large burst of data flow through Internet. The edge devices' computation power can be used to analyse and process data, thus providing easy real time scalability.

4.4 Complexity

In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IoT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability. For example, Domestic Robotics (Domotics) running inside a smart home might only share data within and be available via a local network.

4.5 Space considerations

In the Internet of things, the precise geographic location of a thing—and also the precise geographic dimensions of a thing—will be critical. Therefore, facts about a thing, such as its location in time and space, have been less critical to track because the person processing the information can decide whether or not that information was important to the action being taken, and if so, add the missing information (or decide to not take the action). (Note that some things in the Internet of things will be sensors, and sensor location is usually

important. The GeoWeb and Digital Earth are promising applications that become possible when things can become organized and connected by location. However, the challenges that remain include the constraints of variable spatial scales, the need to handle massive amounts of data, and an indexing for fast search and neighbour operations. In the Internet of things, if things are able to take actions on their own initiative, this human-centric mediation role is eliminated. Thus, the time-space context that we as humans take for granted must be given a central role in this information ecosystem. Just as standards play a key role in the Internet and the Web, geospatial standards will play a key role in the Internet of things.

There are three core sectors of the IoT: enterprise, home, and government, with the Enterprise Internet of Things (EIoT) being the largest of the three. By 2019, the EIoT sector is estimated to account for nearly 40% or 9.1 billion devices.

According to the CEO of Cisco, the commercial opportunity for "connected products ranging from cars to household goods" is expected to be a \$USD 19 trillion. Many IoT devices have a potential to take a piece of this market. Jean-Louis Gassée (Apple initial alumni team, and BeOS co-founder) has addressed this topic in an article on Monday Note, where he predicts that the most likely problem will be what he calls the "basket of remotes" problem, where we'll have hundreds of applications to interface with hundreds of devices that don't share protocols for speaking with one another.

There are multiple approaches to solve this problem, one of them called the "predictive interaction", where cloud or fog based decision makers will predict the user's next action and trigger some reaction. For user interaction, new technology leaders are joining forces to create standards for communication between devices. While AllJoyn alliance is composed of the top 20 World technology leaders, there are also big companies that promote their own protocol like CCF from Intel. Manufacturers are becoming more conscious of this problem, In semi-open or closed loops (i.e. value chains, whenever a global finality can be settled) IoT will often be considered and studied as a complex system due to the huge number of different links, interactions between autonomous actors, and its capacity to integrate new actors. At the overall stage (full open loop) it will likely be seen as a chaotic environment (since systems always have finality). As a practical approach, not all elements in the Internet of things run in a global, public space. Subsystems are often implemented to mitigate the risks of privacy, control and reliability.

CHAPTER 5

ENABLING TECHNOLOGIES FOR IOT

There are many technologies that enable IoT. Crucial to the field is the network used to communicate between devices of an IoT installation, a role that several wireless or wired technologies may fulfil:

5.1 Short-range wireless

Bluetooth low energy (BLE) – Specification providing a low power variant to classic Bluetooth with a comparable communication range. Light-Fidelity (Li-Fi) – Wireless communication technology similar to the Wi-Fi standard, but using visible light communication for increased bandwidth. Near-field communication (NFC) – Communication protocols enabling two electronic devices to communicate within a 4 cm range. QR codes and barcodes – Machine-readable optical tags that store information about the item to which they are attached. Radio-frequency identification (RFID) – Technology using electromagnetic fields to read data stored in tags embedded in other items. Thread – Network protocol based on the IEEE 802.15.4 standard, similar to Zigbee, providing IPv6 addressing.

5.2 Long-range wireless

Low-power wide-area networking (LPWAN) – Wireless networks designed to allow long-range communication at a low data rate, reducing power and cost for transmission. Very small aperture terminal (VSAT) – Satellite communication technology using small dish antennas for narrowband and broadband data. Ethernet – General purpose networking standard using twisted pair and fiber optic links in conjunction with hubs or switches. Multimedia over Coax Alliance (MoCA) – Specification enabling whole-home distribution of high definition video and content over existing coaxial cabling. Power-line communication (PLC) – Communication technology using electrical wiring to carry power and data. Specifications such as Home Plug utilize PLC for networking IoT devices.

CHAPTER 6

Criticism and controversies

6.1 Platform fragmentation

IoT suffers from platform fragmentation and lack of technical standards a situation where the variety of IoT devices, in terms of both hardware variations and differences in the software running on them, makes the task of developing applications that work consistently between different inconsistent technology ecosystems hard. Customers may be hesitant to bet their IoT future on a proprietary software or hardware devices that uses proprietary protocols that may fade or become difficult to customize and interconnect. IoT's amorphous computing nature is also a problem for security, since patches to bugs found in the core operating system often do not reach users of older and lower-price devices. One set of researchers say that the failure of vendors to support older devices with patches and updates leaves more than 87% of active devices vulnerable.

6.2 Privacy, autonomy, and control

Philip N. Howard, a professor and author, writes that the Internet of things offers immense potential for empowering citizens, making government transparent, and broadening information access. Howard cautions, however, that privacy threats are enormous, as is the potential for social control and political manipulation. Concerns about privacy have led many to consider the possibility that big data infrastructures such as the Internet of things and Data Mining are inherently incompatible with privacy. Writer Adam Greenfield claims that these technologies are not only an invasion of public space but are also being used to perpetuate normative behavior, citing an instance of billboards with hidden cameras that tracked the demographics of passers-by who stopped to read the advertisement.

The Internet of Things Council compared the increased prevalence of digital surveillance due to the Internet of things to the conceptual panopticon described by Jeremy Bentham in the 18th Century. The assertion was defended by the works of French philosophers Michel Foucault and Gilles Deleuze. In *Discipline and Punish: The privacy of households could be compromised by solely analyzing smart home network traffic patterns without dissecting the contents of encrypted application data, yet a synthetic packet injection scheme can be used to safely overcome such invasion of privacy.* Peter-Paul Verbeek, a professor of philosophy of technology at the University of Twente, Netherlands, writes that

technology already influences our moral decision making, which in turn affects human agency, privacy and autonomy. He cautions against viewing technology merely as a human tool and advocates instead to consider it as an active agent. Justin Brookman, of the Center for Democracy and Technology, expressed concern regarding the impact of IoT on consumer privacy, saying that "There are some people in the commercial space who say, 'Oh, big data — well, let's collect everything, keep it around forever, we'll pay for somebody to think about security later.' The question is whether we want to have some sort of policy framework in place to limit that." Tim O'Reilly believes that the way companies sell the IoT devices on consumers are misplaced, disputing the notion that the IoT is about gaining efficiency from putting all kinds of devices online and postulating that "IoT is really about human augmentation.

The applications are profoundly different when you have sensors and data driving the decision-making." Editorials at WIRED have also expressed concern, one stating "What you're about to lose is your privacy. Actually, it's worse than that. You aren't just going to lose your privacy, you're going to have to watch the very concept of privacy be rewritten under your nose." The American Civil Liberties Union (ACLU) expressed concern regarding the ability of IoT to erode people's control over their own lives.

The ACLU wrote that "There's simply no way to forecast how these immense powers – disproportionately accumulating in the hands of corporations seeking financial advantage and governments craving ever more control – will be used. Chances are big data and the Internet of Things will make it harder for us to control our own lives, as we grow increasingly transparent to powerful corporations and government institutions that are becoming more opaque to us." In response to rising concerns about privacy and smart technology, in 2007 the British Government stated it would follow formal Privacy by Design principles when implementing their smart metering program.

The program would lead to replacement of traditional power meters with smart power meters, which could track and manage energy usage more accurately. However the British Computer Society is doubtful these principles were ever actually implemented. In 2009 the Dutch Parliament rejected a similar smart metering program, basing their decision on privacy concerns. The Dutch program later revised and passed in 2011.

6.3 Data storage and analytics

A challenge for producers of IoT applications is to clean, process and interpret the vast amount of data which is gathered by the sensors. There is a solution proposed for the analytics of the information referred to as Wireless Sensor Networks. These networks share data among sensor nodes that are send to a distributed system for the analytics of the sensory data. Another challenge is the storage of this bulk data. Depending on the application there could be high data acquisition requirements which in turn lead to high storage requirements. Currently the internet is already responsible for 5% of the total energy generated and this consumption will increase significantly when we start utilizing applications with multiple embedded sensors.

6.4 Security:

Concerns have been raised that the Internet of things is being developed rapidly without appropriate consideration of the profound security challenges involved and the regulatory changes that might be necessary. Most of the technical security issues are similar to those of conventional servers, workstations and smartphones, but the firewall, security update and anti-malware systems used for those are generally unsuitable for the much smaller, less capable, IoT devices. According to the Business Insider Intelligence Survey conducted in the last quarter of 2014, 39% of the respondents said that security is the biggest concern in adopting Internet of things technology.

In particular, as the Internet of things spreads widely, cyber-attacks are likely to become an increasingly physical (rather than simply virtual) threat. In a January 2014 article in Forbes, cyber-security columnist Joseph Steinberg listed many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats. Computer-controlled devices in automobiles such as brakes, engine, locks, hood and trunk releases, horn, heat, and dashboard have been shown to be vulnerable to attackers who have access to the on-board network.

In some cases, vehicle computer systems are Internet-connected, allowing them to be exploited remotely. By 2008 security researchers had shown the ability to remotely control pacemakers without authority. Later hackers demonstrated remote control of insulin pumps and implantable cardioverter defibrillators. David Pogue wrote that some recently published reports about hackers remotely controlling certain functions of automobiles were not as serious as one might otherwise guess because of various mitigating circumstances; such as

the bug that allowed the hack having been fixed before the report was published, or that the hack required security researchers having physical access to the car prior to the hack to prepare for it. The U.S. National Intelligence Council in an unclassified report maintains that it would be hard to deny "access to networks of sensors and remotely-controlled objects by enemies of the United States, criminals, and mischief makers... An open market for aggregated sensor data could serve the interests of commerce and security no less than it helps criminals and spies identify vulnerable targets.

Thus, massively parallel sensor fusion may undermine social cohesion, if it proves to be fundamentally incompatible with Fourth-Amendment guarantees against unreasonable search." In general, the intelligence community views the Internet of things as a rich source of data. As a response to increasing concerns over security, the Internet of Things Security Foundation (IoTSF) was launched on 23 September 2015. IoTSF has a mission to secure the Internet of things by promoting knowledge and best practice. Its founding board is made from technology providers and telecommunications companies including BT, Vodafone, Imagination Technologies and Pen Test Partners. In addition, large IT companies are continuously developing innovative solutions to ensure the security for IoT devices. As per the estimates from KBV Research, the overall IoT security market would grow at 27.9% rate during 2016-2022 as a result of growing infrastructural concerns and diversified usage of Internet of things. In 2016, a distributed denial of service attack powered by Internet of things devices running the Mirai malware took down a DNS provider and major web sites.

Given widespread recognition of the evolving nature of the design and management of the Internet of things, sustainable and secure deployment of IoT solutions must design for "anarchic scalability." Application of the concept of anarchic scalability can be extended to physical systems (i.e. controlled real-world objects), by virtue of those systems being designed to account for uncertain management futures. This "hard anarchic scalability" thus provides a pathway forward to fully realize the potential of Internet of things solutions by selectively constraining physical systems to allow for all management regimes without risking physical failure. Brown University computer scientist Michael Littman has argued that successful execution of the Internet of things requires consideration of the interface's usability as well as the technology itself. These interfaces need to be not only more user-friendly but also better integrated: "If users need to learn different interfaces for their vacuums, their locks, their sprinklers, their lights, and their coffeemakers, it's tough to say that their lives have been made any easier."

6.5 Environmental sustainability impact:

A concern regarding Internet of things technologies pertains to the environmental impacts of the manufacture, use, and eventual disposal of all these semiconductor-rich devices. Modern electronics are replete with a wide variety of heavy metals and rare-earth metals, as well as highly toxic synthetic chemicals. This makes them extremely difficult to properly recycle. Electronic components are often incinerated or placed in regular landfills. Furthermore, the human and environmental cost of mining the rare-earth metals that are integral to modern electronic components continues to grow. With production of electronic equipment growing globally yet little of the metals (from end-of-life equipment) are being recovered for reuse, the environmental impacts can be expected to increase.

Also, because the concept of Internet of things entails adding electronics to mundane devices (for example, simple light switches), and because the major driver for replacement of electronic components is often technological obsolescence rather than actual failure to function, it is reasonable to expect that items that previously were kept in service for many decades would see an accelerated replacement cycle if they were part of the IoT. For example, a traditional house built with 30 light switches and 30 electrical outlets might stand for 50 years, with all those components still original at the end of that period. But a modern house built with the same number of switches and outlets set up for IoT might see each switch and outlet replaced at five-year intervals, in order to keep up to date with technological changes. This translates into a ten-fold increase in waste requiring disposal.

6.6 Intentional obsolescence of devices:

The Electronic Frontier Foundation has raised concerns that companies can use the technologies necessary to support connected devices to intentionally disable or "brick" their customers' devices via a remote software update or by disabling a service necessary to the operation of the device. In one example, home automation devices sold with the promise of a "Lifetime Subscription" were rendered useless after Nest Labs acquired Revolv and made the decision to shut down the central servers the Revolv devices had used to operate. As Nest is a company owned by Alphabet (Google's parent company), the EFF argues this sets a "terrible precedent for a company with ambitions to sell self-driving cars, medical devices, and other high-end gadgets that may be essential to a person's livelihood or physical safety." Owners should be free to point their devices to a different server or collaborate on improved software.

Kevin Lonergan at Information Age, a business-technology magazine, has referred to the terms surrounding IoT as a “terminology zoo”. The lack of clear terminology is not “useful from a practical point of view” and a “source of confusion for the end user”. A company operating in the IoT space could be working in anything related to sensor technology, networking, embedded systems, or analytics. According to Lonergan, the term IoT was coined before smart phones, tablets, and devices as we know them today existed, and there is a long list of terms with varying degrees of overlap and technological convergence: Internet of Things (IoT), Internet of Everything (IoE), Industrial Internet, Pervasive Computing, Pervasive Sensing, Ubiquitous Computing,

Cyber-Physical Systems (CPS), Wireless Sensor Networks (WSN), Smart Objects, Cooperating Objects, Machine-to-Machine (M2M), Ambient Intelligence (AmI), Operational Technology (OT), and Information Technology (IT). Regarding IIoT, an industrial sub-field of IoT, the Industrial Internet Consortium's Vocabulary Task Group has created a "common and reusable vocabulary of terms" to ensure "consistent terminology" across publications issued by the Industrial Internet Consortium. IoT One has created an IoT Terms Database including a New Term Alert to be notified when a new term is published. As of March 2017, this database aggregates 711 IoT-related terms, however, without any attempts to reduce terminological ambiguity and complexity.

CHAPTER 7

IoT ADOPTION BARRIERS

7.1 Complexity and unclear value propositions:

Despite a shared belief in the potential of IoT, industry leaders and consumers are facing barriers to adopt IoT technology more widely. Dan Yarmoluk from ATEK Access Technologies has written that "the IoT industry appears heavily focused on gadgets and not making them relevant to the particular business verticals" and "can appear expensive and intimidating." Mike Farley has argued in Forbes that many IoT solutions are either too complex or lack a clear use case for end-users. "Instead of convincing consumers that they need complex systems to serve needs they don't have, we should fix real problems people struggle with every day."

Many gadgets in the consumer IoT space have appealed to early adopters, yet failed to demonstrate relevance to ordinary people's lives. In order to overcome barriers, "we need to stop making toys no one cares about and instead work on building simple solutions to real, everyday problems for real people." A recent study by Ericsson regarding the adoption of IoT among Danish companies, has suggested that many are struggling "to pinpoint exactly where the value of IoT lies for them". A company must identify where the value of IoT lies in order to capture it, otherwise non-action is the consequence. This indicates that a major roadblock to IoT adoption is not technical but analytical in nature.

7.2 Privacy and security concerns:

According to a recent study by Noura Aleisa and Karen Renaud at the University of Glasgow, "the Internet of Things' potential for major privacy invasion is a concern" with much of research "disproportionally focused on the security concerns of IoT." Among the "proposed solutions in terms of the techniques they deployed and the extent to which they satisfied core privacy principles", only very few turned out to be fully satisfactory. Louis Basenese, investment director at Wall Street Daily, has criticized the industry's lack of attention to security issues: "Despite high-profile and alarming hacks, device manufacturers remain undeterred, focusing on profitability over security. Consumers need to have ultimate control over collected data, including the option to delete it if they choose...Without privacy assurances, wide-scale consumer adoption simply won't happen."

7.3 Traditional governance structures:

A study issued by Ericsson regarding the adoption of Internet of things among Danish companies identified a "clash between IoT and companies' traditional governance structures, as IoT still presents both uncertainties and a lack of historical precedence." Among the respondents interviewed, 60 percent stated that they "do not believe they have the organizational capabilities, and three of four do not believe they have the processes needed, to capture the IoT opportunity." This has led to a need to understand organizational culture in order to facilitate organizational design processes and to test new innovation management practices.

A lack of digital leadership in the age of digital transformation has also stifled innovation and IoT adoption to a degree that many companies, in the face of uncertainty, "were waiting for the market dynamics to play out", or further action in regards to IoT "was pending competitor moves, customer pull, or regulatory requirements." Some of these companies risk being 'kodaked' - "Kodak was a market leader until digital disruption eclipsed film photography with digital photos" - failing to "see the disruptive forces affecting their industry" and "to truly embrace the new business models the disruptive change opens up." Scott Anthony has written in Harvard Business Review that Kodak "created a digital camera, invested in the technology, and even understood that photos would be shared online" but ultimately failed to realize that "online photo sharing was the new business, not just a way to expand the printing business.

CHAPTER 8

FLOW CHART

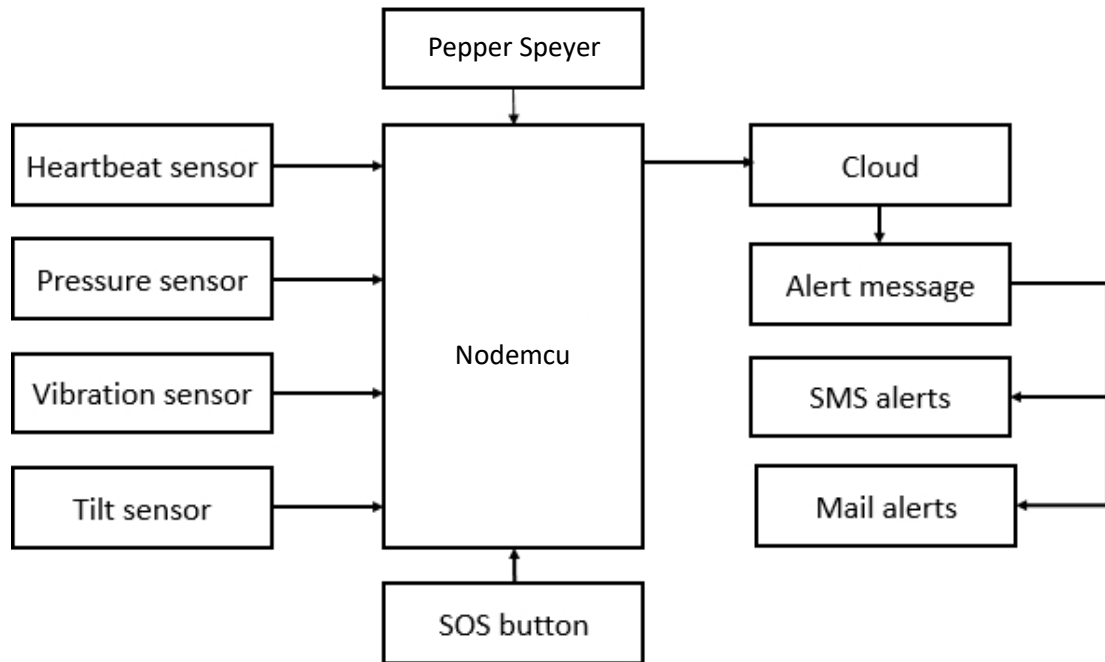


Fig.8.1:Block Diagram

HARDWARE USED:

- Nodemcu
- heartbeat sensor
- pressure sensor
- tilt sensor
- vibration sensor
- GPS
- SOS button

SOFTWARE USED:

- Arduino c

8.1 NODE MCU

NodeMCU is an open source IoT platform. It includes firmware which runs on the ESP8266 Wi-Fi SoC from Espressif Systems, and hardware which is based on the ESP-12 module. The term "NodeMCU" by default refers to the firmware rather than the development kits. The firmware uses the Lua scripting language. It is based on the eLua project, and built on the Espressif Non-OS SDK for ESP8266. It uses many open source projects, such as lua-cjson and SPIFFS

NodeMCU was created shortly after the ESP8266 came out. On December 30, 2013, Espressif Systems began production of the ESP8266. The ESP8266 is a Wi-Fi SoC integrated with a Tensilica Xtensa LX106 core, widely used in IoT applications (see related projects). NodeMCU started on 13 Oct 2014, when Hong committed the first file of nodemcu-firmware to GitHub. Two months later, the project expanded to include an open-hardware platform when developer Huang R committed the gerber file of an ESP8266 board, named devkit v0.9. Later that month, Tuan PM ported MQTT client library from Contiki to the ESP8266 SoC platform, and committed to NodeMCU project, then NodeMCU was able to support the MQTT IoT protocol, using Lua to access the MQTT broker. Another important update was made on 30 Jan 2015, when Devsaurus ported the u8glib to NodeMCU project, enabling NodeMCU to easily drive LCD, Screen, OLED, even VGA displays.

In summer 2015 the creators abandoned the firmware project and a group of independent contributors took over. By summer 2016 the NodeMCU included more than 40 different modules. Due to resource constraints users need to select the modules relevant for their project and build a firmware tailored to their needs.

8.2 ESP8266 Arduino Core

As Arduino.cc began developing new MCU boards based on non-AVR processors like the ARM/SAM MCU and used in the Arduino Due, they needed to modify the Arduino IDE so that it would be relatively easy to change the IDE to support alternate toolchains to allow Arduino C/C++ to be compiled for these new processors. They did this with the introduction of the Board Manager and the SAM Core. A "core" is the collection of software components required by the Board Manager and the Arduino IDE to compile an Arduino C/C++ source

file for the target MCU's machine language. Some ESP8266 enthusiasts developed an Arduino core for the ESP8266 WiFi SoC, popularly called the "ESP8266 Core for the Arduino IDE".^[16] This has become a leading software development platform for the various ESP8266-based modules and development boards, including NodeMCUs. NodeMCU is an open source LUA based firmware developed for ESP8266 wifi chip. By exploring functionality with ESP8266 chip, NodeMCU firmware comes with ESP8266 Development board/kit i.e. NodeMCU Development board.



Fig.8.2:ESP8266

8.3 NodeMCU Development Board

NodeMCU Dev Kit/board consist of ESP8266 wifi enabled chip. The ESP8266 is a low-cost Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. For more information about ESP8266, you can refer ESP8266 WiFi Module. There is Version2 (V2) available for NodeMCU Dev Kit i.e. NodeMCU Development Board), which usually comes in black colored PCB.



Fig.8.3:Node MCU

CHAPTER 9

SENSORS AND ITS WORKING

9.1 Tilt Sensors

Tilt sensors allow you to detect orientation or inclination. They are small, inexpensive, low-power and easy-to-use. If used properly, they will not wear out. Their simplicity makes them popular for toys, gadgets and appliances. Sometimes they are referred to as "mercury switches", (cylindrical is popular, although not always) and a conductive free mass inside, such as a blob of mercury or rolling ball. One end of the cavity has two conductive elements (poles). When the sensor is oriented so that that end is downwards, the mass rolls onto the

Tilt switches used to be made exclusively of mercury, but are rarer now since they are recognized as being extremely toxic. The benefits of mercury is that the blob is dense enough that it doesn't bounce and so the switch isn't susceptible to vibrations. On the other hand, ball-type sensors are easy to make, wont shatter, and pose no risk of pollution. While not as precise or flexible as a full accelerometer, tilt switches can detect motion or orientation simply. Another benefit to them is that the big ones can switch power on their own. Accelerometers, on the other hand, output digital or analog voltage that must then be analyzed with extra circuitry.

The benefits of mercury is that the blob is dense enough that it doesn't bounce and so the switch isn't susceptible to vibrations. On the other hand, ball-type sensors are easy to make, While not as precise or flexible as a full accelerometer, tilt switches can detect motion or orientation simply

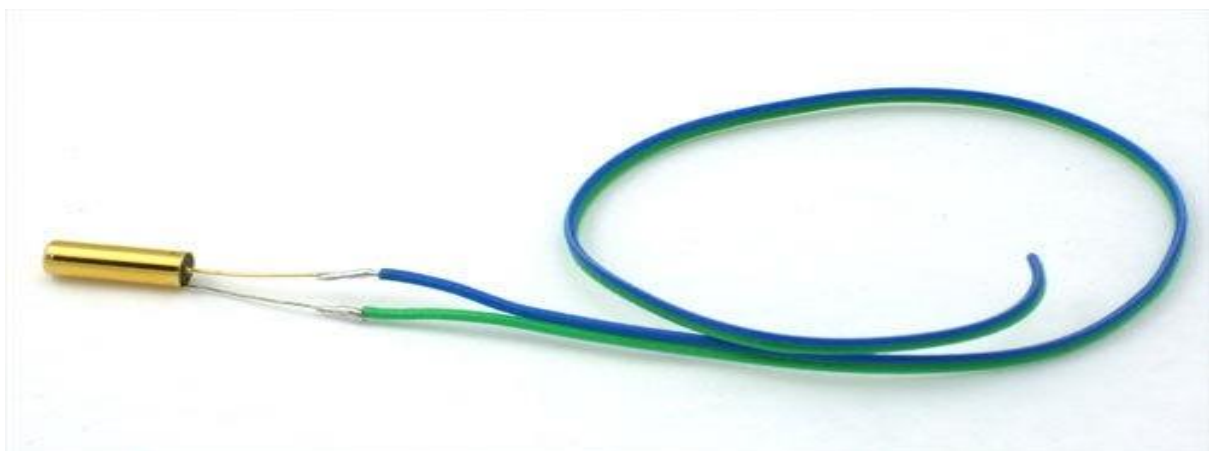


Fig.9.1:Tilt Sensor

9.2 Specifications of Tilt Sensors

The functionality of tilt sensors is influenced by factors such as gravity, vibration, temperature, zero offset, linearity, cross-axis sensitivity, acceleration/deceleration, and shock, clear line of sight between the user and the measured point, and calibration of tilt sensors.

The key specifications of tilt sensors include:

- **Number of axes:** The number of axes is an important factor as it varies from application to application. In robotics, a dual axes tilt sensor is used, in video game controllers and joysticks, a 3 axes tilt sensor is required, and in some smartphones, 4 axes sensors are used
- **Resolution:** The minimum inclination detected by the sensor is called its resolution
- **Sensitivity:** The sensor's ability to react to small changes is called its sensitivity
- **Measuring range:** The range of inclination that can be handled by the sensor is important. Some sensors are capable of measurements up to 10° while others can cover a range of up to 60°
- **Noise tolerance:** Noise tends to cause harmonic distortions in the function of the sensor, resulting in output variation and reduction of system efficiency. Manufacturer's guidelines regarding noise levels should be adhered to.
- **Vibration:** Vibrations can disrupt the sensor's functionality, and hence vibration resistance measures are required, especially when the sensors are used in harsh conditions like off-road vehicles or construction sites.

The Benefits of Tilt Sensors are:

The key benefits of tilt sensors include:

- Compact and simple to use and adapt
- High resolution and accuracy
- Very cost effective
- Low power consumption
- Can be read by industry standard data loggers

9.3 Working Principle

A tilt sensor has a metallic ball that is designed to move the two pins of the instrument from the 'on' to the 'off' position, and vice versa, if the sensor reaches a pre-determined angle. Tilt sensors are the environment-friendly version of a mercury-switch.

The Applications are

The following are key applications of tilt sensors:

To monitor the angle at which a mobile phone or tablet is held for the auto-rotate function

- To detect the position of hand-held game systems and in game controllers
- To indicate roll of boats, vehicles and aircraft
- To measure the angle at which a satellite antenna 'looks' toward a satellite
- To estimate the height of a tree or building using
- To measure the steepness of a ski slope
- As a warning system for the tilt angle of the surface cryogenic liquids during transportation
- To monitor laser levels and seismic activity

9.4 HEARTBEAT SENSOR

A person's heartbeat is the sound of the valves in his/her's heart contracting or expanding as they force blood from one region to another. The number of times the heart beats per minute (BPM), is the heart beat rate and the beat of the heart that can be felt in any artery that lies close to the skin is the pulse.

Manual Way: Heart beat can be checked manually by checking one's pulses at two locations- wrist (the **radial pulse**) and the neck (**carotid pulse**). The procedure is to place the two fingers (index and middle finger) on the wrist (or neck below the windpipe) and count the number of pulses for 30 seconds and then multiplying that number by 2 to get the heart beat rate. However pressure should be applied minimum and also fingers should be moved up and down till the pulse is felt. Using a sensor: Heart Beat can be measured based on optical power variation as light is scattered or absorbed during its path through the blood as the heart beat changes.

9.5 Principle of Heartbeat Sensor

The heartbeat sensor is based on the principle of photo plethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ (a vascular region). In case of applications where heart pulse rate is to be monitored, the timing of the pulses is more important. The flow of blood volume is decided by the rate of heart pulses and since light is absorbed by blood, the signal pulses are equivalent to the heart beat pulses.

There are two types of photoplethysmography:

Transmission: Light emitted from the light emitting device is transmitted through any vascular region of the body like earlobe and received by the detector.

Reflection: Light emitted from the light emitting device is reflected by the regions.

9.6 Working of a Heartbeat Sensor

The basic heartbeat sensor consists of a light emitting diode and a detector like a light detecting resistor or a photodiode. The heart beat pulses causes a variation in the flow of blood to different regions of the body. When a tissue is illuminated with the light source, i.e. light emitted by the led, it either reflects (a finger tissue) or transmits the light (earlobe). Some of the light is absorbed by the blood and the transmitted or the reflected light is received by the light detector. The amount of light absorbed depends on the blood volume in that tissue. The detector output is in form of electrical signal and is proportional to the heart beat rate.

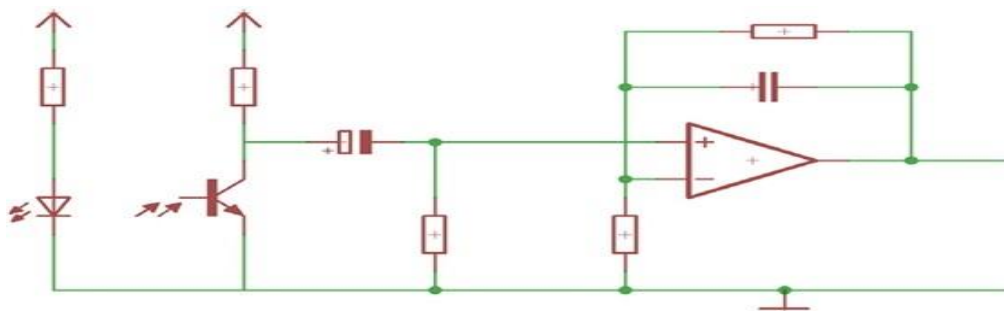


Fig.9.2:Circuit Diagram

To achieve the task of getting the AC signal, the output from the detector is first filtered using a 2 stage HP-LP circuit and is then converted to digital pulses using a comparator circuit or using simple ADC. The digital pulses are given to a microcontroller for calculating the heart beat rate, given by the formula-BPM (Beats per minute) = $60 * f$ Practical heartbeat Sensor examples are **Heart Rate Sensor (Product No PC-3147)**. It consists of an infrared led and an ldr embedded onto a clip like structure. The clip is attached to the organ (earlobe or the finger) with the detector part on the flesh.



Fig.9.3:Heartbeat Sensor

Pin2 and 3 are grounded. Pin 4 is the output. Pin 1 is also the enable pin and pulling it high turns the LED on and the sensor starts working. It is embedded on a wearable device which can be worn on the wrist and the output can be sent wirelessly (through Bluetooth) to the computer for processing.



Fig.9.4:Led

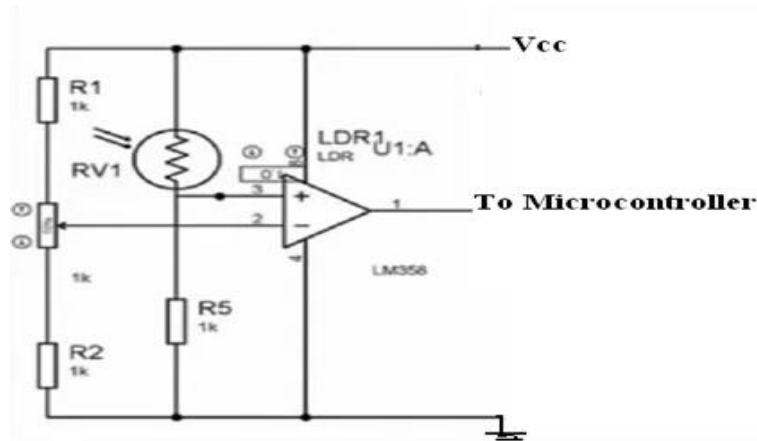


Fig.9.5:Circuit Diagram

As described above regarding the principle of heart beat sensor, when the finger tissue or the earlobe tissue is illuminated using a light source, the light is transmitted after getting modulated i.e. a part getting absorbed by the blood and the rest being transmitted. This modulated light is received by the light detector. Here a comparator is used which compares the output voltage from the LDR to that of the threshold voltage. The threshold voltage is the voltage drop across the LDR when the light with fixed intensity, from the light source falls directly on it. The inverting terminal of the comparator LM358 is connected to the potential divider arrangement which is set to the threshold voltage and the non-inverting terminal is connected to the LDR. When a human tissue is illuminated using the light source, the intensity of the light reduces. As this reduced light intensity falls on the LDR, the resistance increases and as a result the voltage drop increases. When the voltage drop across the LDR or the non-inverting input exceeds that of the inverting input, a logic high signal is developed at the output of the comparator and in case voltage drop being lesser a logic low output is developed. Thus the output is a series of pulses. These pulses can be fed to the Microcontroller which accordingly processes the information to get the heart beat rate and this is displayed on the Display interfaced to the Microcontroller.

9.7 VIBRATION SENSORS

The piezoelectric sensor is used for flex, touch, vibration and shock measurement. Its basic principal, at the risk of oversimplification, is as follows: whenever a structure moves, it experiences acceleration. A piezoelectric shock sensor, in turn, can generate a charge when

physically accelerated. This combination of properties is then used to modify response . Why is that important? Because vibration and shock can shorten the life of any electronic and electromechanical system. Delicate leads and bond wires can be stressed, especially after exposure to long term vibration. Solder joints can break free and PCB traces can even so slightly tear from impact and impulse shock, creating the hardest type of system failure .This article discusses piezoelectric shock and vibration sensors and sensor technology, focusing on available products (all parts mentioned here can be found on the Digi-Key website — links .

9.8 WORKING OF VIBRATION SENSOR

The piezoelectric effect was discovered by Pierre and Jacques Curie in the latter part of the 19th century. They discovered that minerals such as tourmaline and quartz could transform mechanical energy into an electrical output. The voltage induced from pressure (Greek: piezo) is proportional to that applied pressure, and piezoelectric devices can be used to detect single Still, the ability of certain crystals to exhibit electrical charges under mechanical loading was of no practical use until very-high-input impedance amplifiers enabled engineers to amplify the signals produced by these crystals. Several materials can be used to make piezoelectric sensors, including tourmaline, gallium phosphate, salts, and quartz. Most electronic applications use quartz since its growth technology is far along,

Sensors based on the piezoelectric effect can operate from transverse, longitudinal, or shear forces, and are insensitive to electric fields and electromagnetic radiation. The response is also very linear over wide temperature ranges, making it an ideal sensor for rugged environments. For example, gallium phosphate and tourmaline sensors can have a working

The physical design of the piezoelectric sensor depends on the type of sensor you wish to create. For example, the configuration of a pressure sensor, or a shock (impulse) sensor, would arrange a smaller, but well-known mass of the crystal in a transverse configuration, with the loading deformation along the longest tracks to a more massive base (Figure 1). This assures that the applied pressure will load the base from only one direction. A constrained mass is allowed to deform the crystal sensor in one axis. This configuration is good for force and pressure.

An accelerometer based on the piezoelectric effect, would use a known mass to deform the sensing crystal part in either a positive or negative direction depending on the excitation force. It should be noted that you need a known modulus of elasticity in the sensor substrate.

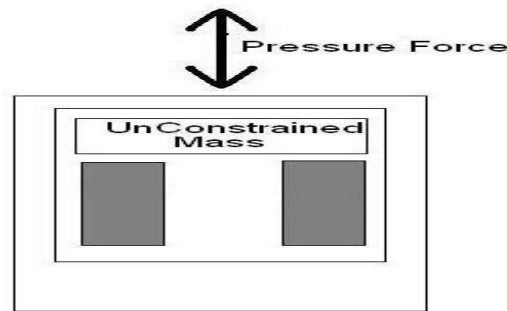


Fig.9.6: Pressure Force Diagram

Piezoelectric sensors require some precautions when connecting to sensitive electronic components. First and foremost, the voltage levels created by hard shock can be very high, even around 100-V spikes. More than likely, an op amp will be used to interface these sensors to an A/D converter, either discrete or on a microcontroller. One tip is to choose a high-input-impedance op amp to minimize current. One possible candidate is the Linear Technology JFET input dual op amp. It has $10^{12} \Omega$ input resistance and a 1 MHz gain bandwidth product, good enough to easily handle the vibration ranges of piezoelectric

Another suitable part is the TLV2771 from Texas Instruments. This rail-to-rail low-power op-amp also has a $10^{12} \Omega$ differential input resistance and a 5 MHz unity-gain bandwidth. Signal conditioning in a single stage can prepare the input from the shock sensor directly into an A/D converter. Op amps such as the TI TLV2772 feature high input impedances to help minimize current from the potentially high-voltage inputs from the piezoelectric sensors.

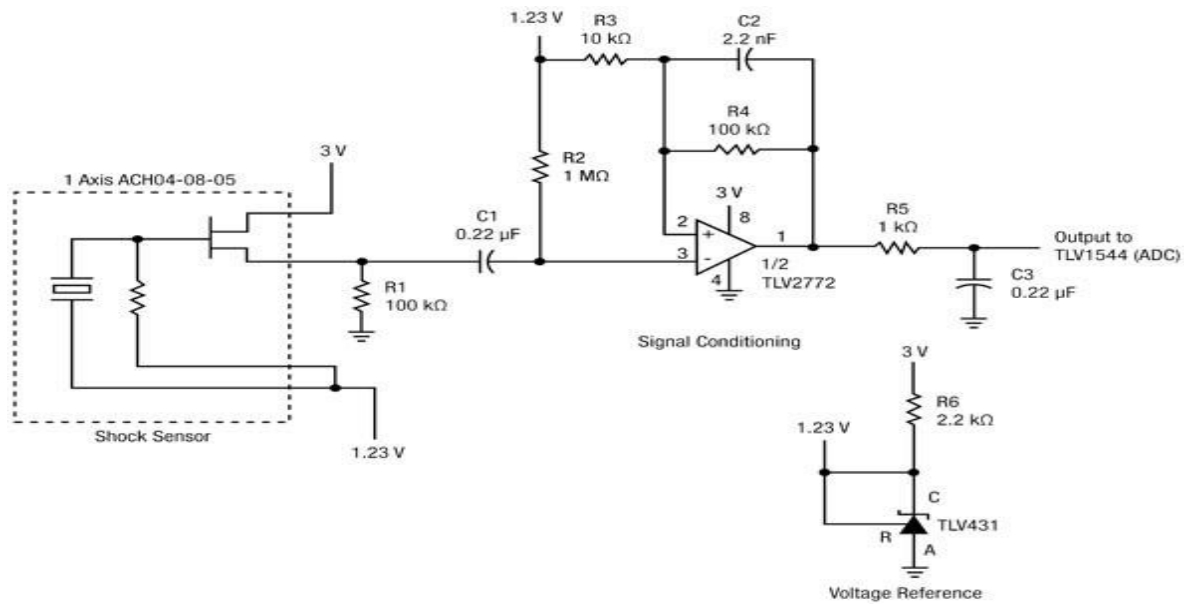


Fig.9.7:Circuit Diagram

Another tip is to attenuate the input signal and use the op amp's gain to bring into the desired range. Be aware that you may need snubbing protection on the inputs of the op amp, especially if the design could be subjected to harsh hits. Also note that you may think that a pressure sensor would generate only a positive voltage, but, in reality, the signal from the sensor can ring and introduce negative voltage spikes (Figure 4). This means that you may need to squelch negative voltage levels on the op-amp inputs, especially if using only a single rail power supply on the op amp.



Fig.9.8:Graph

Care must be taken when using single rail op amps since shock can cause negative voltage spike ringing that can damage op-amp inputs if not squelched.

9.9 Parts for the design

Many off the shelf piezoelectric sensors are readily available to use in your designs. A case in point is the Parallax 605-00004, which is a piezo vibra tab sensor capable of acting as a switch, or as a vibration sensor (Figure 5). A polymer film laminate uses crimped contacts and features a sensitivity of 50 mV/g.

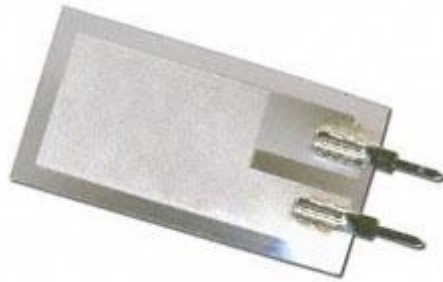


Fig.9.9:LDTO Polymer

The flexible through-hole LDTO polymer film piezoelectric sensors can be hard mounted or free floating to detect strain, shock, or vibration.

You should be aware that adding mass to a piezoelectric sensor can change its resonant frequency as well as change its baseline sensitivity. Many piezoelectric sensors like the 605-00004 are characterized to be used this way and provide supporting tables and graphs.

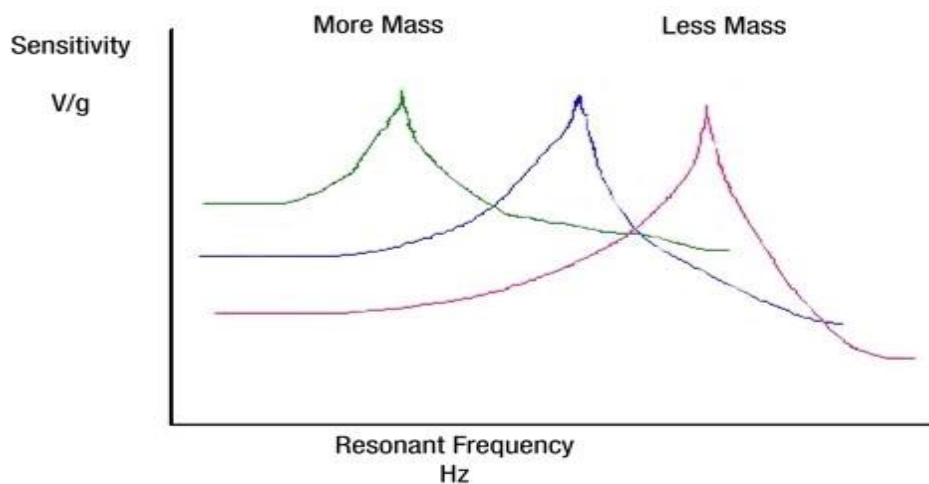


Fig.9.10:Graph

In addition to sensing vibration and shock, a piezoelectric device can also be used to extract ambient energy. Take for example the MideV22BL, which is a hermetically sealed piezoelectric sensor capable of sensing from 26 to 100 Hz vibrations. It can be evaluated using the company's VR001 data logger, which is a portable rechargeable data logger that can measure acceleration and vibration in three axes (Figure 7). As a USB peripheral, it can be configured and have its data transferred to a PC or other USB host device. It can also be used to help you develop your own designs based on the piezoelectric sensors you choose. A Mide training module is available on the Digi-Key website to help bring you up to speed quickly when starting a new design.

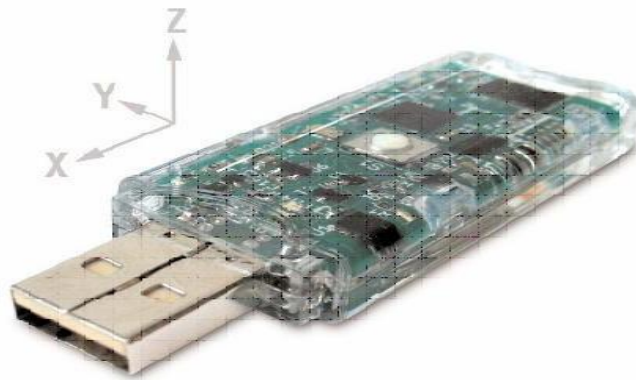


Fig.9.11:USB

Finally, before you select a piezoelectric sensor for shock or vibration duty, evaluate the criteria specific to your intended application (we've provided some examples here), then, spend some time with the manufacturer data sheets and use the links above to get further information from the product and technology pages on the Digi-Key website.

9.10 Pressure sensor

A pressure sensor measures pressure, typically of gases or liquids. Pressure is an expression of the force required to stop a fluid from expanding, and is usually stated in terms of force per unit area. A pressure sensor usually acts as a transducer; it generates a signal as a function of the pressure imposed. For the purposes of this article, such a signal is electrical. Pressure sensors are used for control and monitoring in thousands of everyday applications. Pressure sensors can also be used to indirectly measure other variables such as fluid/gas flow, speed,

water level, and altitude. Pressure sensors can alternatively be called pressure transducers, Pressure sensors can vary drastically in technology, design, performance, application suitability and cost. A conservative estimate would be that there may be over 50 technologies and at least 300 companies making pressure sensors worldwide.

There is also a category of pressure sensors that are designed to measure in a dynamic mode for capturing very high speed changes in pressure. Example applications for this type of sensor would be in the measuring of combustion pressure in an engine cylinder or in a gas turbine. These sensors are commonly manufactured out of piezoelectric materials such as quartz. Some pressure sensors, such as those found in some traffic enforcement cameras, function in a binary (off/on) manner, i.e., when pressure is applied to a pressure sensor, the sensor acts to complete or break an electrical circuit. These types of sensors are also known as a pressure switch.

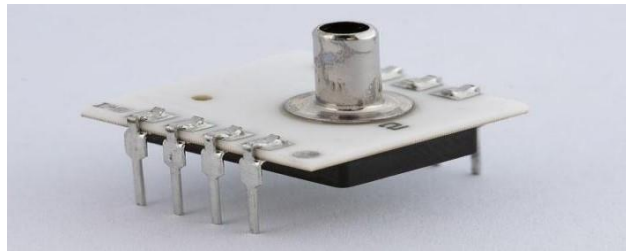


Fig.9.12:Pressure Sensor

CHAPTER 10

ARDUINO IDE SOFTWARE

There are many other microcontrollers and microcontroller platforms available for physical computing. Parallax Basic Stamp, Netmedia's BX-24, Phidgets, MIT's Handyboard, and many others offer similar functionality. All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems:

Inexpensive - Arduino boards are relatively inexpensive compared to other microcontroller platforms. The least expensive version of the Arduino module can be assembled by hand, and even the pre-assembled Arduino modules cost less than \$50

Cross-platform - The Arduino software runs on Windows, Macintosh OSX, and Linux operating systems. Most microcontroller systems are limited to Windows.

Simple, clear programming environment - The Arduino programming environment is easy-to-use for beginners, yet flexible enough for advanced users to take advantage of as well. For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with the look and feel of Arduino

All of these tools take the messy details of microcontroller programming and wrap it up in an easy-to-use package. Arduino also simplifies the process of working with microcontrollers, but it offers some advantage for teachers, students, and interested amateurs over other systems: For teachers, it's conveniently based on the Processing programming environment, so students learning to program in that environment will be familiar with the look and feel of Arduino

CONCLUSION

This type of an idea being the first of its kind plays a crucial role towards ensuring Women Safety in the fastest way possible automatically. The proposed design will deal with critical issues faced by women in the recent past and will help solve them through technologically sound gadgets. With further research and innovation, this project can be implemented in different areas of security and surveillance. The system can perform the real time monitoring of desired area and detect the violence with a good accuracy.

REFERENCES

1. Alexandrous Plantelopoulous and Nikolaos.G.Bourbakis, “A Survey on Wearable sensor based system for health monitoring and prognosis,” IEEE Transaction on system, Man and Cybernetics, Vol.40, No.1, January 2010.
2. B.Chougula, “Smart girls security system,” International Journal of Application or Innovation in Engineering & Management, Volume 3, Issue 4, April 2014.
3. D. Thierer, “The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation,” Rich. J. Law Technol., vol. 21, pp. 615, 2015.
4. D. Thierer, —The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation, Rich. J. Law Technol., vol. 21, pp. 6–15, 2015.
5. Hock Beng Lim, “A Soldier Health Monitoring System for Military Applications,” International Conference on Body Sensor Networks.
6. 1. Vamil B. Sangoi, “Smart security solutions,” International Journal of Current Engineering and Technology, Vol.4, No.5, Oct-2014.
7. Simon L. Cotton and William G. Scanlon, “Millimeter - wave Soldier –to-soldier communications for covert battlefield operation,” IEEE communication Magazine, October 2009.
8. Muruganandham, “Real Time Web based Vehicle Tracking using GPS,” World Academy of Science, Engineering and Techonogy, 37, 2010
9. M. Brachmann, S. L. Keoh, O. Morchon, and S. Kumar, —End-to-end transport security in the ip-based internet of things, in Proc. 21st Int. Conf. Comput. Commun. Netw., 2012, pp. 1–5.

10. Orlando Arias, Jacob Wurm, Yier Jin, "Privacy and Security in Internet of Things and Wearable Devices", IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, VOL. 1, NO. 2, APRIL-JUNE 2015
11. Palve Pramod, "GPS Based Advanced Soldier Tracking With Emergency Messages & Communication System," International Journal of Advance Research in Computer Science and Management Studies Research Article, Volume 2, Issue 6, June 2014
12. R. Ramani, S. Valarmathy, N. Suthanthira Vanitha, S. Selvaraju, and M. Thiruppathi, Vehicle Tracking and Locking System Based on GSM and GPS, I.J. Intelligent Systems and Applications, 2013, 09, 86-93
13. SeokJu Lee, Girma Tewolde, Jaerock Kwon "Design and Implementation of Vehicle Tracking System Using GPS/GSM/GPRS Technology and Smartphone Application" IEEE World Forum on Internet of Things (WF-IoT), March 2014, Seoul
14. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: Threats and challenges," Security Commun. Netw., vol. 7, no. 12, pp. 2728–2742, 2014
15. Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained application protocol (CoAP), draft-ietf-core-coap- 13," in The Internet Engineering Task Force (IETF), 2012.