Six Weeks Industrial Training Synopsis/Report

At

KOCHAR *INFO. TECH. ,AMRITSAR*

Submitted in partial fulfillment of the requirement for the award of the degree of

Bachelor of Technology

in

COMPUTER SCIENCE & ENGINEERING

Submitted By

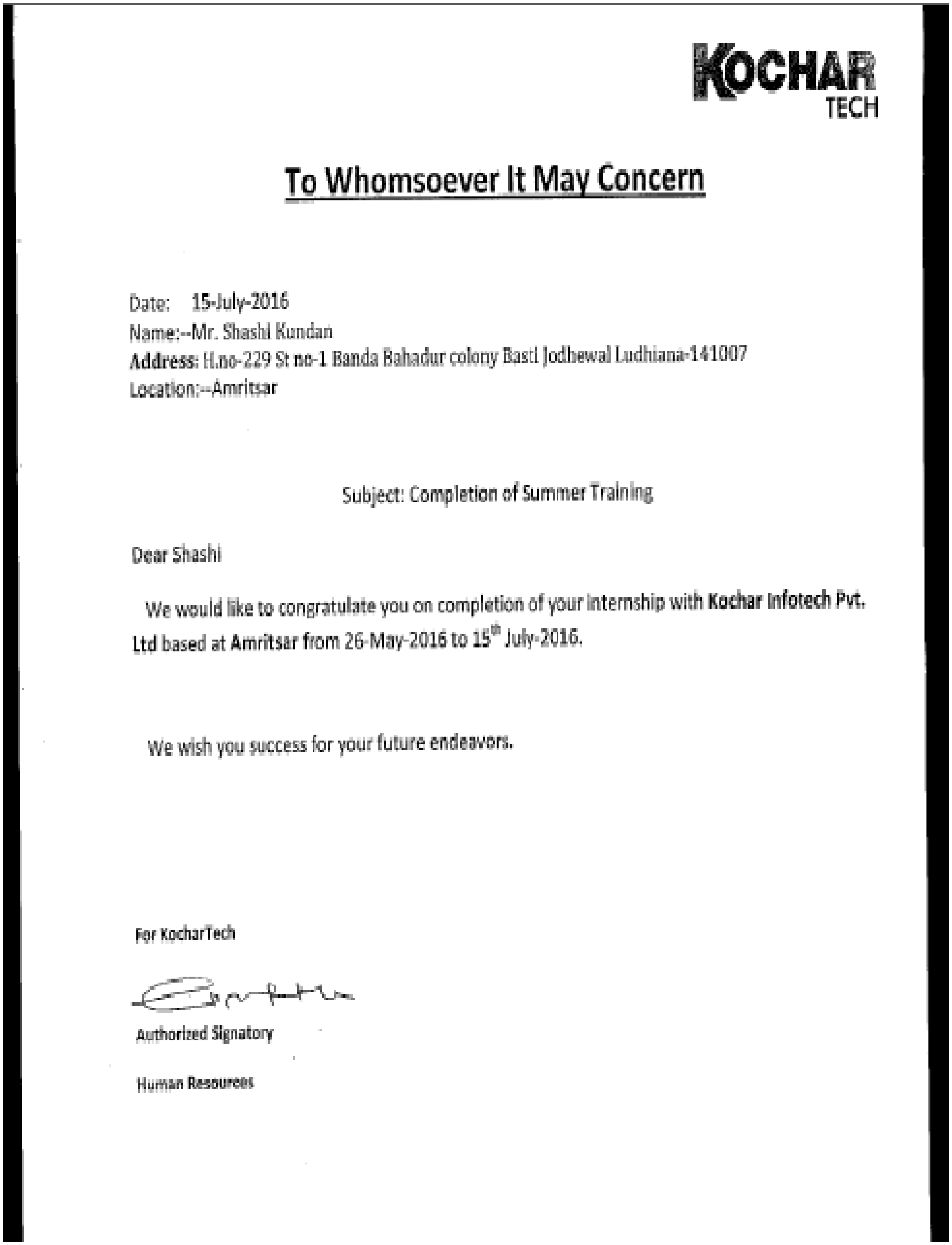
Shashi Kundan

Roll. No. 13103070

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
Dr. B.R. AMBEDKAR NATIONAL INSTITUTE OF TECHNOLOGY

JALANDHAR, PUNJAB, INDIA

Certificate



KOCHAR
TECH

To Whomsoever It May Concern

Date: 15-July-2016
Name:--Mr. Shashi Kundan
Address: H.no-229 St no-1 Banda Bahadur colony Basti Jodhewal Ludhiana-141007
Location:--Amritsar

Subject: Completion of Summer Training

Dear Shashi

We would like to congratulate you on completion of your internship with **Kochar Infotech Pvt. Ltd** based at Amritsar from 26-May-2016 to 15th July-2016.

We wish you success for your future endeavors.

For KocharTech

Authorized Signatory

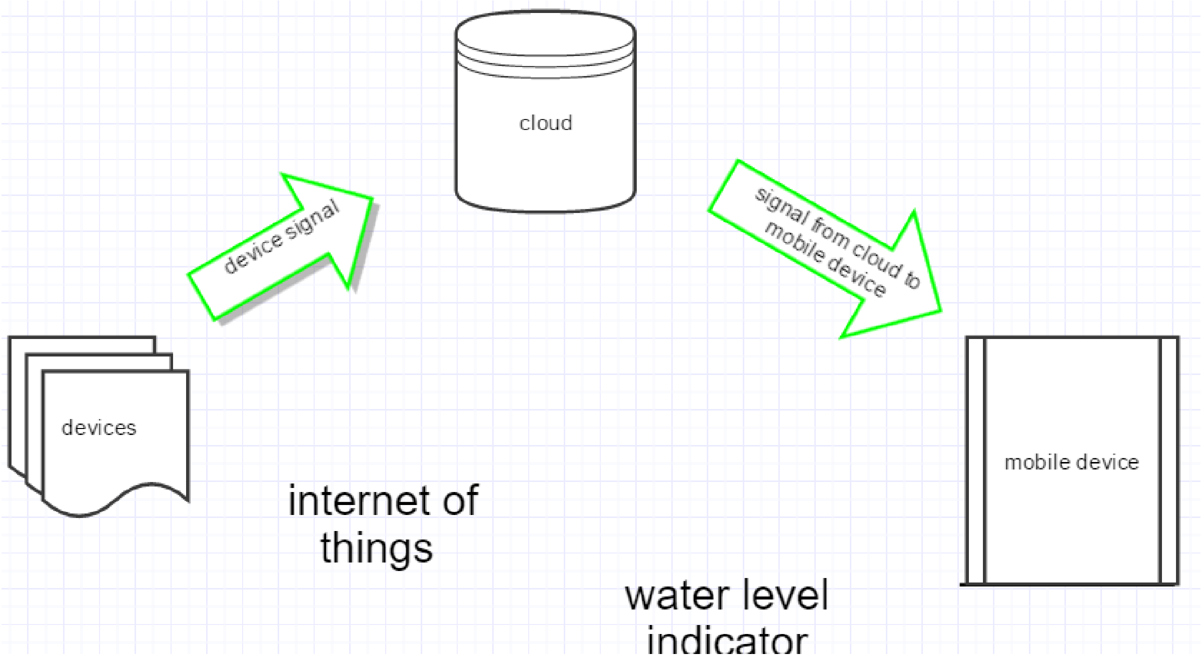
Human Resources

Abstract

I was Intern at_Kochar Infotech,amritsar in Research and development (R&D) department.

ProjectTitle: Water tank level measurement Based on Internet of Things

We made a water tank level measurement instrument using zigbee and arduino .we had sent water level information on your server and from server to mobile device . we make your mobile app which gather all information from server and give proper notification about water level information . We had used kochar server for testing purpose. We had use the zigmo server for sending and receiving the data.


cloud
device signal
signal from cloud to mobile device
devices
mobile device
internet of things
water level indicator

Objective:

This makes the real life of human being much easier .as we know that human being are generally forgot his/her daily life works. And this project provide solution to his/her problem to get notification about daily life works .

Example :

1:Forgot to close water tank

2:Forgot to turn off ac/light etc

This project provide all solution to this king of problems as well as there are many new applications of iot devices

ACKNOWLEDGEMENT

It is our pleasure to be indebted to various people, who directly or indirectly contributed in the development of this work and who influenced my thinking, behavior and acts during the course of study.

I/We express our sincere gratitude to ***Dr. Geeta Sikka*** worthy Head of the Department for providing me/us an opportunity to undergo Industrial Training as the part of the curriculum.

I/We are thankful to **Nitin Bhalla** for his/her support, cooperation, and motivation provided to us during the training for constant inspiration, presence and blessings.

Lastly, I/we would like to thank the almighty and my/our parents for their moral support and friends with whom we shared our day to day experience and received lots of suggestions that improve my/ our quality of work.

Shashi Kundan
13103070

CONTENTS

INTRODUCTION

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution"—from new market opportunities and business models to concerns about security, privacy, and technical interoperability. The large-scale implementation of IoT devices promises to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energyefficiency. Other personal IoT devices like wearable fitness and health monitoring devices and networkenabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost.1 IoT systems like networked vehicles, intelligent traffic systems, and sensors embedded in roads and bridges move us closer to the idea of "smart cities'', which help minimize congestion and energy consumption. IoT technology offers the possibility to transform agriculture, industry, and energy production and distribution by increasing the availability of information along the value chain of production using networked sensors. However, IoT raises many issues and challenges that need to be considered and addressed in order for potential benefits to be realized. A number of companies and research organizations have offered a wide range of projections about the potential impact of IoT on the Internet and the economy during the next five to ten years. Cisco, for example, projects more than 24 billion Internet–connected objects by 2019;2 Morgan Stanley, however, projects 75 billion networked devices by 2020.3 Looking out further and raising the stakes higher, Huawei forecasts 100 billion IoT connections by 2025.[4] McKinsey Global Institute suggests that the financial impact of IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025.[5] While the variability in predictions makes any specific number questionable, collectively they paint a picture of significant growth and influence. Some observers see the IoT as a revolutionary fully–interconnected "smart" world of progress, efficiency, and opportunity, with the potential for adding billions in value to industry and the global economy.[6] Others warn that the IoT represents a darker world of surveillance, privacy and security violations, and consumer lock–in. Attention-grabbing headlines about the hacking of Internet-connected automobiles,[7] surveillance concerns stemming from voice recognition features in "smart" TVs,[8] and privacy fears stemming from the potential misuse of IoT data[9] have captured public attention. This "promise vs. peril" debate along with an influx of information though popular media and marketing can make the IoT a complex topic to understand.

Fundamentally, the Internet Society cares about the IoT as it represents a growing aspect of how people and institutions are likely to interact with the Internet in their personal, social, and economic lives. If even modest projections are correct, an explosion of IoT applications could present a fundamental shift in how users engage with and are impacted by the Internet, raising new issues and different dimensions of existing challenges across user/consumer concerns, technology, policy and law. IoT also will likely have varying consequences in different economies and regions, bringing a diverse set of opportunities and challenges across the globe. This overview document is designed to help the Internet Society community navigate the dialogue surrounding the Internet of Things in light of the competing predictions about its promises and perils. It provides a high-level overview of the basics of IoT and some of the key issues and questions that this technology raises from the perspective of the Internet Society and the core values we promote.[10,11] It also acknowledges some of the unique aspects of the Internet of Things that make this transformational technology for the Internet.

As this is intended to be an overview document, we do not propose a specific course of action for ISOC on IoT at this time. Rather, we see this document as an informational resource and starting point for discussion within the ISOC community on IoT-related issues.

What is the Internet of Things?

Origins, Drivers, and Applications

The term “Internet of Things” (IoT) was first used in 1999 by British technology pioneer Kevin Ashton to

describe a system in which objects in the physical world could be connected to the Internet by sensors.12

Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) tags13 used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items. While the term “Internet of Things” is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use.14 In the 1990s, advances in wireless technology allowed “machine–to–machine” (M2M) enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purpose–built networks and proprietary or industry–specific standards,15 rather than on Internet Protocol (IP)–based networks and Internet standards. Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet “device”—an IP–enabled toaster that could be turned on and off over the Internet—was featured at an Internet conference in 1990.16 Over the next several years, other “things” were IP–enabled, including a soda machine17 at Carnegie Mellon University in the US and a coffee pot18 in the Trojan Room at the University of Cambridge in the UK (which remained Internet–connected until 2001). From these whimsical beginnings, a robust field of research and development into “smart object networking”19 helped create the foundation for today’s Internet of Things.

12 Ashton was working on RFID (radio-frequency identification) devices, and the close association

If the idea of connecting objects to each other and to the Internet is not new, it is reasonable to ask, "Why is

the Internet of Things a newly popular topic today?"
From a broad perspective, the confluence of several technology and market trends20 is making it possible to interconnect more and smaller devices cheaply and easily:

- *Ubiquitous Connectivity*—Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable".
- *Widespread adoption of IP–based networking*— IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.
- *Computing Economics*— Driven by industry investment in research, development, and manufacturing, Moore's law21 continues to deliver greater computing power at lower price points and lower power consumption.22
- *Miniaturization*— Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects.23 Coupled with greater computing economics, this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.
- *Advances in Data Analytics*— New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.
- *Rise of Cloud Computing*– Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.

From this perspective, the IoT represents the convergence of a variety of computing and connectivity trends that have been evolving for many decades. At present, a wide range of industry sectors – including automotive, healthcare, manufacturing, home and consumer electronics, and well beyond -- are considering

the potential for incorporating IoT technology into their products, services, and operations.

In their report “Unlocking the Potential of the Internet of Things’’, the McKinsey Global Institute24 describes

the broad range of potential applications in terms of “settings” where IoT is expected to create value for industry and users.

“Settings” for IoT Applications (Source: McKinsey Global Institute25)
Setting
Description Examples

- Human
- Devices attached or
- inside the human
- body
- Devices (wearables and ingestibles) to monitor and
- maintain human health and wellness; disease
- management, increased fitness, higher productivity
- Home Buildings where
- people live Home controllers and security systems
- Retail
- Environments
- Spaces where
- consumers engage in
- commerce
- Stores, banks, restaurants, arenas – anywhere
- consumers consider and buy; self-checkout, in-store
- offers, inventory optimization
- Offices
- Spaces where
- knowledge workers
- work
- Energy management and security in office buildings;
- improved productivity, including for mobile employees
- Factories
- Standardized
- production
- environments
- Places with repetitive work routines, including hospitals
- and farms; operating efficiencies, optimizing equipment
- use and inventory
- Worksites Custom production
- environments
- Mining, oil and gas, construction; operating efficiencies,
- predictive maintenance, health and safety
- Vehicles Systems inside
- moving vehicles
- Vehicles including cars, trucks, ships, aircraft, and
- trains; condition-based maintenance, usage-based
- design, pre-sales analytics
- Cities Urban environments

- Public spaces and infrastructure in urban settings;
- adaptive traffic control, smart meters, environmental
- monitoring, resource management
- Outside
- Between urban
- environments (and
- outside other settings)
- Outside uses include railroad tracks, autonomous
- vehicles (outside urban locations), and flight navigation;
- real-time routing, connected navigation, shipment
- tracking

Many organizations have developed their own taxonomies and categorizations of IoT applications and use cases. For example, “Industrial IoT” is a term widely used by companies and associations to describe IoT applications related to the production of goods and services, including in manufacturing and utilities.26 Others

discuss IoT by device type, such as wearables27 and appliances.28 Still others focus on IoT in the context of integrated location-based implementations such as “smart homes” or “smart cities”.29 Whatever the application, it is clear that IoT use cases could extend to nearly every aspect of our lives.

As the number of Internet-connected devices grows, the amount of traffic they generate is expected to rise significantly. For example, Cisco estimates that Internet traffic generated by non-PC devices will rise from 40% in 2014 to just under 70% in 2019.30 Cisco also forecasts that the number of “Machine to Machine” (“M2M”) connections (including in industrial, home, healthcare, automotive, and other IoT verticals) will rise from 24% of all connected devices in 2014 to 43% in 2019. One implication of these trends is that over the next ten years we could see a shift in the popular notion of what it means to be “on the Internet”. As MIT Professor Neil Gershenfied noted, “...[T]he rapid growth of the World Wide Web may have been just the trigger charge that is now setting off the real explosion, as things start to use the Net”.31 In the popular mindset, the World Wide Web has almost become synonymous with the Internet itself. Web technologies facilitate most interactions between people and content, making it a defining characteristic of the current Internet experience. The Web-based experience is largely characterized by the active engagement of users downloading and generating content through computers and smartphones. If the growth projections about IoT become reality, we may see a shift towards more passive Internet interaction by users with objects such as car components, home appliances and self-monitoring devices; these devices send and receive data on the user's behalf, with little human intervention or even awareness.

Different Definitions, Similar Concepts

Despite the global buzz around the Internet of Things, there is no single, universally accepted definition for the term. Different definitions are used by various groups to describe or promote a particular view of what IoT means and its most important attributes. Some definitions specify the concept of the Internet or the
Internet Protocol (IP), while others, perhaps surprisingly, do not. For example, consider the following definitions.
The Internet Architecture Board (IAB) begins RFC 7452,33

"Architectural Considerations in Smart Object Networking", with this description:
The term "Internet of Things" (IoT) denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called "smart objects," are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment.

Within the Internet Engineering Task Force (IETF), the term "smart object networking" is commonly used in reference to the Internet of Things. In this context, "smart objects" are devices that typically have significant constraints, such as limited power, memory, and processing resources, or bandwidth.34 Work in the IETF is organized around specific requirements to achieve network interoperability between several types of smart objects.35 Published in 2012, the International Telecommunication Union (ITU) ITU–T Recommendation Y.2060,
Overview of the Internet of things,36 discusses the concept of interconnectivity, but does not specifically tie the IoT to the Internet:
3.2.2 Internet of things (IoT): 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.
Note 1—Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
Note 2—From a broader perspective, the IoT can be perceived as a vision with technological and societal implications

*This definition in a call for papers for a feature topic issue of IEEE Communications Magazine*37 links the IoT back to cloud services:

The Internet of Things (IoT) is a framework in which all things have a representation and a presence in the Internet. More specifically, the Internet of Things aims at offering new applications and services bridging the physical and virtual worlds, in which Machine-to-Machine (M2M) communications represents the baseline communication that enables the interactions between Things and applications in the cloud.

The Oxford Dictionaries38 offers a concise definition that invokes the Internet as an element of the IoT: *Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.*

All of the definitions describe scenarios in which network connectivity and computing capability extends to a constellation of objects, devices, sensors, and everyday items that are not ordinarily considered to be "computers"; this allows the devices to generate, exchange, and consume data, often with minimal human intervention. The various definitions of IoT do not necessarily disagree – rather they emphasize different aspects of the IoT phenomenon from different focal points and use cases.

However, the disparate definitions could be a source of confusion in dialogue on IoT issues, particularly in discussions between stakeholder groups or industry segments. Similar confusion was experienced in recent

years about net neutrality and cloud computing, where different interpretations of the terms sometimes presented obstacles to dialogue. While it is probably unnecessary to develop a single definition of IoT, it

should be recognized that there are different perspectives to be factored into discussions.

For the purposes of this paper, the terms "Internet of Things" and "IoT" refer broadly to the extension of network connectivity and computing capability to objects, devices, sensors, and items not ordinarily considered to be computers. These "smart objects" require minimal human intervention to generate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities.

Networking and communications models for smart objects include those where exchanged data does not traverse the Internet or an IP-based network. We include those models in our broad description of "Internet of Things" used for this paper. We do so as it is likely that the data generated or processed from those smart objects will ultimately pass through gateways with connectivity to IP-based networks or will otherwise be incorporated into product features that are accessible via the Internet. Furthermore, users of IoT devices are likely to be more concerned with the services delivered and the implication of using those services than issues of when or where data passes through an IP-based network.

Internet of Things Communications Models

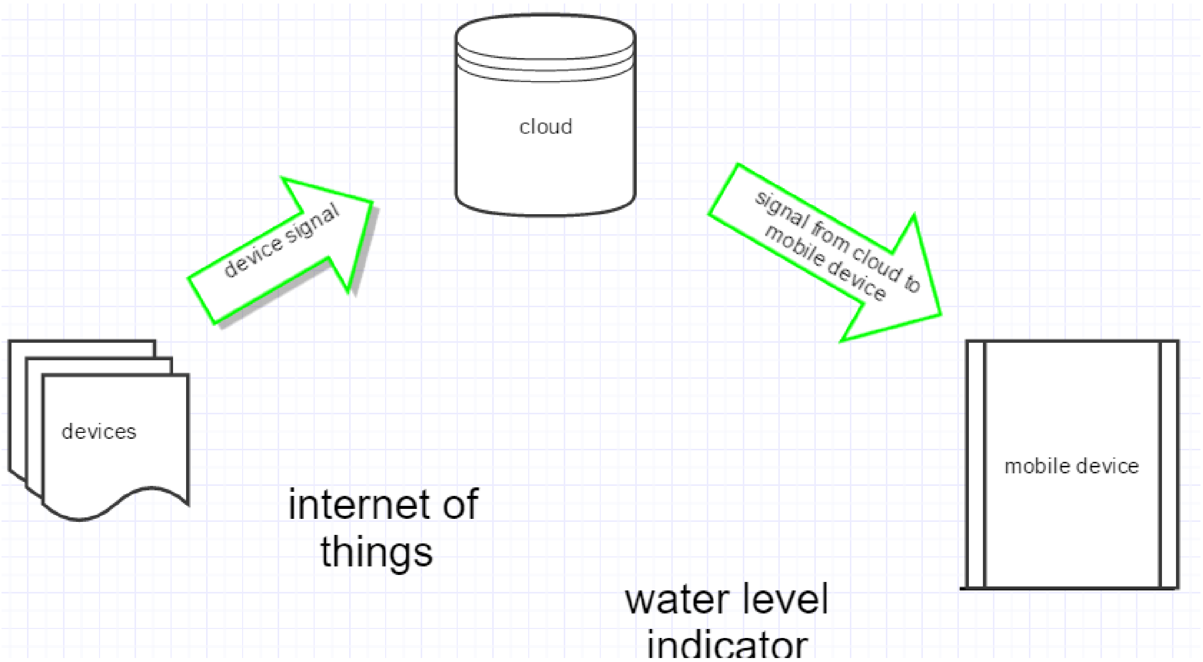
From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452),39 which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework.

Device-to-Device Communications

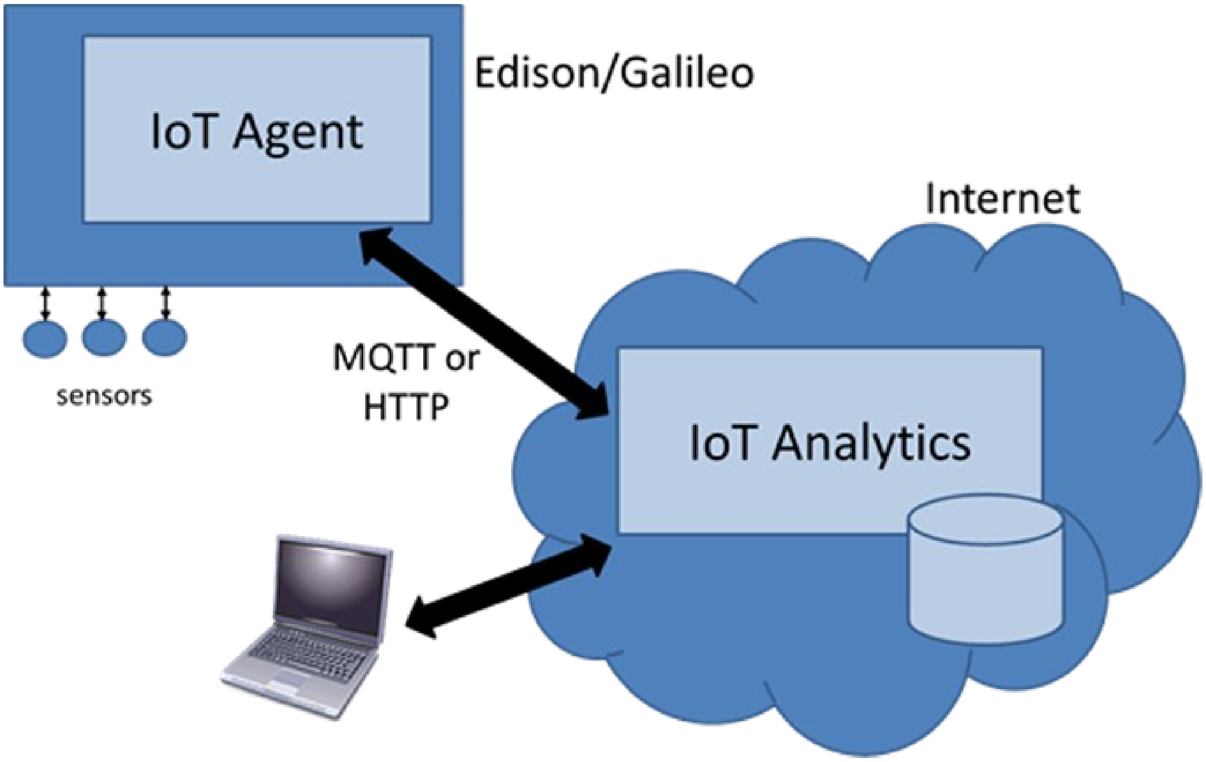
The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth,40 Z-Wave,41 or ZigBee42 to establish direct device-to-device

Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. The model is shown in Figure 3.



architecture supports “the [user’s] desire for granting access to the uploaded sensor data to third parties”.[50] This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where “IoT devices upload data only to a single application service provider”.[51] A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed. For example, a corporate user in charge of an office complex would be interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs. Effective back-end datasharing architectures allow users to move their data when they switch between IoT services, breaking down traditional data silo barriers. The back-end data-sharing model suggests a federated cloud services approach[52] or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud.[53] A graphical representation of this design is shown in Figure 4.


Edison/Galileo
IoT Agent
sensors
MQTT or HTTP
Internet
IoT Analytics

Internet of Things Communications Models Summary

The four basic communication models demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems.

From a general user perspective, these communication models help illustrate the ability of networked devices to add value to the end user. By enabling the user to achieve better access to an IoT device and its data, the overall value of the device is amplified. For example, in three of the four communication models, the devices ultimately connect to data analytic services in a cloud computing setting. By creating data communication conduits to the cloud, users, and service providers can more readily employ data aggregation, big data analytics, data visualization, and predictive analytics technologies to get more value out of IoT data than can be achieved in traditional data-silo applications. In other words, effective communication architectures are an important driver of value to the end user by opening possibilities of using information in new ways. It should be noted, however, these networked benefits come with trade-offs.

Careful consideration needs to be paid to the incurred cost burdens placed on users to connect to cloud resources when considering an architecture, especially in regions where user connectivity costs are high.

While the end user benefits from effective communication models, it should be mentioned that effective IoT communication models also enhance technical innovation and open opportunity for commercial growth. New products and services can be designed to take advantage of IoT data streams that didn’t exist previously, acting as a catalyst for further innovation.

What issues are raised by the Internet of Things?

It would be impossible to cover the broad scope of issues surrounding the Internet of Things in a single paper. Below, however, we provide an overview of five topics frequently discussed in relation to IoT. These include: security; privacy; interoperability and standards; legal, regulatory and rights; and emerging economies and development.

We begin to examine these issues through the lens of “the Abilities” – the statement of fundamental principles that guide ISOC’s work in terms of the capabilities we believe all Internet users should enjoy that must be protected. These include the ability to *connect, speak, innovate, share, choose*, and *trust*.[55] With these principles as a guide, we present important aspects of each issue and propose several questions for discussion.

Security Issues

The IoT Security Challenge

As we note in the principles that guide our work, ensuring the security, reliability, resilience, and stability of Internet applications and services is critical to promoting *trust* and use of the Internet.[56] As users of the Internet, we need to have a high degree of trust that the Internet, its applications, and the devices linked to it are secure enough to do the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in IoT is fundamentally linked to the ability of users to trust their environment. If people don’t believe their connected devices and their information are reasonably secure from misuse or harm, the resulting erosion of trust causes a reluctance to use the Internet. This has global consequences to electronic commerce, technical innovation, free speech, and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered a top priority for the sector.

As we increasingly connect devices to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyberattack by allowing malicious individuals to re-program a device or cause it to malfunction. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices also can create security vulnerabilities. These problems are just as large or larger for the small, cheap, and the endpoints of Internet connectivity. Competitive cost and technical constraints on IoT devices challenge manufacturers to adequately design security features into these devices, potentially creating security and long-term maintainability vulnerabilities greater than their traditional computer counterparts.

Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly interconnected nature of IoT devices, every poorly secured device that is connected online potentially affects the security and resilience of the Internet *globally*, not just locally. For example, an unprotected refrigerator or television in the US that is infected with malware might send thousands of harmful spam emails to recipients worldwide using the owner's home Wi-Fi Internet connection.[57]

To complicate matters, our ability to function in our daily activities without using devices or systems that are Internet-enabled is likely to decrease in a hyperconnected world. In fact, it is increasingly difficult to purchase some devices that are *not* Internet-connected because certain vendors only make connected products. Day by day, we become more connected and dependent on IoT devices for essential services, and we need the devices to be secure, while recognizing that no device can be absolutely secure. This increasing level of dependence on IoT devices and the Internet services they interact with also increases the pathways for wrongdoers to gain access to devices. Perhaps we could unplug our Internet-connected TVs if they get compromised in a cyber attack, but we can’t so easily turn off a smart utility power meter or a traffic control system or a person’s implanted pacemaker if they fall victim to malicious behavior. This is why security of IoT devices and services is a major discussion point and should be considered a critical issue. We increasingly depend on these devices for essential services, and their behavior may have global reach and impact.

Privacy Considerations

Internet of Things Privacy Background

Respect for privacy rights and expectations is integral to ensuring *trust* in the Internet, and it also impacts the ability of individuals to *speak*, *connect,* and *choose* in meaningful ways. These rights and expectations are sometimes framed in terms of ethical data handling, which emphasizes the importance of respecting an individual's expectations of privacy and the fair use of their data.[63] The Internet of Things can challenge these traditional expectations of privacy.

IoT often refers to a large network of sensor-enabled devices designed to collect data about their environment, which frequently includes data related to people. This data presumably provides a benefit to the device's owner, but frequently to the device's manufacturer or supplier as well. IoT data collection and use becomes a privacy consideration when the individuals who are observed by IoT devices have different privacy expectations regarding the scope and use of that data than those of the data collector.

Seemingly benign combinations of IoT data streams also can jeopardize privacy. When individual data streams are combined or correlated, often a more invasive digital portrait is painted of the individual than can be realized from an individual IoT data stream. For example, a user's Internet-enabled toothbrush might capture and transmit innocuous data about a person's tooth-brushing habits. But if the user's refrigerator reports the inventory of the foods he eats and his fitness-tracking device reports his activity data, the combination of these data streams paint a much more detailed and private description of the person’s overall health. This data-aggregation effect can be particularly potent with respect to IoT devices because many produce additional metadata like time stamps and geolocation information, which adds even more specificity about the user.

In other situations, the user might not be aware that an IoT device is collecting data about the individual and potentially sharing it with third parties. This type of data collection is becoming more prevalent in consumer devices like smart televisions and video game devices. These kinds of products have voice recognition or vision features that continuously listen to conversations or watch for activity in a room and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A person might be in the presence of these kinds of devices without knowing their conversation or activities are being monitored and their data captured. These kinds of features may provide a benefit to an informed user, but can pose a privacy problem for those who are unaware of the presence of the devices and have no meaningful influence over how that collected information is used.

Independent of whether the user is aware of and consents to having their IoT data collected and analyzed, these situations highlight the value of these personalized data streams to companies and organizations seeking to collect and capitalize on IoT information. The demand for this information exposes the legal and regulatory challenges facing data protection and privacy laws.

These kinds of privacy problems are critical to address because they have implications on our basic rights and our collective ability to trust the Internet. From a broad perspective, people recognize their privacy is intrinsically valuable, and they have expectations of what data can be collected about them and how other parties can use that data. This general notion about privacy holds true for data collected by Internet of Things devices, but those devices can undermine the user’s ability to express and enforce privacy preferences. If users lose confidence in the Internet because their privacy preferences aren’t being respected in the Internet of Things, then the greater value of the Internet may be diminished.

Emerging Economy and Development Issues

Ensuring IoT Opportunities are Global

The spread and impact of the Internet is global in nature, providing opportunity and benefits to developed and developing regions alike. At the same time, there are often unique challenges in developing regions related to the deployment, growth, implementation, and use of technology, including the Internet. It is reasonable to expect the same to be true for the potential benefits and challenges associated with the Internet of Things.

From an Internet Society principle perspective, we believe that the Internet should be a source of empowerment globally, regardless of a user’s location, region, or state of economic development, and that the full range of abilities and principles97 that drive our work and the success of the Internet apply globally.

From early in the history of the Internet, the Internet technical community, civil society, governmental organizations, and private industry, among others, have focused on the opportunities and challenges related to the Internet in emerging economies. So this also should be true regarding opportunities and challenges related to the Internet of Things

Economic and Development Opportunities

In terms of opportunity, McKinsey Global Institute notes that IoT technology has significant potential in developing economies. By 2025, they project that as much as 38% of annual economic impact of IoT applications will derive from less developed regions.[99] From an economic perspective, it is expected that both demographics and marketplace trends will drive opportunity. For example, developing countries have a high potential number of IoT users (particularly in China), global economic growth is shifting to developing economies, and industrial IoT applications (such as in factories, worksites, and transportation) are expected to drive economic value creation.[100]

Should expectations regarding innovation and application of the technology be realized, IoT implementations could hold considerable promise as fundamental enablers of social development, including the achievement of the United Nations Sustainable Development Goals.[101] The Sustainable Development Goals, or SDGs, are a set of 17 goals framing over 100 development targets aimed at guiding efforts to achieve dignity, wellbeing, and equality for all the world’s people -- especially the poor and underserved. They cover the vast range of fundamental development challenges, including sustainable agriculture, energy, water availability, industrialization, and management of terrestrial and maritime resources, among others.

In considering the potential for smart object and Internet of Things technology to meaningfully address development challenges, the opportunities appear compelling. For example, the application of sensor networks to environmental challenges, including water quality and use, sanitation, disease, and health, climate change, and natural resource monitoring, could have significant impact beyond resource management. The data derived from such applications also could be used in research contexts, assisting local scientists and universities in making unique contributions to the broader body of global scientific knowledge and providing an incentive for local academic talent to stay in country to conduct research.

The growing world population, particularly in emerging economies, and challenges associated with providing access to quality, safe, and affordable food are set to grow over time. The potential use of IoT to combat hunger and promote sustainable agricultural has received particular attention, perhaps more than any other development issue.[102] From managing agricultural production cycles, disease threats, and growing inputs through to automated harvesting, distribution logistics, and quality monitoring, IoT-enabled "smart agriculture" techniques are envisioned across the entire value chain to improve the sustainability and productivity of the food supply.[103,104]

project description:

Introduction

Today I am going to talk about a very useful project that I had taken up. It is called the Water Level Indicator. Nowadays everybody has overhead tank at their homes. But everyone who has a water tank above knows the kind of problems that they face. Firstly there is no system to track the water in the tank. Then there come a secondary problem that is when their water pump is started they have no idea when it gets filled up and sometimes there are situation where the pump keeps on *pumping water to the tank* and the water starts *spilling out from the tank.* There is wastage of energy as well as *wastage of water*.

Later History

This project that i had taken up is the result of long hours of research of work at the Internet as well as long hours of thinking. I had made various *versions* of the projects earlier but at last i came up with this *final product.* I bet this has been tested and i can now firmly say that the model would work flawlessly without any complains for years. I am saying this as i have installed this models to various houses in my neighborhood and all are working fine without any maintenance. And indeed this model is admired by all who uses it.

The Situation

The house where I live in has an overhead tank which is about 30 feet from the ground level. I was getting bored going up the rooftop to check whether the tank has filled or the water level was below to start the pump. I had to do this again and again. Then I sought for a solution. I always used to think of the possibilities of how can this problem be tackled in an electronic way. After years of research and by trial and error, I found one and wanted to put whatever I have done out here so that it may be helpful to someone who has a overhead water tank at their homes

Basically the unit is made up of various sensors *acting as a switch*. Let me explain in a simple way. What happens is when you turn on you water pump, the water starts to get pumped from your underground reservoir or from your underground water supply from the pipes to your water tank. In the tank there is a *set of sensors(to be precise there are 7 sensors),* in the water tank. Just think them as a switch, as the work of the sensor will be to connect a circuit. . So the water starts to get filled in the tank and when the water level in the tank starts to rise up, what happens is that the sensors that is installed in the tank starts to get activated one by one indicating the water level in the tank. And finally when it reaches to its top most sensor, there will be a visual display as well as a sound from the unit indicating that the water has filled in the tank and one can be alerted that the tank has been filled up and the water pump has to be *switched off* saving the *electricity bill* as well as *over flow of water from the tank.*

There are Four parts in this project:-

(i) The Sensor Part

It is generally a fixed support inside the tank having some nuts and bolt with wires coming out.

(ii) The Circuit Part

It comprises the brain of the module, where in all the various inputs from the sensors are fed. It is the unit from where you will get all the information of how much of water is in the tank.

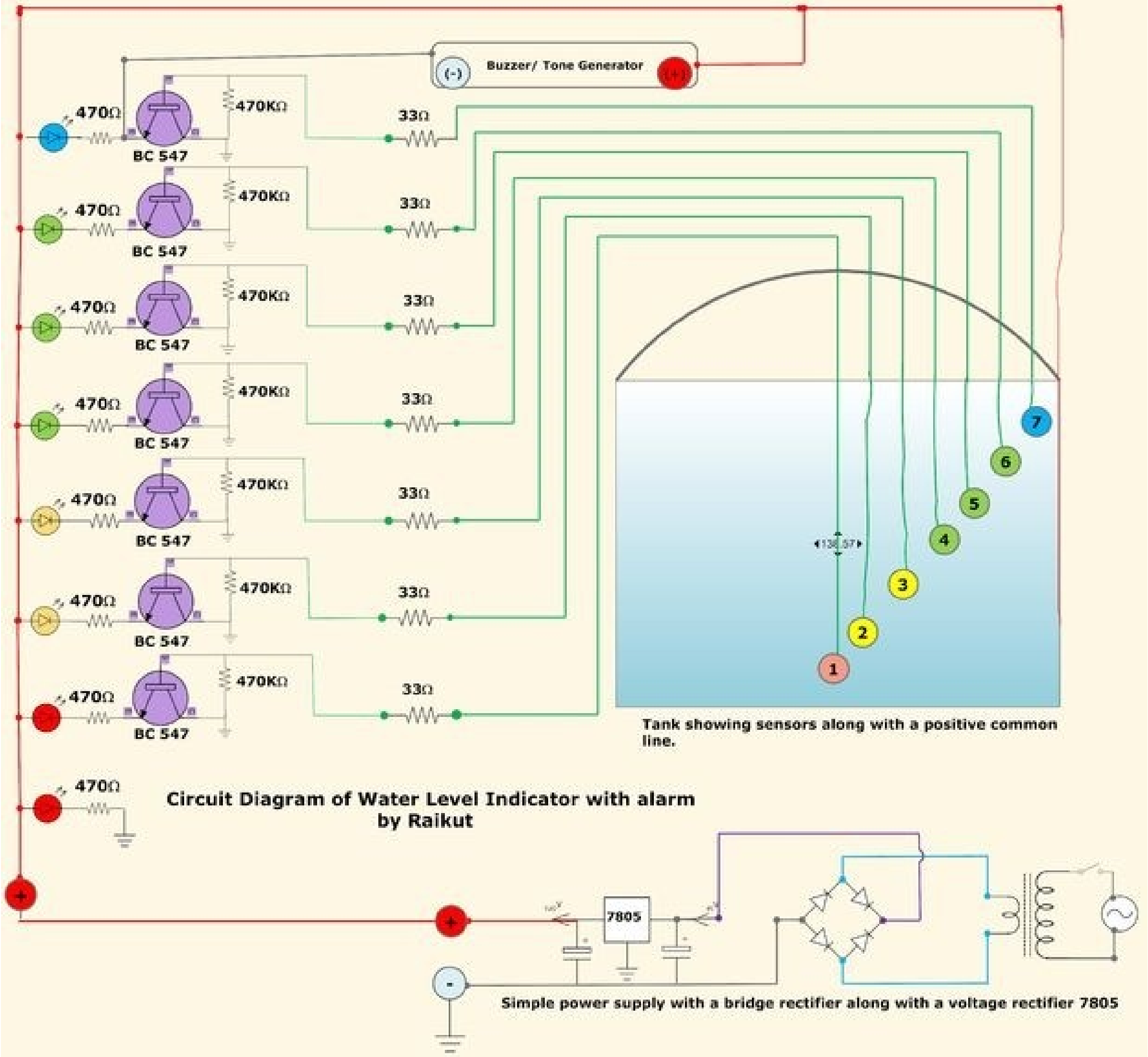
(iii) The Power Supply

It is the part where in you will be converting the A/C voltage to a regulated voltage of 5V to the Circuit.

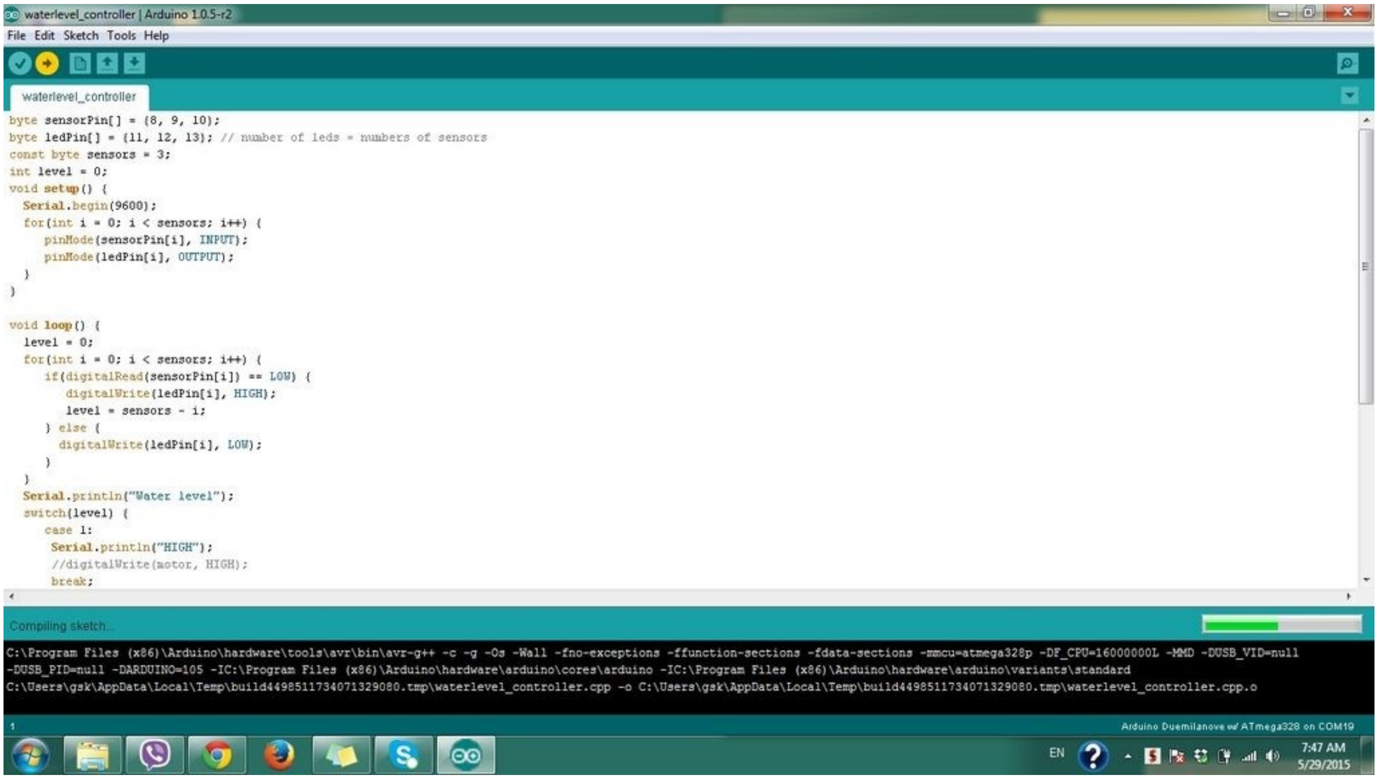
(IV) The Buzzer Part

It is responsible for bringing up the sound when the water level fills up in the tank. It will also be having a speaker or a buzzer to alert

The Circuit


(-)
Buzzer/ Tone Generator
(+)
470Ω
BC 547
470KΩ
33Ω
1
2
3
4
5
6
7
Tank showing sensors along with a positive common line.
Circuit Diagram of Water Level Indicator with alarm by Raikut
+
-
7805
Simple power supply with a bridge rectifier along with a voltage rectifier 7805

source code:



waterlevel_controller | Arduino 1.0.5-r2
File Edit Sketch Tools Help
waterlevel_controller

```
byte sensorPin[] = {8, 9, 10};
byte ledPin[] = {11, 12, 13}; // number of leds = numbers of sensors
const byte sensors = 3;
int level = 0;
void setup() {
  Serial.begin(9600);
  for(int i = 0; i < sensors; i++) {
     pinMode(sensorPin[i], INPUT);
     pinMode(ledPin[i], OUTPUT);
  }
}

void loop() {
  level = 0;
  for(int i = 0; i < sensors; i++) {
     if(digitalRead(sensorPin[i]) == LOW) {
        digitalWrite(ledPin[i], HIGH);
        level = sensors - i;
     } else {
       digitalWrite(ledPin[i], LOW);
     }
  }
  Serial.println("Water level");
  switch(level) {
     case 1:
      Serial.println("HIGH");
      //digitalWrite(motor, HIGH);
      break;
```

Compiling sketch...

```
C:\Program Files (x86)\Arduino\hardware\tools\avr\bin\avr-g++ -c -g -Os -Wall -fno-exceptions -ffunction-sections -fdata-sections -mmcu=atmega328p -DF_CPU=16000000L -MMD -DUSB_VID=null
-DUSB_PID=null -DARDUINO=105 -IC:\Program Files (x86)\Arduino\hardware\arduino\cores\arduino -IC:\Program Files (x86)\Arduino\hardware\arduino\variants\standard
C:\Users\gsk\AppData\Local\Temp\build4498511734071329080.tmp\waterlevel_controller.cpp -o C:\Users\gsk\AppData\Local\Temp\build4498511734071329080.tmp\waterlevel_controller.cpp.o
```

Code In C

```
byte sensorPin[] = {8, 9, 10};

byte ledPin[] = {11, 12, 13}; // number of leds = numbers of sensors
const byte sensors = 3;
int level = 0;
void setup()
{
Serial.begin(9600);
for(int i = 0; i < sensors; i++)
{
pinMode(sensorPin[i], INPUT);
pinMode(ledPin[i], OUTPUT);
}
}
void loop()
{
level = 0;
for(int i = 0; i < sensors; i++)
{
if(digitalRead(sensorPin[i]) == LOW)
{
digitalWrite(ledPin[i], HIGH);
level = sensors - i;
}
else
{
digitalWrite(ledPin[i], LOW);
}
}
Serial.println("Water level");
switch(level)
{
case 1:
Serial.println("HIGH");
break;
case 2:
Serial.println("AVERAGE");
break;
case 3:
Serial.println("LOW");
break;
default:
Serial.println("NO WATER");
break;
}
delay(50);
}
```

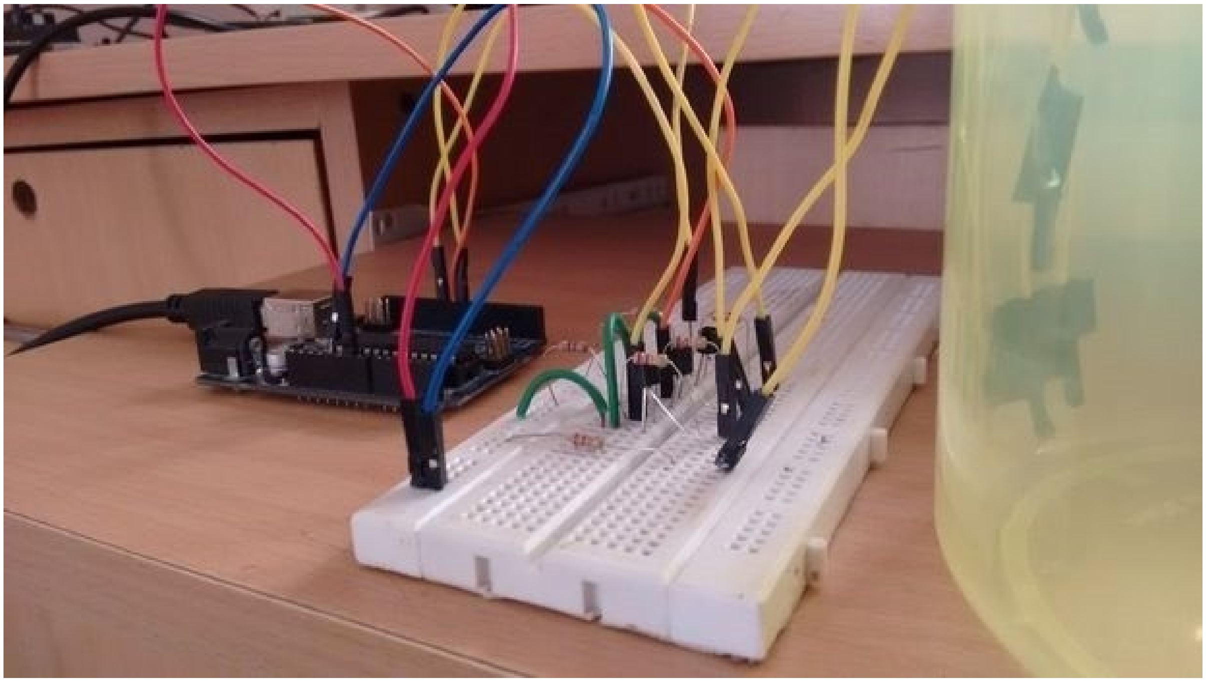
The Buzzer Part

Here you can add any of the normal buzzers that are readily available in the market and if it is not then you can make yourself with a simple 555 IC. I am giving a small circuit diagram, it is really simple to make and there are minimum parts. It is a simple audio oscillator. I have also provide a circuit diagram here but if you are able to manage a buzzer then no need to assemble this circuit.

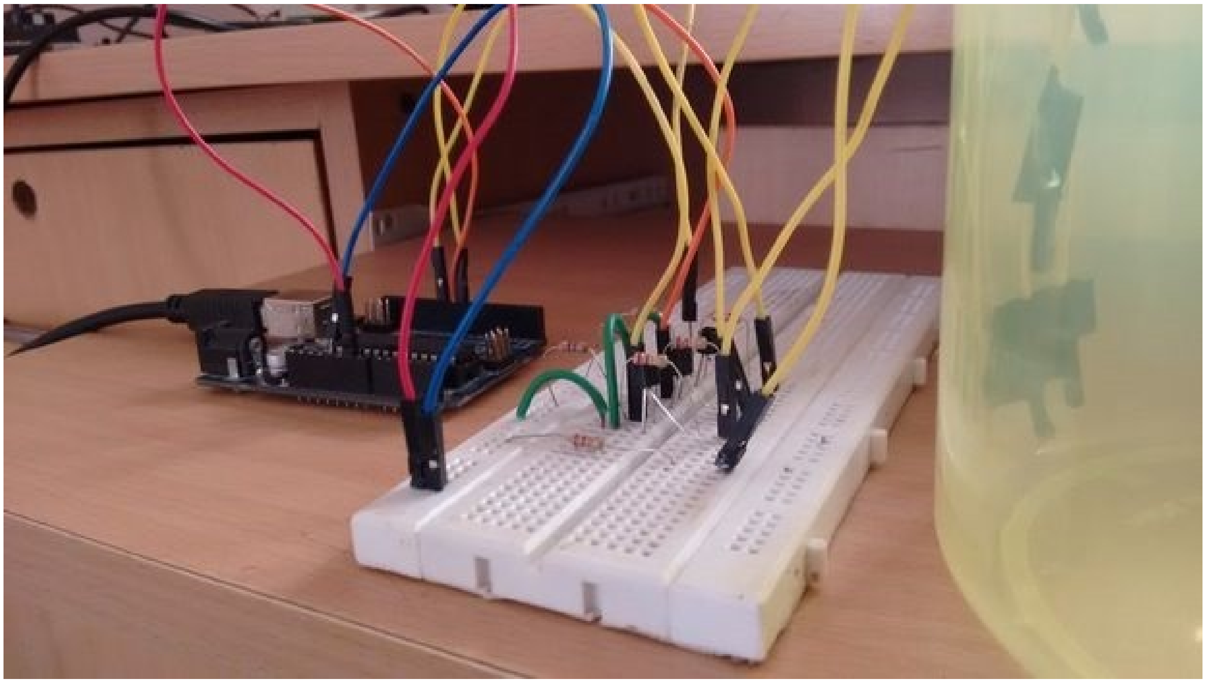
The Power Supply

This section contains a transformer converting the mains voltage 220V bring down to 9V. There is a bridge rectifier containing 4 diodes and making the Alternating current to Direct Current. After the filtering the voltage is then directly fed to the voltage regulator (7805) with a filtering capacitor. From the regulator IC the output voltage is then again filtered with a capacitor and is fed to the circuit. This comprises the power supply of the device.

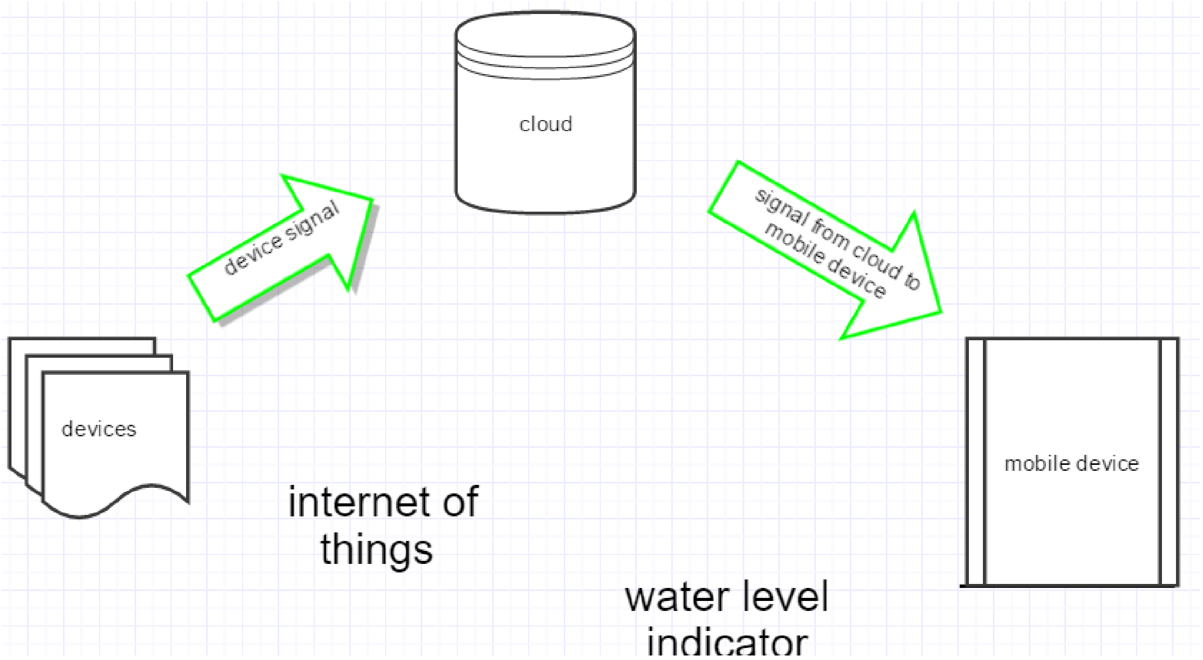
HARDWARE SETUP 1:



HARDWARE SETUP 2:

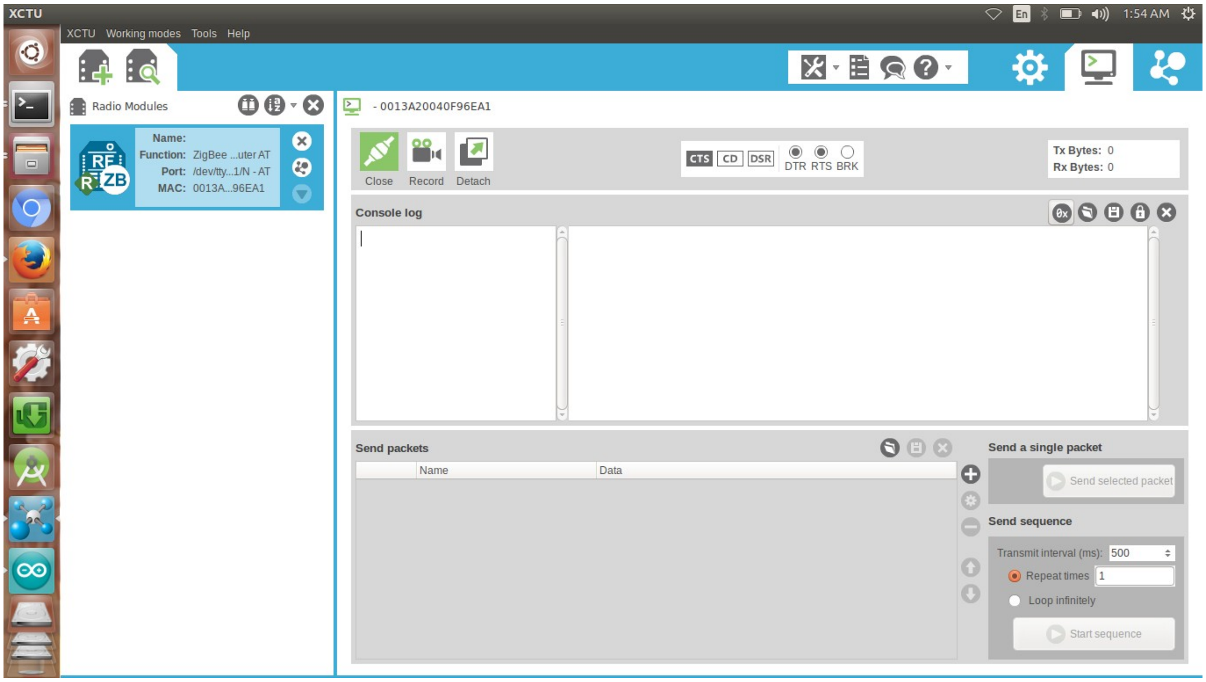


Brief overview of working of project



Output on emulator:

Starting phase:



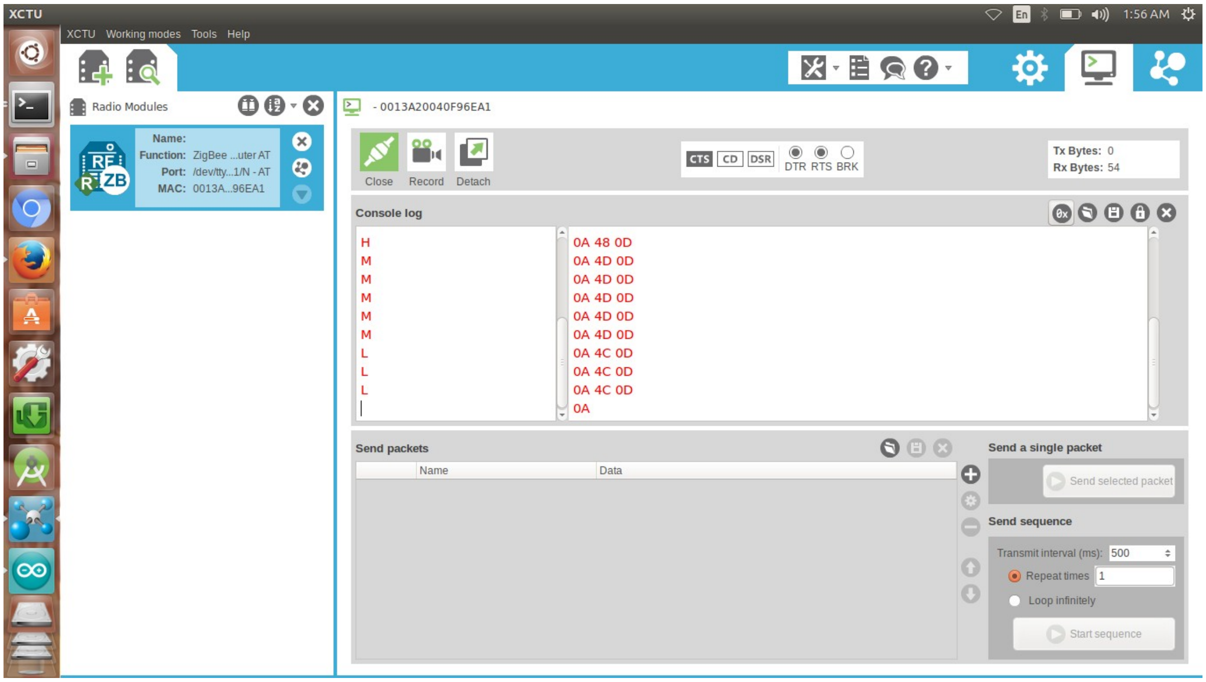
- 0013A20040F96EA1

Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

Tx Bytes: 0
Rx Bytes: 0

Transmit interval (ms): 500
● Repeat times 1
○ Loop infinitely

Second Level:



- 0013A20040F96EA1

Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

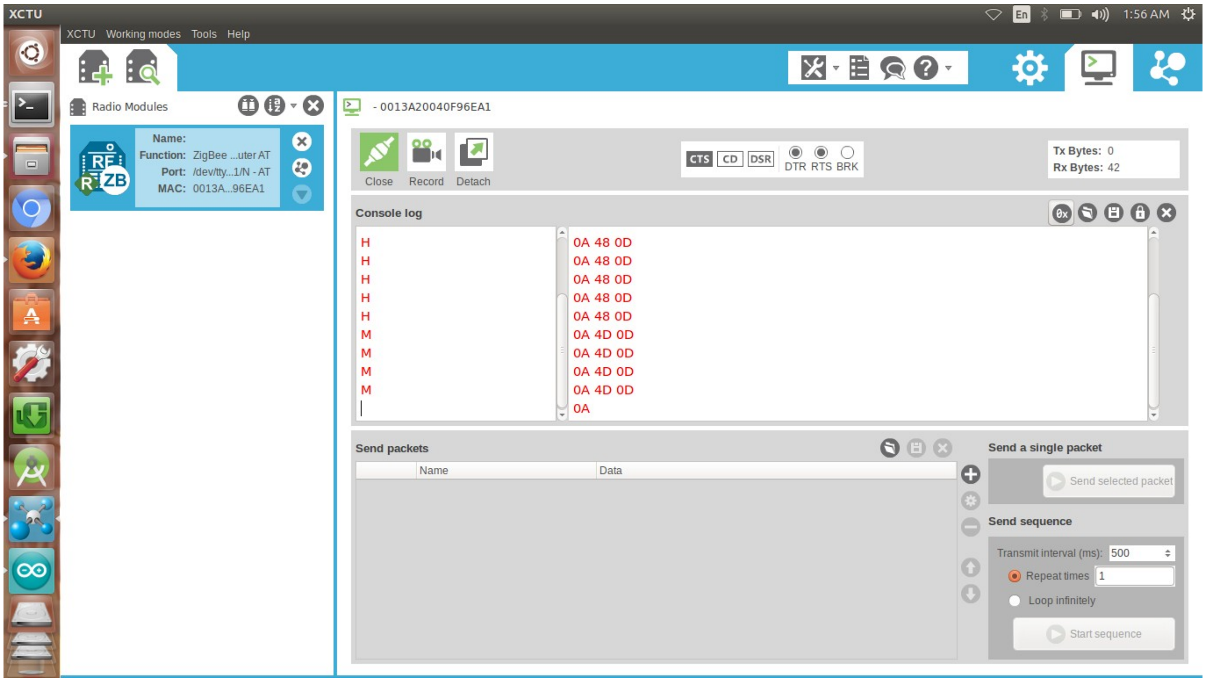
Tx Bytes: 0
Rx Bytes: 54

Console log

```
H    0A 48 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
L    0A 4C 0D
L    0A 4C 0D
L    0A 4C 0D
     0A
```

Transmit interval (ms): 500
● Repeat times 1
○ Loop infinitely

Third Level:



Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

- 0013A20040F96EA1

Tx Bytes: 0
Rx Bytes: 42

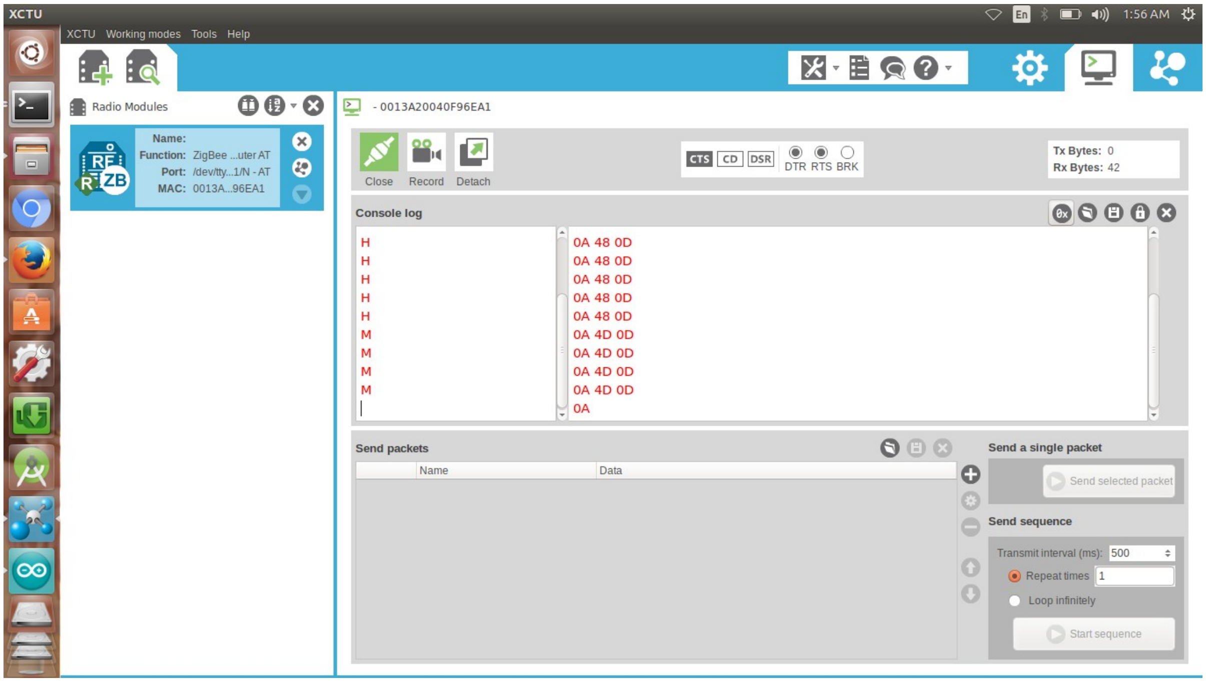
```
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
     0A
```

Name	Data

Transmit interval (ms): 500

● Repeat times 1

Medium Level:



- 0013A20040F96EA1

Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

Tx Bytes: 0
Rx Bytes: 42

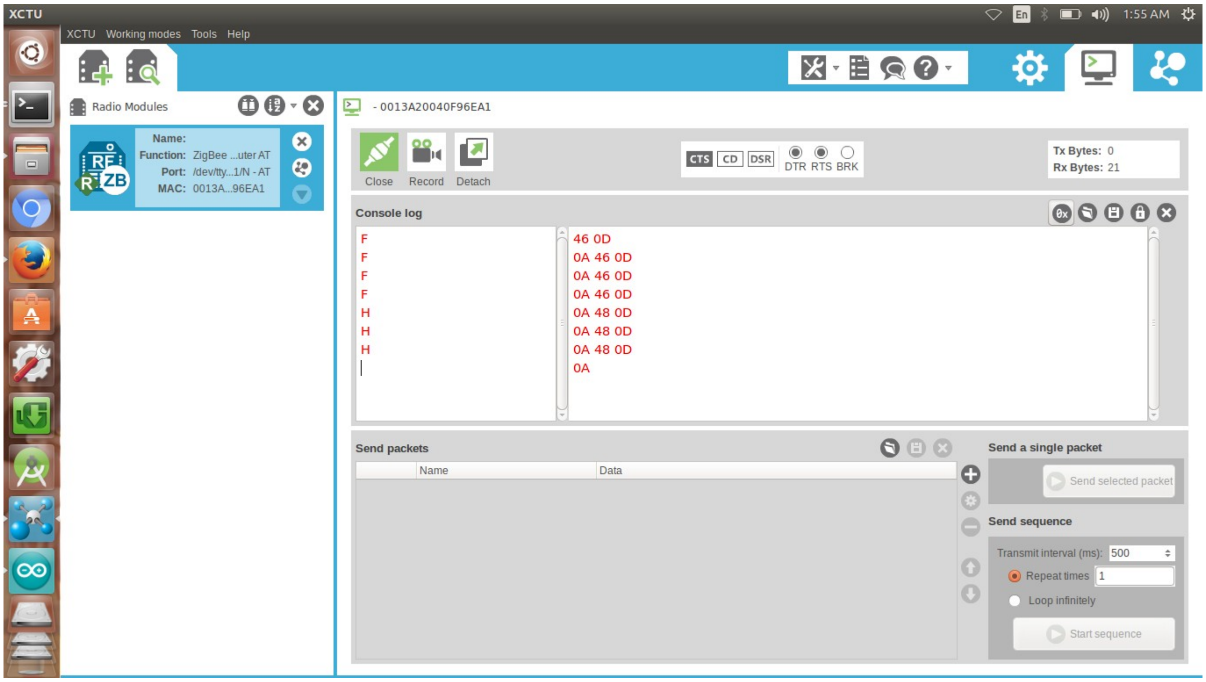
```
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
M    0A 4D 0D
     0A
```

Transmit interval (ms): 500

● Repeat times 1

○ Loop infinitely

High Level



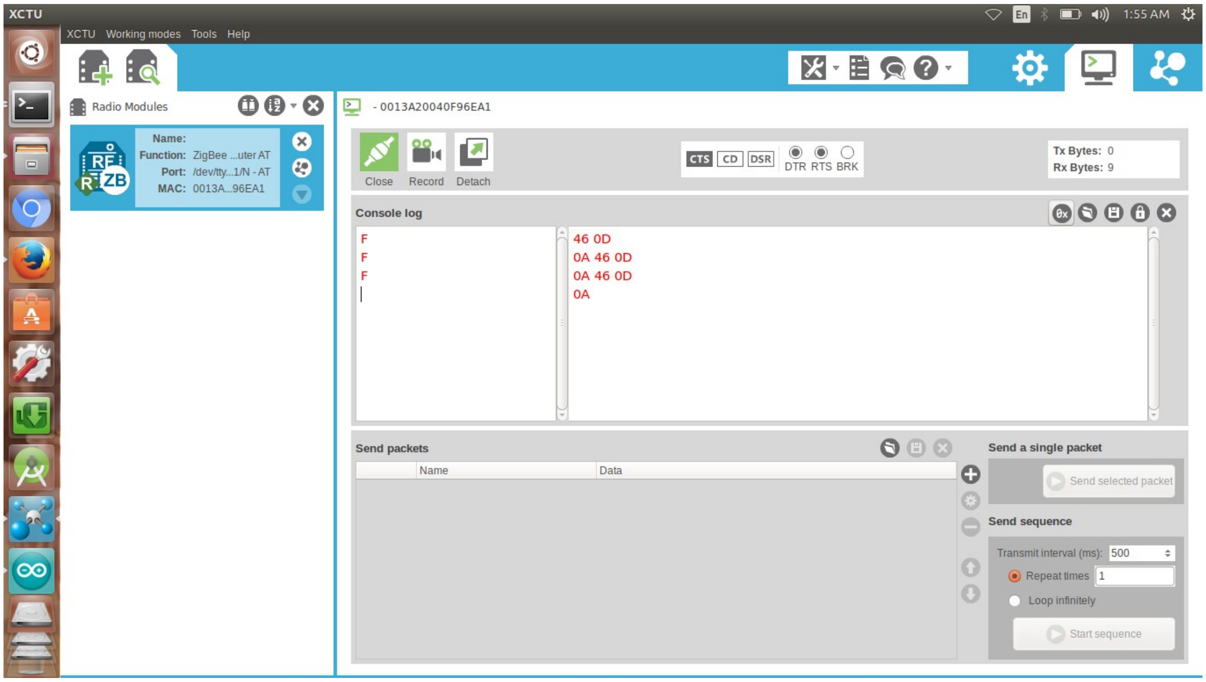
Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

Tx Bytes: 0
Rx Bytes: 21

```
F    46 0D
F    0A 46 0D
F    0A 46 0D
F    0A 46 0D
H    0A 48 0D
H    0A 48 0D
H    0A 48 0D
     0A
```

Transmit interval (ms): 500
● Repeat times 1
○ Loop infinitely

Full Level:



- 0013A20040F96EA1

Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

Tx Bytes: 0
Rx Bytes: 9

```
F        46 0D
F        0A 46 0D
F        0A 46 0D
         0A
```

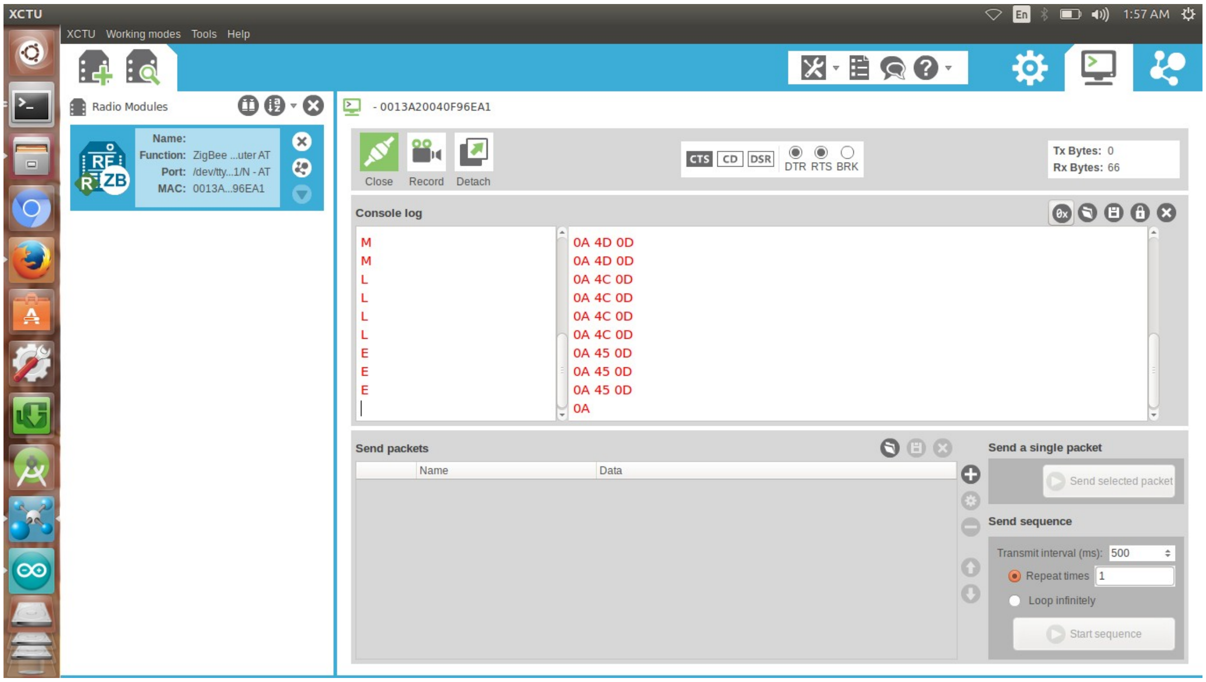
Name	Data

Transmit interval (ms): 500

● Repeat times 1

○ Loop infinitely

Last Level:



Name:
Function: ZigBee ...uter AT
Port: /dev/tty...1/N - AT
MAC: 0013A...96EA1

- 0013A20040F96EA1

Tx Bytes: 0
Rx Bytes: 66

```
M      0A 4D 0D
M      0A 4D 0D
L      0A 4C 0D
L      0A 4C 0D
L      0A 4C 0D
L      0A 4C 0D
E      0A 45 0D
E      0A 45 0D
E      0A 45 0D
       0A
```

Transmit interval (ms): 500
● Repeat times 1
○ Loop infinitely

➢ References:

Reference to a book:
[1] Porup, J.M. ""Internet of Things" security is hilariously broken and getting worse". Ars Technica. Condé Nast. Retrieved June 27, 2016.
Reference to web page:
[1] http://www.instructables.com/id/Water-Level-Indicator-with-Alarm/

Reference to research paper:

Raikut , Water Level Indicator with Alarm,Retrieved from http://www.instructables.com/