**Analysis and Challenges of Security In Internet of Things**

BY

**RAVIKIRAN YADAVA**

A Graduate Paper in

Partial Fulfillment

Of the

Requirements for Master Degree of

MASTER OF SCIENCE

In Electrical Engineering

Approved by:

Professor -

**(Associate Professor Mark Indelicato)**

Professor-

**(Dr. Sohail A. Dianat - Department Head)**

**DEPARTMENT OF ELECTRICAL AND MICROELECTRONIC ENGINEERING**

**KATE GLEASON COLLEGE OF ENGINEERING**

**ROCHESTER INSITUTE OF TECHNOLOGY**

**ROCHESER, NEW YORK**

**ABSTRACT**

Internet of Things is a network of Physical objects comprised of electronics and software for data processing and analysis, sensors for transferring information from person to machine (P2M) and machine to person (M2P) and network connectivity through internet for global and local transmission of sensor data for processing and storage purposes. As the Internet or World Wide Web connected the people across the globe into a single real time network of nodes, Internet of Things is diminishing the distance between inanimate objects of every description and building an automated network for these devices with very little human involvement. IoT has enabled the inanimate objects to be connected to the internet using sensors and controllers.

IoT technology in simple terms is a network of physical devices connected to the internet through radio frequency identification (RFID). It supports various types of input-output devices and sensors like camera, microphone, keyboard, speaker, monitors, near field communication (NFCs), Bluetooth, IR tags. All these systems can be connected through RFID systems that can detect idle or moving devices.

Security is the fundamental requirement for safe and reliable operation of IoT connected devices. Because the idea of networking applications using IoTs is relatively new, security has not always been considered in the product design. IoT devices often come with the outdated software and operating systems. Sometimes user may use less secure passwords for critical IoT devices like a heart rate monitor. Network firewalls and internet protocols secure the internet at system level but there is security protocol void at the embedded endpoint device level, there is not enough computational capacity on these devices for implemented advanced security protocols. Existing state of the art protocols require application layer gateways at both software and hardware level that provides application specific connectivity to IoT devices.

This paper considers important security issues related to the IoT devices and networks and analyzes the threat models and challenges to solve the security issues. Chapter 1 describes about the basics of internet of things and their working towards the field of RFID. This chapter mainly talks about the Machine to machine communication where the central servers and multiple devices that do not require direct human interaction. Chapter 2 describes about the machine to machine communication, RFID tags, RFID anti collision protocols and the implementation towards the internet of things. Chapter 3 discusses about the architecture of Internet of things, in which various aspects of headers which are used. Finally chapter 4 discusses about applications of internet of things such as smart grid and wearable technologies.

The abstract of 280 words is approved as to form and content

Associate Professor Mark Indelicato

Department of Telecommunication Engineering

**TABLE OF CONTENTS**

CHAPTERS PAGES

ABSTRACT ……………………………………………………………………………………………………………………………. 4

ACKNOWLEDGMENTS…………………………………………………………………………………………………………….5

LIST OF FIGURES………………………………………………………………………………………………………………………6

LIST OF TABLES……………………………………………………………………………………………………………………….7

CHAPTERS

CHAPTER 1 – INTRODUCTION TO INTERNET OF THINGS ………………………………………………………….8

CHAPTER 2 – Machine to machine communication…………………………………………………………………14

CHAPTER 3 – Architecture of Internet of things ………………………………………………………………………19

CHAPTER 4- Few Internet of things application Smart Grids and Wearable’s…………………………..31

Conclusion……………………………………………………………………………………………………………………………….37

References………………………………………………………………………………………………………………………………39

**ACKNOWLEDGEMENTS**

Working with Professor Mark Indelicato was a valuable experience. I would like to thank for giving me this opportunity and his support, guidance and motivation. I was fortunate to have him as my mentor. I am very grateful to him for his cooperation and accommodation for letting me finish my grad paper after such long break.

And also I would like to thank my fellow mates and my friends in my Master program with whom I have worked in course assignment and course projects. Without their presence my Masters program would not have successful.

Finally I would like to thank my parents and family members for supporting in every way possible and helping me succeed.

**LIST OF FIGURES**

|  |  |
| --- | --- |
| Figure 1 |  |
| Figure 2 |  |
| Figure 3 |  |
| Figure 4 |  |
| Figure 5 |  |
| Figure 6 |  |
| Figure 7 |  |
| Figure 8 |  |
| Figure 9 |  |
| Figure 10 |  |
| Figure 11 |  |
| Figure 12 |  |
| Figure 13 |  |
| Figure 14 |  |

**LIST OF TABLES**

|  |  |
| --- | --- |
| TABLE 1 |  |
| TABLE 2 |  |
| TABLE 3 |  |
| TABLE 4 | Analysis of Reduction of Junction temperature [6] |

**CHAPTER 1**

**INTRODUCTION TO INTERNET OF THINGS**

In internet of things the objects around us such as automobile, home appliance and security devices will be on the network in one form or the other. A large amount of data which have to be stored, processed and presented in a seamless, efficient and easily interpretable form. There are other ways to provide the virtual infrastructure for utility computing which combines monitoring devices, storage devices and client delivery by the use of cloud computing. The indispensable part of internet of things is use of smart connectivity with existing networks and context aware computation using network resources [1]. For the internet of things to be successful the computing paradigm will need to go beyond traditional mobile computing devices that use smart phones; and they try to evolve into connecting everyday existing objects and embedding intelligence into our environment. A progressive evolution of current Internet into a network of interconnected objects that not only harvest information from sensing and interacting with physical world but also using existing internet standards to provide service for information sending, analytics, application and communication[1]. This revolution has made interconnection between people at unprecedented scale and pace and further there will be interconnection of various objects to create a better environment. In 2011 a number of interconnected devices have overtaken the total number of people. Currently there are 9 billion interconnected devices more than total number of people [1]. The discovery of internet has made a milestone in achieving ubicomps vision which provides individual devices to communicate with any other devices in the world. The proceeding in Advanced technology have made system technology, wireless communication, and digital electronics has made a tremendous improvement in devices having the ability to sense, compute and communicate wirelessly in short distance[1]. These nodes used to interconnect the devices to form wireless sensor networks and finding a wide range of application in environmental monitoring, infrastructure monitoring and traffic monitoring. It has been said by Atzori that internet of things can be perceived in three paradigms such as Middleware, sensors and knowledge, due to interdisciplinary nature of the subject, the usefulness of internet of things can realized only in an application domain where the three paradigm intersect.

C:\Users\Shiv Sagar\Downloads\first1.png

Figure 1: Internet of things schematic showing the end users and application based on data [1]

Technological improvement towards the low power integrated circuits and wireless communication have made available for low cost and efficiency is increased in remote sensing application [1]. As result of this the visibility of utilizing a sensor network consisting a large number of intelligent sensors, enabling the collection. Wireless sensor network consists of components that monitor the network such as WSN hardware, WSN communication stack, WSN middleware, secure data aggregation.

1. WSN hardware – A node consist of sensor interfaces, processing units, transceiver units and power supply [1]. And there is always a multiple Analog to digital converts for sensors interfacing and more modern sensor nodes that can communicate with one frequency band.
2. WSN communication stack- Deployment of nodes should be done using Ad-hoc. WSN nodes should be able to communicate themselves to transmit data in single or multiple hops to the base station. For the internet to act as subnet between the outside world and the internet , the communication should be established [1]
3. WSN Middleware- To provide access to the heterogeneous sensor resources in deployment independent manner, a procedure is used to combine cyber infrastructure with service oriented architecture and sensor networks. Open sensor architecture is used for developing sensor application which is platform independent middleware [1].
4. Secure data aggregation – The lifetime of the network can be extended and also to ensure the reliable data collected from sensor a method called secure data aggregation is used [1].

In telecommunication field where people try to contact each other by sending information across different places and different time zones which can be done by instant messaging or through emails. In today’s generation where with help of mobile internet services and utilizing high speed mobile network such as 3G or 4G, users can connect each other from any location [2].

C:\Users\Shiv Sagar\Downloads\telecoomm_network.png

Figure 2: Internet of things in field of Telecommunication environment [1]

Connectivity will take entirely on new dimension; users can connect at any time and at any location. Nowadays it is possible to make communication at any time and at any location. With the benefit of integrated information processing capacity, industrial products will take on smart characteristic and capabilities [2]. Electronic identities can be queried remotely or can be fitted with sensor for recognizing physical changes around them and sometimes even particles and dust might be tagged and networked. These improvements will make the static objects into dynamic things. The importance of creation of internet of things is that it will entail the connection of everyday object and devices to all kinds of networks for example company intranets, peer to peer to network and global network. As a result of this establishment, a lot of advantages in telecommunication industry will be seen [2]. There would be many challenges within the existing structures within established companies and they form a new opportunities and business models. A revolutionary success can be seen in field of mobile and internet networks by expanding the world network by the application of technological enablers such as Radio frequency identification. Through RFID it will be able to detect and monitor changes in the physical status of connected things. Internet of things is not a single technology; it’s a concept in which most new things will be connected and things like embedded sensors, image recognition functionality, and augmented reality, which is close by to field communication and decision support [2], asset management and new services. There is a heterogeneous mix of communication technologies to accommodate the diversity of the internet of things which can be adapted in order to address the needs of internet of things application such as energy efficiency, security and reliability [2]. It is possible that the level of diversity will be scaled to number of manageable connectivity technology that address the needs of internet of things application, that can be adopted by the market which have proved to be serviceable which include wired and wireless technologies like Ethernet, Wi-fi, Bluetooth and Z-wave.

Internet of things gives a best solution when all the components are integrated with information technology which has both software and hardware which can be used to store, retrieve and process data communication technology which includes electronic system used for communication between individual. The rapid convergence of information and communication will take place in three layers of technology such as cloud, data and communication [2].

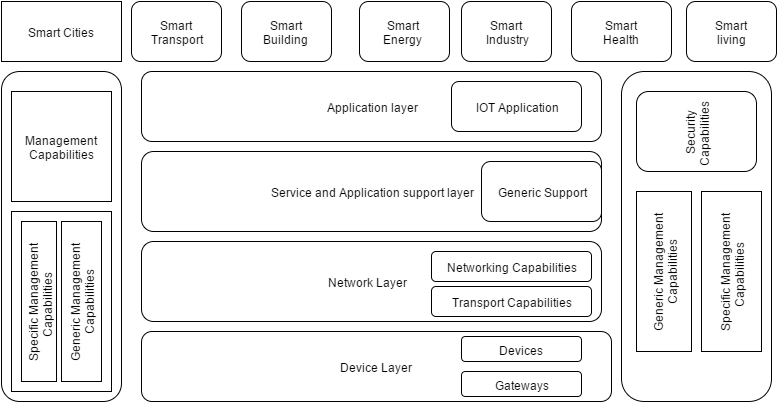


Figure 3: Internet of thing layered architecture [2]

Internet of things is not an only a network of computers but also a network of devices of all types and sizes, vehicles, mobile, refrigerator, micro oven and industrial systems. The internet of things has different levels of abstraction through value chain from low level semiconductor through the service providers. The growth of enabling technologies such as nano-electronics, communication, sensors, smart phones, embedded systems, cloud networking, network virtualization and software will be important aspect to provide to things the capability to be connected all the time everywhere. Technologies such as embedded or cyber physical system form the edge of internet of things bridging the gap between cyber space and physical world of real things and are important in enabling internet of things to deliver on its vision and become a part of the bigger system[3]. The internet of things brings about a paradigm were everything should be connected which makes machines and humans interfaces and the way they interact with world around them. The automation and management of asset intensive enterprise will be transformed with the rise of internet of things. New high performance systems which can support internet and cloud as well as predictive asset management are reaching the market. These development have the potential to radically transform products, channel and company business model as result will create disruption in business and opportunities for all types of organization [2]. The internet of things concept to refer uniquely identifiable things with virtual representation in an internet like structure and the internet of things which makes them compromise for other details:

* Module for interaction with local internet of things which can be used for various resources
* Machine to machine communication solution and services which have a wider role to play
* The infrastructure which can be constructed to large scale production for data analysis and for management system
* The Market for machine to machine communication can applied effectively for the development of smart, sustainable societies and cities
* In private sector where internet of things are rapidly becoming an area of concern for professional working in the place.

**CHAPTER 2**

**Machine to Machine communication**

Machine to machine communication, where two machines communicate each other is done within devices of the same type and for a specific application with wireless communication networks. The machine to machine communication solutions will allow an end user to capture data about the events such as temperature or inventory levels. Machine to machine communication can achieve productivity gains; reduce cost and increase safety or security. Connectivity has been a main focus for other enterprise scenarios namely vending machines or online card transaction [3].

M2M device

Enterprise process

Service enablement

Asset

Application

Figure 4: Machine to Machine system solution [3]

A machine to machine system solution consists of Machine to Machine devices, Communication network, Application, Service enablement and enterprise process. Figure 4 tell us about the machine to machine communication network where the asset which connect to the machine to machine device, providing sensing and actuation capabilities. Machine to machine devices can be categorized into number of different realization of the devices which has both low end sensor nodes to high end devices [3]. The machine to machine device is then connected to network which can provide remote connectivity between the machine to machine device and the server side. In the network node consists of Wide area network and local area network. The network node has one more name to that called capillary network or machine to machine area networks. The main purpose of the network node is to provide remote connectivity between machine to machine device and server side [3]. The service enablement can do a generic functionality which is common to a number of different applications; the purpose was to reduce cost of the implemented design and the ease of application development. The application node which is connected to the enterprise process thus can be separated into a business process system of the enterprise. Machine to machine communication can explained in such way that when the a large number of devices such as sensors and other system which are connected to the internet, the internet of things ecosystem comes into picture where the electronic appliance can communicate, connect and interact the same way the human beings do, as a result of which the day to day task gets reduced and it makes the task much faster. Machine to machine architecture can be build to solve problems, application of interest and get solutions when there would be errors occurring while communicating in the machines. The problem is solved by taking reference architecture is used get the design of applied architecture. This architecture which had been taken as reference architecture is the blueprint to the system solution.

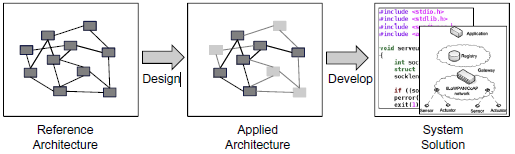


Figure 5: From Reference architecture to system solution [3]

From the figure 5 it can seen that the reference architecture is taken and design rules are applied, before applying the design rules the overall objective of the architecture should be clear and the design principles should also be formulated which is got by simulating the major system solution [3]. For example an overall objective might be to remove the application logic from communication mechanism and the design rules would be design for protocol interoperability and to design for the encapsulated service descriptions. Sometime the system solution will be in form of the code written in any of software language such as C++ or JAVA. So to create a system solution the applied architecture should follow the design rules, for example the one node which created from the previous node will be functional or behavioral. And the written code will be synthesized into hardware and that hardware can hardwired into a circuit boards for further testing [3].

C:\Users\Shiv Sagar\Downloads\changes.png

Figure 6: Problem and Solution partitioning [3]

The problem and solution partitioning is a partitioned into System solution, Concept base technologies and needs problems constraints. The problem domain mainly deals with the understanding the application of interest developed through a scenario and use those data get the solution of the problem [3]. In the problem domain where an application needs some problem constraints, that application requirement is gathered and sometimes the application will have business and technical constraints. An international industry called Open Geospatial Consortium (OGC) has few hundred companies; other companies provide other good standards that provide geographical information support to the web and other wireless services [3]. Open Geospatial Consortium (OGC) has partnered with Sensor Web Enablement to develop standards for Sensor system model, sensor information model and also the sensor Web services that follow the service oriented architecture. The main functions of OGC and SWE are:

1. More research on Sensor capabilities and quality measurement
2. The main the requirements of the sensor system and observation that will meet the application criteria
3. Subscription to, and alerts will be issued based on the services on certain criteria.

Some of the OGC [Open Geospatial Consortium] and SWE [Sensor web enablement] also include some of the standards.

1. SensorML and Transducer model language (TML) has an XML schema for sensor and actuator system and processes. A temperature sensor can be taken as an example which gives description about measuring temperature in Celsius, where this measurement is converted into Fahrenheit units.
2. For the observation and measurement of the sensor an XML and Observation and Measurement(O&M) model
3. Common data model by SWE for implementing low level models in the information exchanged between OGC and SWE functional entities
4. For requesting, filtering and retrieving observation and sensor information, a Sensor observation service is used which is an intermediary between client and observation repository
5. For an application requesting a user defined sensor observation and the measurement of acquisition , a sensor planning service is used[3]
6. Metadata information for serial port or Ethernet enabled sensor devices a protocol called PUCK is used.

The above standards mentioned here can be explained in detail by an example. The SAO paradigm follows the OGC which is then stored in CAT which is maintained by the previous OGC services. After the installation of the sensor system using the PLUCK protocol. The registers in the SOS [4] , where the client send a request to the sensor planning service for which a every sensor has 10 seconds and publish the measurements using O&M and SWE model . One more request is sent by the client application 2 and looks up in the registers to locate an SOS model.

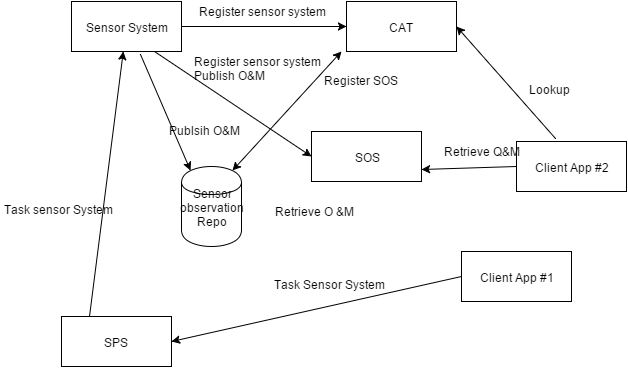


Figure 7: Sensor System [3]

In the figure 7 it can be seen that there are two client requests being sent. The client application 1 sends a request to SPS standard for taking care of the task sensor system, where the SPS can be made available to the above network for processing of the information [3]. Secondly after which the information is passed on from SPS to the sensor system via task sensor system or the register sensor system. After the completion of registration in the sensor observation repository it is returned back to the CAT [3]. The client application 2 makes a request to the SOS to retrieve the question and the measurement, the other part is also sent to the lookup table where the content is stored to make sure that when a search is made a register sensor system publishes onto CAT for proper validation.

**CHAPTER 3**

**Architecture of Internet of things**

The application which run through towards higher capabilities and processing speeds, but also which allows for very large application to run on these embedded processors. The market for the small scale embedded processors such as 8, 16 and 32 bit with flash memory, I/O capabilities and networking interfaces such as IEEE 802.15.4 which are developed on a tiny system on chip. These devices are capable of hosting an entire transmission control protocol which also includes small web server. Several properties such as power source, sensor and actuators, communication, Operating system, applications, User Interface, Device management and Execution environment [5]. These properties are hosted on gateway for several reasons such as a gateway can handle heavy function such as WAN connectivity and application logic that would require powerful processor as result of which leads to reduced cost.

There are two categories of devices such as Basic device and advanced devices. The basic device which can provide services of sensors reading and actuation task for LAN communication which is supported via wired or wireless technology as result of which gateway is needed to provide WAN connection [5]. In the case of advanced devices the application logic and the WAN connection would be hosted. The basic devices which can be employed for basic necessitate for example such as home alarms, smart meters, Building Automation System, Standalone smart thermostats, Onboard units, Robots and autonomous vehicles, Video cameras, Oil well monitoring and connected printers. These basic devices are often intended single purpose for measuring air pressure and other several functions which are deployed on the same devices for monitoring humidity, temperature and light level. A translator which serves as a gateway between different levels in the protocol layers and these Gateways perform translation of the physical and link layer [6]. The hardware which is in basic gateway which will focus on simplicity and low cost, but the frequently the gateway devices also used other task for data management, device management and for local application. The device management is very important for internet of thing which can provide efficient which can perform many of management tasks for device. The advanced devices which provide distinction between basic devices, gateways and advanced devices which will be characterize advanced devices.

The architecture reference model has basically two main parts for the functioning of the internet of things, the reference model and reference architecture. The reference architecture describes about a number of sub modules, where these sub modules tell us about the machine to machine communication and Internet of things [3]. There is barrier between the domain model and these sub modules where the user using the Internet of things visualize them and marks downs the relationship between these concepts [5]. The relationship between the sub modules and the main modules which serve as base for improvement of the information model to work for a system which needs to capture and process the information about the main entities and their uses.

C:\Users\Shiv Sagar\Downloads\Untitled Diagram.png

Figure 8: Internet of things reference model [3]

From the figure 8 it can been seen that the LOT domain model connects each machines explicitly through the main frequency controlled by each users, the frequency might vary according to the appliance based on the requirement and power each domain taking. The architecture model has similar attributes to reference architecture in many ways for example; the domain model which sends the concepts to functional group is same in both the reference model and architecture model.

**Architecture of Domain model**

The important model in reference model and architecture is Domain model which captures main concepts or entities in the domain and it also includes main concepts of specific area of interest like the internet of things. The unified modified language can be used for domain model; it consists of two classes such as CLASS A and CLASS B. Both these classes are interconnected with each other; both are connected through the dotted lines or solid lines which represent different characteristic. Each class have name to that and they have their own properties, usually class A would represent the name and other would represent the attribute [3]. In the figure 8 it can be seen that the first class name is also called IS-A relationship which is similar to the concepts in object oriented programming where the class B inherits from class A, the class a attributes will be called as objects which will be similar to class a [6]. These classes can classified further into Generalization, Aggregation and Reflexive aggregation, association.

C:\Users\Shiv Sagar\Downloads\classes.png

Figure 9: Architecture of Reference model [3]

Secondly the IS-A relation also known as Generalization, where child class inherits the properties from the parent class and sometimes the class b will have its own attributes associated with no one other class. The aggregation has class B attached to class A with diamond pointing towards the class A, the contents in class A varies differently to which other attributes can’t be matched with other composition. For example if one machine wants to communicate with other they need have some composition with either class A or class B. So for a machine which all the attributes that cannot be same as the class A but very similar to class B. So if one of class has a plain line or solid line, the domain model and reference model might have changes to the class explicitly associated with that class B [7]. As we can see from the figure 8 sometime there might be class that does not have the solid line or dotted line indicating that the mac address will be sharing between the two classes. The architecture of reference model can be implemented to physical world which would have direction relation with the digital world. The digital world would interact with the physical world with the software, for example a big parking lot in multiplex complex with lot car that have been parked, so sometimes there would be parking spot available and sometime there would not be [7]. By using the Internet of things and software related to this which will be installed in the phone, so the physical object which is the car tries to communicate with the sensors that would be placed in the parking lot, so when these sensors comes in contact with that, the owner would get message saying details of car parked. So the total number of cars parked in the parking lot will be calculated and the people who are trying to find a spot can easily get a spot and park their car which saves their time and fuel too [8]. So the human user who tries to communicate to physical object which is the car in the above example, binary data is sent to the software when the physical object tries making contact the sensor. So the digital artifact has two types a) Active Digital artefact and b) Passive digital artefact. So the passive digital artifact is when the physical object is passive with the sensor making no contact and the active digital artefact when the physical object is moving and sensor tries to communicate with it.

So the model which is capable of capturing the human to human application whether it is digital artefact or the passive artefact which really does not matter the, but the main the environment where the environment need is the devices or the machines where these device can be embedded with those properties [7]. So the device include three main types

1. Sensors: The basic properties of sensors are to detect, convert temperature into electrical signals, and they basically have transducer in them. The transducer function in the sensor is it converts the electrical signals into digital signals. For example a video camera has the function to detect the image and convert those into videos through sensors [3].
2. Tags: These tags are usually embedded into the device, the physical object will these tags making them detectable by the sensors. RFID acts a tag in the physical object and also the Quick response code acts like tags. The tags play vital role in the reference model, these tags can be printed on the physical objects.
3. Actuators: Actuators plays a similar role as a transducer but the actuators converts electrical signals to a change in physical property which has the potential capabilities of communication, intermediate storage and conversion of analog signals to digital. The actuators can function in two ways, firstly it can be mounted on the physical object or it can be placed near the mobile which can detect and make sure they have the right value towards the end [3].

So this software that is installed in the phone can have the controlling capabilities which have the device such as actuators, tags and the sensors. The lot reference model has other units such as the communication model where the devices are connected with other node that can be passed by human-service interaction or the service to service interaction [9]. The user interaction can have many features which have application accessing services or this service is based on typically on hyper text transfer protocol which are hosted on the embedded systems are constrained [9]. Secondly the communication model have several gateways which provides a bridge between customers and owners establish communication gap in the devices and these powerful devices which is makes multiple type of communication stacks which gives safety between the user and human digital artifacts. The concern in the lot architect is it can provide physical entities where the people can benefit from these features. So the device which can be equipped with reference model and communication model can have the physical properties which are transformed into electrical signals. The architecture model which includes the main method to include subscripts of the reference model may have the MAC address stored in that specific address or it may also contain entity level service which would later provide loops that are physically wired to the sensors.

**Sensor System**

The sensor systems which are used in almost every day devices that are mounted on the physical objects have the sensors build in them, the components of sensors which usually have conventional CMOS, actuators, biochips [8]. The application specific lot [internet of things] similar to application specific integrated circuits which have sensors specific to that application have end units and mid-units, whose application are power, security and cost. The lot power has desired life time depends on the element that are currently using such as Lithium polymer, Lithium thin-film and Alkaline [8].

C:\Users\Shiv Sagar\Downloads\vlsidesign.png

Figure 10: VLSI design using Internet of things [6]

The desired life time also changes based on the power budget and technology nodes that are currently being used in the industry. Some companies follow the 10µm which all the standard industries follow this technology node proposed by Moore law. In most device which have sensors build in them, these sensors which is capable of detecting the temperature and communication between environments via internet. These sensors can have key generators installed in them which could be controlled by internet, it main uses would include controlling the temperature which is a major beneficial factor for efficiency and performance of these devices. The keys which are generated by key generators have an address each time when a new key is generated and this key can be accessed by internet. The key is generated by the Fibonacci generator which is installed in Microblaze FPGA board and this can tested on various LVCMOS [low voltage complementary metal oxide semiconductor] for variety of temperatures such as C,C,,C. It was observed that as the frequency increases in the board the temperature also increases which makes these devices heated up and in-efficient. The sensors first detect the junction temperature in the sensors; junction temperature has the highest operating temperature in these electronic devices and various factor effect theses junction temperature such as its physical properties of semiconductor material and the diffusion rate of the dopant elements. The junction temperature can be calculated using, this is total ambient temperature of the sensor and the power dissipation of the senor [8].

(1) [6]

In the above equation 1 which describes about the junction temperature, as it can be seen that the power dissipation directly proportional to the junction to ambient thermal resistance. As the sub-threshold leakage in the CMOS increase there is a current inversion between the source and drain which is directly related to the gate voltage. By taking an example of reverse biased PN junction diode, the electrons flows from the valence band to conduction band. The sub threshold current which has exponential function of drain voltage which has very low makes the junction temperature very high [8]. As the channel length becomes smaller there would be a scaled CMOS which has a depletion layer width of the source and drain equals to the channel length.

In a sensor circuit usually we have three main attributes that has to be more efficient when compared with the temperature.

* Noise: With increase in junction temperature the thermal energy will also increase the energy of the charge carrier, this causes the charge carrier to increase and thermal energy will make more collision between electrons and increase the noises. The channel length of the CMOS and LVCMOS circuits makes more dependent on mobility of the electrons, the component of material, gradient temperature. The gradient temperature of CMOS is value of the junction temperature which directly proportional to the noise in the circuit, if noise decibels are more than required it the temperature might increase [6].
* Speed: If the temperature is more the speed is reduced due to various reasons, the propagation delay assumes that will increase the voltage and decrease the temperature but this assumption fails for low voltage application which causes cell delay as result of temperature values. The propagation delay of LVCMOS which is function of drain current and is sensitive device parameters. The temperature rise in the device will make circuit more vulnerable to reduction in speed of both of CMOS and LVCMOS circuits.
* Reliability: The circuit reliability degrades if it’s the operating temperature is more than the circuit temperature, the circuit temperature is maintained in order to maintain the MOSFET operating at very low temperature which makes the carrier mobility, decreasing the leakage current , improved electro migration. The mobility of electron and holes vary ranging on the electron size and hole size which will result in increase in temperature, which makes the reliability of the circuit
* Power Consumption: When temperature is high, the performance will be degraded as it consumes more power and the leakage current will automatically increase with temperature. So with increase in temperature the power consumption of the idle circuit will increase and make the leakage current more and the junction temperature will also increase [9].

For the above case the different temperatures were taken for the analysis of the junction temperature of for five different frequencies for which the increase in temperature was noted down for different frequencies from the range 0.5 GHz to 1 THz. At different ambient temperatures of C, C, the values of is noted. The devices which are embedded in the sensors have a well protected key for access which can be generated by a Fibonacci generator which is designed in the sensors. The Fibonacci generator is written using java programming, the Fibonacci generator has many flip flops, adders, multipliers and clock enable.

C:\Users\Shiv Sagar\Downloads\fibono.png

Figure 11: Fibonacci Generator [6]

As we can see the figure 10, the Fibonacci generator has internally 31 pins with four other pins such as CLK, CE, enable, reset and Output pin. All electronic devices to work efficiently, a operating range of temperature called the junction temperature should be minimum, different devices have different junction temperature based on their frequency. The maximum value of junction temperature a device can attain is beyond which the device will be damaged, so make sure the junction temperature does not attain maximum value the sensors are embed with coolants that devices safe from external temperature and internal temperature [6].

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Frequency | Temp | C | C | C | C |
| 0.5Ghz | | C | C | C | C |
| 10.5Ghz | | C | C | C | C |
| 105Ghz | | C | C | C | C |
| 0.5THz | | C | C | C | C |

Table 1: Various Junction temperatures for LVCMOS10 [6]

From the table 1 it can be seen that as frequency increases the junction temperature also increase for LVCMOS10 due to factors such as Noise, Leakage current, Reliability. The junction temperature might vary for different LVCMOS circuits, table 2 and table 3 shows different values of junction temperature [6].

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Frequency | Temp | C | C | C | C |
| 0.5Ghz | | C | C | C | C |
| 10.5Ghz | | C | C | C | C |
| 105Ghz | | C | C | C | C |
| 0.5THz | | C | C | C | C |

Table 2: Various Junction temperature for LVCMOS20 [6]

In the table 2 the frequency range for LVCMOS20 is from 0.5GHz to 0.5THz and the temperature increases from C to C. When LVCMOS20 is compared with LVCMOS10, there is gradual increase in temperature with respect to frequency increase.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| FREQ | Temp | C | C | C | C |
| 0.5Ghz | | C | C | C | C |
| 10.5Ghz | | C | C | C | C |
| 105Ghz | | C | C | C | C |
| 0.5Thz | | C | C | C | C |

Table 3: Various Junction Temperatures for LVCMOS26 [6]

Table 3 explains about the junction temperature of LVCMOS26, as it can be seen that as there increase in frequency with respect to the temperature there is also increase in the ambient temperature. The content of table1, 2 and 3 of different LVCMOS is compared to check the efficiency and the performance at particular ambient temperature, in the above case C is considered [6].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Freq | LVCMOS | LVCMOS10 | LVCMOS20 | LVCMOS26 |
| 0.5Ghz | | C | C | C |
| 10.5Ghz | | C | C | C |
| 105Ghz | | C | C | C |
| 0.5Thz | | C | C | C |

Table 4: Analysis of Reduction of Junction temperature [6]

From table 4 it can be seen that for LVCMOS20 there is more reduction of junction temperature when compared with LVCMOS10 and LVCMOS26. The junction temperature LVCMOS20 is reduced due to reliability of the sensor and polarity between the NMOS and CMOS circuit. As result of noise gain increase which makes the circuit less reliable when compared with LVCMOS10 and LVCMOS26 [6]. The noise gain can be reduced by increasing the frequency and as noise margin is inversely proportion to the ambient temperature, the gain might be decreased which makes the increase in drain current in the inverter circuit. If the drain current in the sensor is increased the gate voltage and source voltage will gradually decrease making the frequency to operate in the range 0.5GHz to 105GHz.

The gate diffusion capacitances present in the sensor which mainly depend on minimum length of the transistor whose capacitance have non linear voltage dependence [6]. The nMOS and pMOS transistor have twice capacitance and resistance which makes the sensor to draw lot holes compared to electrons which make these circuit more prone noise. So to avoid these problems the circuit is embedded with equivalent RC circuit model which will cancel the noise and power consumption effect making the circuit more reliable [11].

The Fibonacci generator which is used in the sensors to generate the keys for the 64 bit IP which would be attached to the devices which are made micro making sure that these sensors will work more efficiently, the Fibonacci generator which could also be designed for 32 bit IP may not work as efficiently as 64 bit due the components present in the 32 bit is less and power consumption is also less, from the example of LVCMOS we could see that it more similar to the 64 bit having C as ambient temperature. From the table 4, the LVCMOS26 can be connected to the sensors but as junction temperature is more it makes the inverter with less gate voltage, which makes current to increase linearly and reach the saturation point where the PMOS transistor is ON and NMOS transistor is OFF [6]. The pMOS transistor in the circuit provide less current and more dynamic voltage when compared to pMOS as result of which the performance and efficiency is slower.

The depletion region of pMOS is also a prime factor which makes the electrons and holes to act as insulator making the sensor a small capacitor which can store a very little charge. The diffusion capacitance present in the pMOS can change the resistance to a large value which makes the source and drain to overlap each other which makes the threshold voltage greater in the sensor which causes two effects mobility degradation and bandwidth saturation, if the mobility degradation is increased the oxide thickness increases making the sensor size more with electron count and less with hole count which makes it more static and giving a better performance and more reliable. Even though there is more leakage current which makes the transistor OFF, the current will automatically becomes zero which can also be termed as sub-threshold leakage. So the sub-threshold leakage can be stopped by building deep junctions through various fabrication process, one among them are the chemical vapor deposition which is splattered on the sensor forming different densities of impurities present on top of the sensor [6].

**CHAPTER 4**

**FEW INTERNETS OF THINGS APPLICATIONS- SMART GRID AND WEARABLE’S**

There are many ways to send information and establish connectivity, but the most efficient and best productivity way is through smart grid. Managing the devices through new ways through internet of things for the consumers, manufacturers will help to conserve the resources by which a lot of money can be saved by using these smart houses which have smart meters, smart plugs and connected appliances [8]. By 2020 it is estimated to have more than 50 billion devices connected through internet of things, devices across every industry will connected to internet making them smart grid system. Smart houses can operate though smart grid where all the application present in the home under Zigbee, PLC and z-wave. Each of this appliance present and also the device will have unique IP address, so as the number of appliances increase there need to be grid which can have this large number of IP address stored, as result of which smart grid was introduced [8].

So this IP address which are stored in the smart grid, where the IPV4 is increasing from 32 bits to 128 bits size which can address up to devices and IPV6 has more than IPV4 which can address up to . But there would a problem with this addressing scheme where the 6LOWPAN communication protocol would block the IPV6 addressing because the frame size of IPV6 is limited and it can include only 31 bytes for the UDP and 21 for TCP [9]. The only solution to this is that to model the smart grid within internet of things context where the smart home appliances, renewable energy resources and design tools. Modeling of the devices can be done in 6 ways

1. **Smart home appliances**

All the devices such as refrigerator, Micro oven, automated light and electric rechargeable vehicle which can be considered as an object, so these objects have unique IP address which could be accessed through internet by only who has a permit and the data will transmitted through phone which could be easily monitored and controlled by the user.

1. **Distributed renewable energy resources**

These distributed renewable energy resources are smart grid which enables to use the external power sources which can be used during emergencies and also it can be used during night times when there would be power surge which could be installed quickly and the operation of the renewable energy resources is easily available [9].

1. **Mobile workforce tool and devices**

To maintain the smart grid to work efficiently some tools and devices are used which can be utilized as mobile workforce that can monitor and debug those issues regarding meters, power outrages, transformers and feeders. The operators who work on these tools and devices are usually given laptop, smart phone and meter.

1. **Utility data and control center infrastructure**

So the each of the operator who work on smart grid are given unique IP address and these address should be stored database, there are many database services such as distribution management system, outage management system and customer information system [9].

1. **Substation devices**

In substation there are many devices such as breakers, switches, meters, capacitor banks etc and these devices have unique IP address where each of them are connected through internet and be controlled by phone or desktop and these devices and operated remotely from other places, and each device can send the device status and receive command from external source which occupy very less memory [9].

The smart house can be having other external features which will be able to have high level of communication through web services. Many of the internal features which are based on the product based service interaction are part of complex system. These smart houses will have a common gateway which tries to run on very small resource constrained which makes the device to have its own IP address which could be verified by a 32 bit memory bus.

C:\Users\Shiv Sagar\Downloads\smart house.png

Figure 12: Smart house and its external entities [11]

There are number different protocols which are embedded in the hardware and also in other protocol layers which might even increase in near future. As the number of IP’s goes on increasing, the information present such as the IP header, IP infrastructure and P2P interaction can be saved in the smart house application. From the figure 11 it can be seen that smart house is in collaboration with SAO, Data evaluation, Discovery, Time monitoring and Management [11]. The data evaluation present in the smart grid is very useful as it can be used to monitor the data present in application layer, the development of the middleware for the devices for good connectivity is a must approach and theses devices offer standard interface with very little connectivity and the devices can be used to enhance their own functionality by invoking the services which are we’re not been introduced at time of device design [11]. As the consumption of electricity increases the money rewarded where the business opportunity can be exploited if the price would be decreased which could lead to kick starting facilities which could consume or store energy and can benefit from a negative price and also change the customer monetarily.

Energy efficiency can be improved and maintained by introducing dynamic energy product labels, where the smart houses objects such as refrigerator, micro oven, air conditioner and smart meters which provide static energy information which is not much useful because it does not consider main energy consumption, the problem of measuring energy during the discrete production steps or if any logistics operation is happening and also sometimes during transportation [11]. The way dynamic energy product labeling works, for example a vehicle which travels a particular distance which consumes lot energy and fuel but to calculate the total energy the static energy product labels is not an efficient way, so the dynamic energy product label will give customers a good efficient way and a good indication of the device.

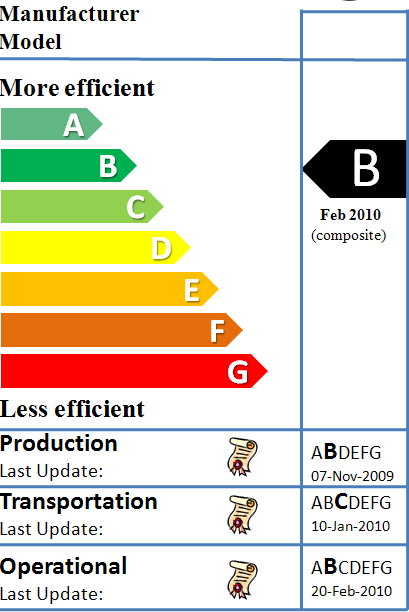


Figure 13: Dynamic Energy label [11]

From the figure 13 it can be seen that for different energy consumption and energy efficiency for a single device where the software monitors in different section in which the highest efficient is A and a very less efficient is G, and also it can be seen that for different scenarios such as Production, Transportation and operational the different dynamic energy model can be seen [11].

**Wearable Devices**

Wearable device are major devices oriented growth using Internet of things technology, where the users wear these devices which monitors their body vitals and sends information or notification to app or in case of any emergency it is sent to a doctor. All the data that is got is sent to the right database and sometimes the data is sent through icloud. Usually smart phone are taken as primary devices have their wearable devices embedded with micro sensors which have a proxy API that can provide developers to test the system without exploding for as it gives with very low kits. Many companies such as Google, Samsung and Apple are trying to come up with innovative ideas for the wearable devices, all the companies have their own API which is installed in the device [11].



Figure 14: Wearable devices [6]

In Figure 14 show an image of wearable devices which many companies are in mass production which works when devices are placed to the body which can detect and monitor pulse, temperatures and other variation in the body [11]. These devices can capture the information and will be able to send to our personal devices such as mobile and pager. The data that these wearable devices send would be stored based on cloud based software in which a large percentage data which depends on SQL database such as Cassendra, Hadoop and other database frameworks.

The first smart watch was Pebble which was into mass production which has RTOS kernel as operating system which has got many updates and the display of the apps in smart watch were not as complicated which when paired to smart phone or tablet [12]. As there was progress in pebble, it introduced for UNIX based operating system, following this Google started to develop wearable’s with android wear platform and android 5.0 lollipop which is now a open source, now other companies too have started with wearable devices such Sony, LG and Asus.

In nearby future many companies are planning for smart clothing and eyewear, companies such as Nanosonic has developed a prototype which can measure person’s temperature and socks can provide impact measurement, the main advantage of smart clothing is that all the data from different part of body can provide data of each person where a lot of embedded sensors are placed and it can be used for heart patient to monitor if there is a problem with any heart related issues [12]. Some of the keys points to remember is that security and privacy of maintaining the user’s data, so many companies are making the wearable devices with fingerprint enabled which a very good approach towards security as a finger print which is very unique for each person which makes the security much better than other approach. As the years goes the developers makes changes to these devices which eventually becomes a basic necessity tool for everyone. The wearable devices have low power MCU intel i7 processor embedded which makes the devices faster and also the connectivity, and also there is huge reduction of power which makes them more stable and charging time for these devices will be very less and the activity tracking where a core sensor such as an accelerometer that is placed can monitor any movements [12].

**Conclusion**

From house hold application to VLSI industry, almost day to day products, use internet of things. There is steep incline from 2015 where all the wearable devices use internet of things as well the smart grid where the objects are communicated also know as machine to machine communication. There was also great demand for the machine to machine communication in recent years, where telsa developed a car model which introduced a new concept based on machine to machine communication which made a huge success in automobile industry, and few other companies such as Google, Samsung, Apple and Intel are planning to implement this new concept. The architecture of internet of things was complicated, as it was implemented only for 32 bit but not for 64 bit processor, as result of which the different protocols where changed and internet of things communication model which has few components such as communication functional group, domain model and deployment view. After the reference architecture design is completed with addition of few minor changes the efficiency and space constraint was improved as result of which the design architecture has more headers than the reference architecture.

In VLSI domain which follows the moore’s law where the number of transistors doubles approximately every two years, the transistor count can be reduced by internet of things where the one core chip communicates with other making it more faster and efficient, energy consumption, noise margin and few others can be improved. The nano bio sensors which are of very small components present in the circuit board, these sensors are build in with internet of things where each sensor communicates with each. These sensors when embedded in the hardware make the nano particles much faster. From the Fibonacci generator we could see the generation of different key’s which is used for different LVCMOS circuits, as these LVCMOS circuits less dynamic voltage making them more sustainable to power consumption and more efficient than other circuits. The smart home appliances can be connected with each other making bigger network, as result in case of emergencies in these equipments can be communicated to the users and make sure they are working, as result of which work force is faster and debugging becomes easier.

This paper has presented has the basic ideas how internet of things works, architecture of sensor system, RFID and few application of internet of things such as smart grid and wearable’s. The main advantages of internet of things are highlighted in this paper and machine to machine communication which is different sensor nodes has the capability of connecting to network forming a bigger network as result of which makes the network bigger and makes it faster. The different nodes that are present in the architecture can be manipulated by adding few extra nodes. This paper also speak about the embedding internet of things in field of VLSI sensors which makes the sensor make efficient and smaller following the moore’s law.

This paper has therefore represented different methodologies of Internet of things and its application which make the network performance faster and a basic understanding of machine to machine communication and working of RFID.

**REFERENCES**

[1] Jayavardhana gubbi, Rajkumar Buyya, Slaven Marusic & Marimuthu Palaniswami (2013): “Internet of things (lOT): A vision, architectural elements and future directions”, Future Generation Computer system, 2013

[2]Ovidiu Vermesan, Peter Friess: “Internet of things-From Research and Innovation to market deployment”

[3]Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stamatis Karnouskos, Stefan Avesand and David Boyle: “From Machine-to-Machine to the Internet of things, Introduction to New Age of Intelligence”

[4]Frederic Thiesse, Florian Michahelles:” Building the Internet of things using RFID, The RFID ecosystem experience”, University of Washington, 2009 IEEE

[5]Dhananjay Singh, Gaurav Tripathi and Antonio J.Jara: “A survey of internet of things: Future Vision, Architecture, Challenges and services”, 2014 IEEE World forum on Internet of things

[6]Tanesh Kumar, S.H.A Musavi, Munsif Ali Jatoi, S.H.A Musavi, Karandeep Kaur: “Internet of things enabled green VLSI design on FPGA” Computing for Sustainable global development, 2015 2nd International Conference

[7]Lu Yan, Yan Zhang, Laurence T.Yang, Huansheng Ning: “From RFID to next-generation pervasive networked system” Conference organized by DG Information Society and media, March 2006

[8]Micheal Goshey: “RFID Convergence- the Internet of things 2.0 “, Department of Computer Science and Engineering, University of Minnesota

[9]Gerald Santucci., Sebastian Lange: “Internet of things in 2020- A roadmap for the future” RFID Working Group of the European Technology Platform on Smart System Integration (EPoSS), 05 Septemeber 2008

[10] A.R Al-Ali., RaafatAburukba. “Role of internet of things in the smart grid technology” Journal of Computer and communication, 2015, 3, 299-233

[11]Stamatis Karnouskos.,”The cooperative Internet of things enabled smart grid”, SAP Research

[12] Karen Rose, Scott Eldridge and Lyman Chapin., “The internet of things: An Overview”, 2015 Internet Society, October 2015