

*SEMINAR REPORT ON*

***Internet of Things (IoT): Security Challenges,***

***Business Opportunities &Multilayered Method***

***For End to End Data Communications***

*SUBMITTED TO:*

**Department of Computer Science & Engineering**

*by*

Vishal Vimal Kumar

Registration No:160905071

Roll Number:21

Semester and Section:7C

Name & Signature of Evaluator 1 Name & Signature of Evaluator 2 (Aug 2019)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Table of Contents** | | | | |
|  | | | | Page No |
| **Chapter 1** | | | **INTRODUCTION** |  |
|  | **1.1** | Internet of Things (IoT) | | 3 |
|  | **1.2** | Applications of IOT | | 4 |
|  | | | | |
| **Chapter 2** | | | BACKGROUND THEORY and/or LITERATURE REVIEW |  |
|  | **2.1** | Security Challenges for IOT | | 8 |
|  | **2.2** | IOT business opportunities | | 9 |
|  | **2.3** | Multilayered Method for End to End Data Communications | | 13 |
|  | | | | |
| **Chapter 3** | | | **METHODOLOGY** |  |
|  | **3.1** | Objective | | 15 |
|  | **3.2** | Approach | | 15 |
|  | | | | |
| **Chapter 4** | | | **RESULTS AND DISCUSSION** |  |
|  | **4.1** | Dematerialization | | 17 |
|  | **4.2** | Road Ahead | | 17 |
|  | **4.3** | Business imperative | | 17 |
|  | | | | |
| **Chapter 5** | | | **CONCLUSIONS AND FUTURE ENHANCEMENTS** | 18 |
|  | | | | |
| **REFERENCES** | | | | 19 |
| **PLAGIARISM REPORT** | | | | 20 |

**INTRODUCTION**

**1.1** Internet of Things (IoT)

The Internet of things (IoT) is the extension of [Internet](https://en.wikipedia.org/wiki/Internet) connectivity into physical devices and everyday objects. Embedded with [electronics](https://en.wikipedia.org/wiki/Electronics), [Internet connectivity](https://en.wikipedia.org/wiki/Internet_access), and other forms of hardware (such as [sensors](https://en.wikipedia.org/wiki/Sensor)), these devices can communicate and interact with others over the Internet, and they can be remotely monitored and controlled. The definition of the Internet of things has evolved due to the convergence of multiple technologies, real-time [analytics](https://en.wikipedia.org/wiki/Analytics), [machine learning](https://en.wikipedia.org/wiki/Machine_learning), commodity sensors, and [embedded systems](https://en.wikipedia.org/wiki/Embedded_system). Traditional fields of embedded systems, [wireless sensor networks](https://en.wikipedia.org/wiki/Wireless_sensor_network), [control systems](https://en.wikipedia.org/wiki/Control_system), [automation](https://en.wikipedia.org/wiki/Automation) (including [home](https://en.wikipedia.org/wiki/Home_automation) and [building automation](https://en.wikipedia.org/wiki/Building_automation)), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as [smartphones](https://en.wikipedia.org/wiki/Smartphone) and [smart speakers](https://en.wikipedia.org/wiki/Smart_speaker).

The IoT concept has faced prominent criticism, especially in regards to [privacy](https://en.wikipedia.org/wiki/Digital_privacy) and [security](https://en.wikipedia.org/wiki/Digital_security) concerns related to these devices and their intention of pervasive presence.

**1.2** Applications

### Consumer applications

A growing portion of IoT devices are created for consumer use, including connected vehicles, [home automation](https://en.wikipedia.org/wiki/Home_automation), [wearable technology](https://en.wikipedia.org/wiki/Wearable_technology) (as part of Internet of Wearable Things (IoWT)[]](https://en.wikipedia.org/wiki/Internet_of_things#cite_note-25)), connected health, and appliances with remote monitoring capabilities.

[](https://en.wikipedia.org/wiki/File:Nest_Learning_Thermostat_(cropped).JPG)

A [Nest](https://en.wikipedia.org/wiki/Nest_Labs) learning thermostat reporting on energy usage and local weather.

#### Smart home

IoT devices are a part of the larger concept of home automation, which can include lighting, heating and air conditioning, media and security systems. Long-term benefits could include energy savings by automatically ensuring lights and electronics are turned off.

A smart home or automated home could be based on a platform or hubs that control smart devices and appliances. For instance, using [Apple](https://en.wikipedia.org/wiki/Apple_Inc.)'s [HomeKit](https://en.wikipedia.org/wiki/HomeKit" \o "HomeKit), manufacturers can have their home products and accessories controlled by an application in [iOS](https://en.wikipedia.org/wiki/IOS) devices such as the [iPhone](https://en.wikipedia.org/wiki/IPhone) and the [Apple Watch](https://en.wikipedia.org/wiki/Apple_Watch). This could be a dedicated app or iOS native applications such as [Siri](https://en.wikipedia.org/wiki/Siri). This can be demonstrated in the case of Lenovo's Smart Home Essentials, which is a line of smart home devices that are controlled through Apple's Home app or Siri without the need for a Wi-Fi bridge. There are also dedicated smart home hubs that are offered as standalone platforms to connect different smart home products and these include the [Amazon Echo](https://en.wikipedia.org/wiki/Amazon_Echo), [Google Home](https://en.wikipedia.org/wiki/Google_Home), Apple's [HomePod](https://en.wikipedia.org/wiki/HomePod" \o "HomePod), and Samsung's [SmartThings Hub](https://en.wikipedia.org/wiki/SmartThings). In addition to the commercial systems, there are many non-proprietary, open source ecosystems; including Home Assistant, OpenHAB and Domoticz.

[](https://en.wikipedia.org/wiki/File:Ring_video_doorbell.jpg)

A [Ring](https://en.wikipedia.org/wiki/Ring_(company)) doorbell connected to the Internet

#### Elder care

One key application of a smart home is to provide [assistance for those with disabilities and elderly individuals](https://en.wikipedia.org/wiki/Home_automation_for_the_elderly_and_disabled). These home systems use assistive technology to accommodate an owner's specific disabilities. [Voice control](https://en.wikipedia.org/wiki/Voice_Control) can assist users with sight and mobility limitations while alert systems can be connected directly to [cochlear implants](https://en.wikipedia.org/wiki/Cochlear_implant) worn by hearing-impaired users. They can also be equipped with additional safety features. These features can include sensors that monitor for medical emergencies such as falls or seizures. Smart home technology applied in this way can provide users with more freedom and a higher quality of life.

The term "Enterprise IoT" refers to devices used in business and corporate settings. By 2019, it is estimated that the EIoT will account for 9.1 billion devices.

#### Transportation

[](https://en.wikipedia.org/wiki/File:Variable_speed_limit_digital_speed_limit_sign.jpeg)

Digital variable speed-limit sign.

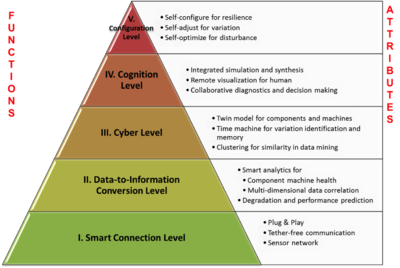
The IoT can assist in the integration of communications, control, and information processing across various [transportation systems](https://en.wikipedia.org/wiki/Intelligent_transportation_system). Application of the IoT extends to all aspects of transportation systems (i.e. the vehicle, the infrastructure, and the driver or user). Dynamic interaction between these components of a transport system enables inter- and intra-vehicular communication, smart, smart parking, [electronic toll collection systems](https://en.wikipedia.org/wiki/Electronic_toll_collection), [logistic](https://en.wikipedia.org/wiki/Logistics_management)s and [fleet management](https://en.wikipedia.org/wiki/Fleet_management), [vehicle control](https://en.wikipedia.org/wiki/Autonomous_cruise_control_system), safety, and road assistance. In Logistics and Fleet Management, for example, an IoT platform can continuously monitor the location and conditions of cargo and assets via wireless sensors and send specific alerts when management exceptions occur (delays, damages, thefts, etc.). This can only be possible with the IoT and its seamless connectivity among devices. Sensors such as GPS, Humidity, and Temperature send data to the IoT platform and then the data is analysed and then sent to the users. This way, users can track the real-time status of vehicles and can make appropriate decisions. If combined with [Machine Learning](https://en.wikipedia.org/wiki/Machine_learning), then it also helps in reducing traffic accidents by introducing [drowsiness](https://en.wikipedia.org/wiki/Driver_drowsiness_detection) alerts to drivers and providing self-driven cars too.

### Industrial applications: Manufacturing

The IoT can realize the seamless integration of various manufacturing devices equipped with sensing, identification, processing, communication, actuation, and networking capabilities. Based on such a highly integrated smart cyberphysical space, it opens the door to create whole new business and market opportunities for manufacturing. Network control and management of [manufacturing equipment](https://en.wikipedia.org/wiki/Reconfigurable_Manufacturing_System), [asset](https://en.wikipedia.org/wiki/Asset_management) and situation management, or manufacturing [process control](https://en.wikipedia.org/wiki/Process_control) bring the IoT within the realm of industrial applications and smart manufacturing as well. The IoT intelligent systems enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and [supply chain networks](https://en.wikipedia.org/wiki/Supply_chain_network), by networking machinery, sensors and control systems together.

[Digital control systems](https://en.wikipedia.org/wiki/Digital_control) to automate process controls, operator tools and service information systems to optimize plant safety and security are within the purview of the IoT. But it also extends itself to asset management via [predictive maintenance](https://en.wikipedia.org/wiki/Predictive_maintenance), [statistical evaluation](https://en.wikipedia.org/wiki/Statistical_model), and measurements to maximize reliability. Industrial management systems can also be integrated with [smart grids](https://en.wikipedia.org/wiki/Smart_grid), enabling real-time energy optimization. Measurements, automated controls, plant optimization, health and safety management, and other functions are provided by a large number of networked sensors.

Industrial IoT (IIoT) in manufacturing could generate so much business value that it will eventually lead to the [Fourth Industrial Revolution](https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution), also referred to as [Industry 4.0](https://en.wikipedia.org/wiki/Industry_4.0). The potential for growth from implementing IIoT may generate $12 trillion of global GDP by 2030.

[](https://en.wikipedia.org/wiki/File:CPS_for_Manufacturing.png)

Design architecture of cyber-physical systems-enabled manufacturing system

[Industrial big data](https://en.wikipedia.org/wiki/Industrial_big_data) analytics will play a vital role in manufacturing asset predictive maintenance, although that is not the only capability of industrial big data.[Cyber-physical systems](https://en.wikipedia.org/wiki/Cyber-physical_system) (CPS) is the core technology of industrial big data and it will be an interface between human and the cyber world. Cyber-physical systems can be designed by following the 5C (connection, conversion, cyber, cognition, configuration) architecture, and it will transform the collected data into actionable information, and eventually interfere with the physical assets to optimize processes.

An IoT-enabled intelligent system of such cases was proposed in 2001 and later demonstrated in 2014 by the [National Science Foundation](https://en.wikipedia.org/wiki/National_Science_Foundation) Industry/University Collaborative Research Center for [Intelligent Maintenance Systems](https://en.wikipedia.org/wiki/Intelligent_maintenance_system) (IMS) at the University of Cincinnati on a [bandsaw](https://en.wikipedia.org/wiki/Bandsaw) machine in IMTS 2014 in Chicago. Bandsaw machines are not necessarily expensive, but the bandsaw belt expenses are enormous since they degrade much faster. However, without sensing and intelligent analytics, it can be only determined by experience when the band saw belt will actually break. The developed [prognostics](https://en.wikipedia.org/wiki/Prognostics) system will be able to recognize and [monitor the degradation](https://en.wikipedia.org/wiki/Intelligent_maintenance_system) of band saw belts even if the condition is changing, advising users when is the best time to replace the belt. This will significantly improve user experience and operator safety and ultimately save on costs.

**BACKGROUND THEORY**

2.1 Security challenges for IOT

The IoT market size in Europe is estimated to reach €242,222 million by the end of 2020. This rise in popularity of IoT-connected devices leading to rise in [IoT app development](https://www.peerbits.com/internet-of-things-iot-applications-development-company.html) does come with its fair share of concerns and security challenges.

## 1. Insufficient testing and updating

Currently, there are over 23 billion IoT connected devices worldwide. This number will further rise up to reach 30 billion by 2020 and [over 60 billion](https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/) by the end of 2025. This massive wave of new gadgets doesn’t come without a cost. In fact, one of the main problems with tech companies building these devices is that they are too careless when it comes to handling of device-related security risks. Most of these devices and IoT products don’t get enough updates while, some don’t get updates at all. This means that a device that was once thought of as secure when the customers first bought it becomes insecure and eventually prone to hackers and other security issues. Early computer systems had this same problem, which was somewhat solved with automatic updates. IoT manufacturers, however, are more eager to produce and deliver their devices as fast as they can, without giving security too much of a thought. Unfortunately, most manufacturers offer firmware updates only for a short period of time, only to stop the moment they start working on the next headline-grabbing gadget. Even worse, they use unsupported legacy Linux kernels. This leaves their trusted customers exposed to potential attacks as a result of outdated hardware and [software](https://www.peerbits.com/software-development-company.html). To protect their customers against such attacks, each device needs proper testing before being launched into the public and companies need to update them regularly. Failing to do so is bad for both the companies and their consumers, as it only takes a single large-scale breach in consumer data to completely ruin the company.

2. IoT malware and ransomware

As the number of IoT connected devices continues to rise in the following years, so will the number of malware and ransomware used to exploit them. While the traditional ransomware relies on encryption to completely lock out users out of different devices and platforms, there’s an ongoing hybridization of both malware and ransomware strains that aims to merge the different types of attack.The ransomware attacks could potentially focus on limiting and/or disabling device functionality and stealing [user data](https://www.peerbits.com/blog/blockchain-iot-development-can-secure-data.html) at the same time.For example, a simple IP camera is ideal for capturing sensitive information using a wide range of locations, including your home, work office or even the local gas station. The webcam can then be locked and footage funneled to an infected web address which could extract sensitive data using the malware access point and demand ransom to unlock the device and return the data. The ever-increasing number of IoT devices will give birth to unpredictability in regards to future attack permutations.

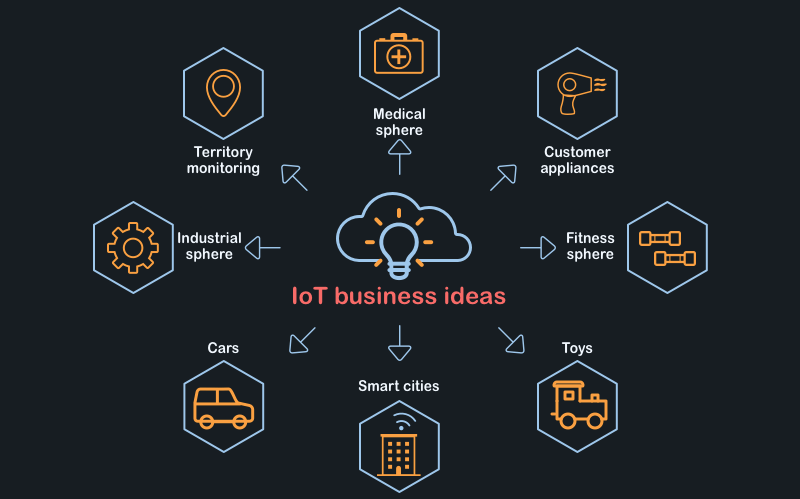
3. Data security and privacy concerns (mobile, web, cloud)

Data privacy and security continues to be the single largest issues in today’s interconnected world. Data is constantly being harnessed, transmitted, stored and processed by large companies using a wide array of IoT devices, such as smart TVs, speakers and lighting systems, connected printers, HVAC systems, and smart thermostats. Commonly, all this user-data is shared between or even sold to various companies, violating our rights for privacy and data security and further driving public distrust. We need to set dedicated compliance and privacy rules that redact and anonymize sensitive data before storing and disassociating IoT data payloads from information that can be used to personally identify us. Cached and no longer needed data should then be disposed of securely.

If the data is stored, then the largest challenge is in compliance with various legal and regulatory structures. The same practice should be employed with mobile; web and cloud applications and services used to access, manage and process data associated with IoT devices. [Secure development of mobile app](https://www.peerbits.com/blog/build-secure-mobile-apps.html) and web-based IoT applications can be quite difficult for small companies with limited budgets and manpower. As we already mentioned, most manufacturers tend to focus solely on getting the app and device on the market fast to attract even more funding and start growing their user base. Unless you want to risk a major breach of security and ruin your brand authority and trustworthiness, then you might want to consider going through a directory of mobile and [web development companies](https://www.designrush.com/agency/website-design-development) and find the best one to help you iron out the kinks that come with multi-layered data management and its security.

## 2.2 IOT business opportunities

There are so many IoT business ideas which you can use to build your business or a startup with that it would probably need a book to be written to describe all of them. That's why we choose 5 of the most promising and innovative Internet of things business opportunities. Here they are:



### 1. Medical and fitness spheres

Fitness wearables are not new to us and it seems that they are connected to the Internet as they communicate with our smartphones. But IoT goes further. A fit bracelet connected with the IoT system can do much more. The easiest and the most obvious ability of such devices is to pass data about your heartbeat to a medical establishment or to a doctor in an emergency occasion. But let's think outside of the box. How about a device that passes information about your training to your smartphone which calculates the nutrition you need to eat now and synchronizes it with your smart fridge which sends information about the products available. For instance, such an app can offer recipes based on the intensity of your training and many other things.

The medical sphere is even wider. Hospitals are nice places to be improved. I am sure I'm not the only person on this planet who hates hospitals and when I get there I have only a strong desire to leave the place as fast as I can. If we add IoT technologies here along with modern devices we can reduce the average time a person spends on a visit dramatically, starting with making an appointment (the task can be easily performed by your smartphone even without your supervision) to leaving a hospital.

### 2. Industrial internet of things

If you don't have an idea for your business here's a tip for you - think about a common problem in a workplace and try to think of its solution with the help of IoT technologies. In such a case your business idea would be easily sold. For instance, a problem which we've already mentioned - breakage detection. As well as that, various sensors which help collect environmental metrics to optimize workflow.

### 3. Smart cities

This is a vast sphere where you can easily implement everything that you like. The best part is that the niche is almost empty so you have every chance to become a pioneer.   
Solar roads: They are reusable and removable panels made of cheap materials. The panels use solar energy and have lots of advantages. For instance, they can warn drivers about obstacles and animals on the road. They have led lights that improve the visibility, can be used as a carriageway marking and help control traffic. Here is a short video about them.

Traffic controllers: Various sensors could be used to predict dangerous situations on the road. They can track the number of cars and redirect upcoming vehicles to different roads.

Smart bus stops: They can not only show the information about traffic but also be interactive, turn heating\air conditioning on and off when there are people on the bus stop and when it's empty.

They are just some of the examples because every device and aspect of city life can be modernized and improved with the help of IoT technologies. Smart shops, smart traffic lights, railway-crossing, and even sensors that listen to the sounds in the city and classify them according to the volume of sound. Such sensors can be taught to define gunshots and pass data to the nearest police department.

### 4.Cars

We can assume that cars have already become smart. The fact that soon we are going to be driven by self-driving cars is a fact not a fiction. So don't lose your chance to make your contribution to the future.

Nowadays the biggest and the most urgent problem of all car owners is security. Security when a driver is in a car and when he or she isn't. Multiple built-in sensors can easily identify a driver defining such parameters as weight, height and arm length. If these parameters don't match the IoT car locks itself immediately. As well as that, sensors can also improve security on the road, when a driver is in a car. Simple distance measurements between cars can save lots of lives.

### 5. Territory IoT monitoring

In farming, IoT devices can do lots of tasks. They can measure the soil humidity and control the water supply. They can control how ripe fruit and vegetable are and inform the farmer about harvesting time and so on. Smart approaches reduce costs and advances forecasts, planning and harvesting processes.

Infrared cameras and air filters can save our forests in summer time. These appliances are commonly used in countries where this problem is not an empty phrase. If we combine and improve weather forecast systems with these sensors we can do the same.

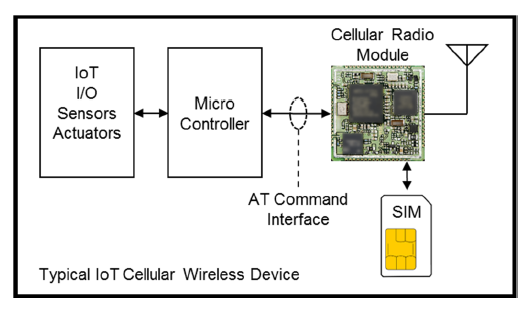
2.3 Multilayered Method for End to End Data Communications

SIM-BASED AUTHENTICATION AND KEY AGREEMENT

The first critical element of the secure architecture is the subscriber identifier module (SIM). The SIM’s basic function is to protect authentication keys from being compromised. The SIM consists of a microprocessor that incorporates a number of hardware protection technologies to prevent compromise through chemical decomposition, x-ray or any number of attempts to reverse engineer. Additionally, protection procedures are applied to the I/O pins of the SIM to

prevent forced external anomalies from rendering the SIM vulnerable to compromise. For instance, inducing a higher or lower voltage on the TX and RX pins in reference to the supply and ground in an effort to cause the I/O circuitry to latch up or go into an unintended state is monitored by the SIM I/O

circuitry and will disable the SIM if these conditions exist. The SIM is also protected against anomalous clocking and input data.



As shown in Fig. 2, the connectivity to the SIM is only through the cellular radio module preventing the onboard microprocessor from directly accessing the SIM. Any communications with the SIM are performed solely by the radio stack layer built into the radio module. When a cellular device, in this case an Internet of Things device, is powered up the radio is automatically programed to scan the available radio band and catalog possible cell carriers

that it may be able to attach to 1. This process is set to prefer a carrier tower that first matches its own carrier’s mobile network code (MNC). This is accomplished by searching the radio bands looking for broadcast codes that match the SIM’s International Mobile Subscriber identity (IMSI) code. If a

matching carrier is not located, namely the SIM home carrier, the radio scans for other serving carriers and compare them to an updatable list of preferred roaming partners.

**METHODOLOGY**

3.1 Objective

The Internet of Things (IoT) represents a diverse technology and usage with unprecedented business opportunities and risks. The Internet of Things is changing the dynamics of security industry & reshaping it. It allows data to be transferred seamlessly among physical devices to the Internet. The growth of number of intelligent devices will create a network rich with information that allows supply chains to assemble and communicate in new ways. The technology research firm Gartner predicts that there will be 26 billion installed units on the Internet of Things (IoT) by 2020.

This project explains the concept of Internet of Things (IoT), its characteristics, explain security challenges, technology adoption trends and multi-layered method for securing data transport from a cellular connected Internet of Things device to a host through a cellular network.

3.2 Approach

The aim of IoT is to make our day to day life safer & more efficient. More IoT devices means increased efficiency & more interconnected world. Some of the approaches of IoT as discussed below:

1. Smarter Analytics

More number of inter-connected devices means more data and applying analytics on all aspects of the business will provide an opportunity to improve strategy and the customer

experience. For example, Intel IoT Platforms solutions generate actionable information by running analytics software on data for industrial, retail, automotive industries etc.

B. Enhanced Security

The smart doorbells and surveillance systems will help identify & recognize the person which will boost security.

C. Increased Productivity

IoT will facilitate optimal utilization of resource and time. For example if a printer is running low on ink, it will order more on its own & save precious time. And it will send notification if printer machine is not working properly.

D. Smart Inventory

Businesses will be able to trace goods in the supply chain with Internet-connected inventory. It will provide enhanced in-transit visibility.

E. Safer Travel

The Internet-connected cars can a better sense of real time traffic conditions and vehicle diagnostics which will make travel safer.

F. Real time demand visibility

The tightly coupled warehouse & order system provides better real time demand visibility.

**RESULTS AND DISCUSSION**

4.1 Dematerialization

We’re increasingly substituting atoms, the smallest unit of physical matter, with electrons, an element of an atom itself.  In short, humans are relying less on physical resources and instead working smarter.  Examples include better utilization of acreage and water in farming and a decline of petroleum consumption.

IoT will accelerate dematerialization by enabling us to work smarter.

## 4.2 Road ahead

Connecting heavy equipment, appliances, and even people, with sensors enables businesses to learn from what is going on in the real world.  Consider how much we as humans rely on our five senses as the basis for our learning.

The byproduct of this learning is, minimally, the ability to operate at even higher levels of efficiency or, at the other end of the spectrum, finding entirely new, disruptive business models. Online companies like Amazon and Facebook have long understood the benefits of using connected data to guide their activities – what the military refers to as “situational awareness.”

## 4.3 Business imperative

Business leaders interested in the IoT opportunity need to move quickly. Schneider explains that 38 percent of companies already have a strategy in place and are in the exploratory stage while 19 percent have deployed IoT at scale.

With all the potential value enabled by IoT, perhaps the most important guidance shared at the summit was foreshadowed by McAfee’s closing prediction: “leading firms in most industries and geographies will be very different in 20 years than they are today.”

The guidance: join leaders like Porsche, Siemens, UnderArmor and others and innovate from a position of strength.

**CONCLUSIONS AND FUTURE ENHANCEMENTS**

According to research firm International Data Corporation (IDC) the fast growth of cloud and Internet connected devices is expected to boost IoT market. The Internet of Things (IoT) market is expected to hit $7.1 trillion by 2020.

The Vision Mobile Q1 2015 Developer Economics survey data reveals that 53% of mobile developers are working on Internet of Things (IoT) projects. And global population for Internet of Things (IoT) developer's is set to top 4.5 million by 2020.

The only way to make profit in the Internet of Things (IoT) market is to create unique value on top of commodity hardware, connectivity and cloud services. The major markets within the Internet of Things (IoT) field are smart homes and wearable devices.

This project also has set forth a multi-tiered solution for securely establishing end-to-end TCP/IP based Internet of Things communications over UMTS/LTE cellular-based networks.

**REFERENCES**

[1] Gartner Says a Thirty-Fold Increase in Internet-Connected Physical

Devices by 2020 Will Significantly Alter How the Supply Chain Operates, <http://www.gartner.com/newsroom/id/2688717>

[2] IBM Connects “Internet of Things” to the Enterprise, http://www-

03.ibm.com/press/us/en/pressrelease/46453.wss

[3] IDC: 30 Billion Autonomous Devices By 2020,

https://securityledger.com/2013/10/idc-30-billion-autonomous-devicesby-

2020/

[4] Seize New Product and Revenue Opportunities with the Internet of

Things, http://www.cisco.com/web/solutions/trends/iot/portfolio.html

[5] Forecast: The Internet of Things, Worldwide,2013,

https://www.gartner.com/doc/2625419/forecast-internet-thingsworldwide-

[6] Internet of Things: Six Key Characteristics, <http://designmind.frogdesign.com/2014/08/internet-things-six-keycharacteristics/>

[7] 3GPP TS 11.113rd Generation Partnership Project; Technical Specification Group Terminals Specification of the Subscriber Identity Module - Mobile Equipment (SIM- ME) interface

[8] 3GPP TS 22.022 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Personalization of Mobile Equipment (ME); Mobile functionality specification

[9] 3GPP TS 23.122 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode

[10] 3GPP TS 33.102 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture

[11] 3GPP TS 21.111 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)

PLAGIARISM REPORT