NAME:

KELVIN OMOZOKPIA

DEPARTMENT:

COMPUTER SCIENCE

FACULTY:

PHYSICAL SCIENCES

TOPIC:

INTERNET OF THINGS (IoT): VISION,APPLICATIONS AND CHALLENGES

ABSTRACT

Internet, a revolutionary invention, is always transforming into some new kind of hardware and software making it unavoidable for anyone. The Internet of Things (IoT) is defined as a paradigm in which objects equipped with sensors, actuators, and processors communicate with each other to serve a meaningful purpose. The form of communication that we see now is either human-human or human-device, but the Internet of Things (IoT) promises a great future for the internet where the type of communication is machine-machine (M2M). This seminar aims to provide a comprehensive overview of the IoT scenario and reviews its enabling technologies and the sensor networks. Also, it describes a six-layered architecture of IoT, key features, challenges, protocols, and applications in this new emerging area.

1. INTRODUCTION

Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways. However, the journey is far from over. We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web. We are entering an era of the “Internet of Things” (abbreviated as IoT). This term has been defined by different authors in many different ways. Let us look at two of the most popular definitions.

Vermesan(2011),define the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators. Another definition by Peña-López(2005) defines the Internet of Things as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object. We use these capabilities to query the state of the object and to change its state if possible. In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network. We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.

For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers. IoT is not a single technology; rather it is an agglomeration of various technologies that work together in tandem.

Sensors and actuators are devices, which help in interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment). An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner.

The storage and processing of data can be done on the edge of the network itself or in a remote server. If any preprocessing of data is possible, then it is typically done at either the sensor or some other proximate device. The processed data is then typically sent to a remote server. The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to limitations of size, energy, power, and computational capability. As a result, the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy. Along with the challenges of data collection, and handling, there are challenges in communication as well. The communication between IoT devices is mainly wireless because they are generally installed at geographically dispersed locations. The wireless channels often have high rates of distortion and are unreliable. In this scenario reliably communicating data without too many retransmissions is an important problem and thus communication technologies are integral to the study of IoT devices.

Now, after processing the received data, some action needs to be taken on the basis of the derived inferences. The nature of actions can be diverse. We can directly modify the physical world through actuators. Or we may do something virtually. For example, we can send some information to other smart things. The process of effecting a change in the physical world is often dependent on its state at that point of time. This is called context awareness. Each action is taken keeping in consideration the context because an application can behave differently in different contexts. For example, a person may not like messages from his office to interrupt him when he is on vacation.

Sensors, actuators, compute servers, and the communication network form the core infrastructure of an IoT framework. However, there are many software aspects that need to be considered. First, we need a middleware that can be used to connect and manage all of these heterogeneous components. We need a lot of standardization to connect many different devices.

The Internet of Things finds various applications in health care, fitness, education, entertainment, social life, energy conservation, environment monitoring, home automation, and transport systems. In all these application areas, IoT technologies have significantly been able to reduce human effort and improve the quality of life.

1.1 KEY SYSTEM-LEVEL FEATURES OF INTERNET-OF-THINGS

Summarizing, we can preliminarily identify the following key system-level features that Internet-of-Things needs to support:

i. **Devices heterogeneity:**IoT will be characterized by a large heterogeneity in terms of devices taking part in the system, which are expected to present very different capabilities from the computational and communication standpoints. The management of such a high level of heterogeneity shall be supported at both architectural and protocol levels. In particular, this may question the "thin waist" approach at the basis of IP networking.

ii. **Scalability:** As everyday objects get connected to a global information infrastructure, scalability issues arise at different levels, including:

- Naming and addressing due to the sheer size of the resulting system,
- Data communication and networking due to the high level of interconnection among a large number of entities,
- Information and knowledge management due to the possibility of building a digital counterpart to any entity and/or phenomena in the physical realm and
- Service provisioning and management due to the massive number of services/service execution options that could be available and the need to handle heterogeneous resources.

iii. **Ubiquitous data exchange through proximity wireless technologies:** In IoT, a prominent role will be played by wireless communications technologies, which will enable smart objects to become networked. The ubiquitous adoption of the wireless medium for exchanging data may pose issues in terms of spectrum availability, pushing towards the adoption of cognitive/dynamic radio systems.

iv. **Energy-optimized solutions:** For a variety of IoT entities, minimizing the energy to be spent for communication/computing purposes will be a primary constraint. While techniques related to energy harvesting (by means, e.g., of piezoelectric materials or micro solar panels) will relieve devices from the constraints imposed by battery operations, energy will always be a scarce resource to be handled with care. Thereby the need to devise solutions that tend to optimize energy usage (even at the expenses of performance) will become more and more attractive.

v. **Localization and tracking capabilities:** As entities in IoT can be identified and are provided with short-range wireless communications capabilities, it becomes possible to track the location (and the movement) of smart objects in the physical realm. This is particularly important for application in logistics and product life-cycle management, which are already extensively adopting RFID technologies.

vi. **Self-organization capabilities:** The complexity and dynamics that many IoT scenarios will likely present calls for distributing intelligence in the system, making smart objects (or a subset thereof) able to autonomously

react to a wide range of different situations, in order to minimize human intervention. Following users' requests, nodes in IoT will organize themselves autonomously into transient ad hoc networks, providing the basic means for sharing data and for performing coordinated tasks. This includes ability to perform device and service discovery without requiring an external trigger, to build overlays and to adaptively tune protocols' behavior to adapt to the current context.

vii. **Semantic interoperability and data management:** IoT will be much about exchanging and analyzing massive amounts of data. In order to turn them into useful information and to ensure interoperability among different applications, it is necessary to provide data with adequate and standardized formats, models and semantic description of their content (meta-data), using welldefined languages and formats. This will enable IoT applications to support automated reasoning, a key feature for enabling the successful adoption of such a technology on a wide scale.

viii. **Embedded security and privacy-preserving mechanisms:** Due to the tight entanglement with the physical realm, IoT technology should be secure and privacy-preserving by design. This means that security should be considered a key system-level property, and be taken into account in the design of architectures and methods for IoT solutions. This is expected to represent some key requirements for ensuring acceptance by users and the wide adoption of the technology.

2. VISION AND CONCEPT OF INTERNET OF THINGS

In 2005, ITU reported about a ubiquitous networking era in which all the networks are interconnected and everything from tires to attires will be a part of this huge network (Ma, 2011). Imagine yourself doing an internet search for your watch you lost somewhere in your house. So, this is the main vision of IoT, an environment where things are able to talk and their data can be processed to perform desired tasks through machine learning (Nich, 2015). A practical implementation of IoT is demonstrated by a soon-to-be released Twine, a compact and low-power hardware working together with real-time web software to make this vision a reality. However different people and organizations have their own different visions for the IoT(De-Li *et. al.,* 2010).

An article published in Network World revealed IoT strategies of top IT vendors, they carried out some interviews from the key IT vendors. As of HP's vision, they see a world where people are always connected to their content. Cisco believes in the industrial automation and convergence of operational technology. Intel is focused on empowering billions of existing devices with intelligence. Microsoft does not consider IoT as any futuristic technology; they believe that it already exists in today's powerful devices and that the devices just need to be connected for a large amount of information which could be helpful. While, IBM has a vision of a Smarter Planet by remotely controlling the devices via secured servers. Despite of having different visions, they all agree about a network of interconnected devices therefore more developments within

the coming decades are expected to be seen including that of a new converged information society (Harald*et. al.,* 2016).

2.1 PONTENTIALS OF INTERNET OF THINGS

From a broad perspective, the confluence of several technology and market trends is making it possible for IoTto interconnect more and smaller devices cheaply and easily, the following are potentials of IoT:

i. **Ubiquitous Connectivity:**Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable".

ii. **Widespread adoption of IP–based networking:** IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.

iii. **Computing Economics:** Driven by industry investment in research, development, and manufacturing, Moore's law (2000) continues to deliver greater computing power at lower price points and lower power consumption.

iv. **Miniaturization:**Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects. Coupled with greater computing economics, this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.

v. **Advances in Data Analytics:**New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.

vi. **Rise of Cloud Computing:**Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.

3. ARCHITECTURE

More than 25 Billion things are expected to be connected by 2020 which is a huge number so the existing architecture of Internet with TCP/IP protocols, adopted in 1980, cannot handle a network as big as IoT which caused a need for a new open architecture that could address various security and Quality of Service (QoS) issues as well as it could support the existing network applications using open protocols (Jian, et. al., 2012). Without a proper privacy assurance, IoT is not likely to be adopted by many (Lan, 2005). Therefore, protection of data and privacy of users are key challenges for IoT. For further development of IoT, a number of multi-layered security architectures are proposed. (Wang, 2012) described a three key level architecture of IoT while (Hui et. al., 2012) described a four key level architecture. (Miao *et. al.,* 2010) proposed a five layered architecture using the best features of the architectures of Internet and Telecommunication management networks based on TCP/IP and TMN models respectively.

Similarly, a six-layered architecture was also proposed based on the network hierarchical structure (Xu et. al., 2012). So generally it's divided into six layers as shown in the Fig. 2. The six layers of IoT are described below:

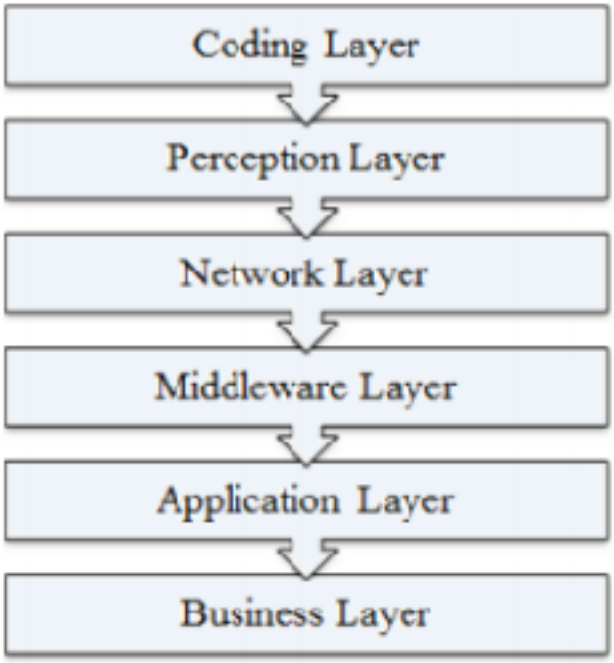

Fig. 2.1The six layers of IoT

i. **Coding Layer**: Coding layer is the foundation of IoT which provides identification to the objects of interest. In this layer, each object is assigned a unique ID which makes it easy to discern the objects (Xu*et. al.,* 2012). Fig. 2. Six-Layered Architecture of IoT

ii. **Perception Layer**: This is the device layer of IoT which gives a physical meaning to each object. It consists of data sensors in different forms like RFID tags, IR sensors or other sensor networks (Debasis and Jaydip, 2016) which could sense the temperature, humidity, speed and location etc of the objects. This layer gathers the useful information of the objects from the sensor devices linked with them and converts the information

into digital signals which is then passed onto the Network Layer for further action.

iii. **Network Layer**: The purpose of this layer is receive the useful information in the form of digital signals from the Perception Layer and transmit it to the processing systems in the Middleware Layer through the transmission mediums like WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G etc with protocols like IPv4, IPv6, MQTT, DDS etc(Ying, 2011).

iv. **Middlware Layer**: This layer processes the information received from the sensor devices (Guicheng and Bingwu, 2011). It includes the technologies like Cloud computing, Ubiquitous computing which ensures a direct access to the database to store all the necessary information in it. Using some Intelligent Processing Equipment, the information is processed and a fully automated action is taken based on the processed results of the information.

v. **Application Layer**: This layer realizes the applications of IoT for all kinds of industry, based on the processed data. Because applications promote the development of IoT so this layer is very helpful in the large scale development of IoT network (Miao *et. al.,* 2010). The IoT related applications could be smart homes, smart transportation, smart planet etc.

vi. **Business Layer**: This layer manages the applications and services of IoT and is responsible for all the research related to IoT. It generates

different business models for effective business strategies (Rafiullah*et. al.,* 2012).

3.1 TECHNOLOGIES

The development of a ubiquitous computing system where digital objects can be uniquely identified and can be able to think and interact with other objects to collect data on the basis of which automated actions are taken, requires the need for a combination of new and effective technologies which is only possible through an integration of different technologies which can make the objects to be identified and communicate with each other.

i. **Radio Frequency IDentification(RFID)**: RFID is the key technology for making the objects uniquely identifiable. It's reduced size and cost makes it integrable into any object (Wang, 2012). It is a transceiver microchip similar to an adhesive sticker which could be both active and passive, depending on the type of application. Active tags have a battery attached to them due to which they are always active and therefore continuously emit the data signals while Passive tags just get activated when they are triggered. Active tags are costlier than the Passive tags however they have a wide range of useful applications (Guicheng and Bingwu, 2011). RFID system is composed of readers and associated RFID tags which emit the identification, location or any other specifics about the object, on getting triggered by the generation of any appropriate signal (Zhang and Zhu, 2014). The emitted object related data signals are

transmitted to the Readers using radio frequencies which are then passed onto the processors to analyze the data.

ii. **Wireless Sensor Network (WSN):** WSN is a bi-directional wirelessly connected network of sensors in a multi-hop fashion, built from several nodes scattered in a sensor field each connected to one or several sensors which can collect the object specific data such as temperature, humidity, speed etc and then pass on to the processing equipment. The sensing nodes communicate in multi-hop each sensor is a transceiver having an antenna, a micro-controller and an interfacing circuit for the sensors as a communication, actuation and sensing unit respectively along with a source of power which could be both battery and any energy harvesting technology (Sohraby*et. al.,* 2007). However, (Guicheng and Bingwu, 2011) has proposed an additional unit for saving the data, named as Memory Unit which could also be a part of the sensing node.

iii. **Cloud Computing**: With millions of devices expected to come by 2020, the cloud seems to be the only technology that can analyze and store all the data effectively. It is an intelligent computing technology in which number of servers are converged on one cloud platform to allow sharing of resources between each other which can be accessed at any time and any place (Rao *et. al.,* 2012). Cloud computing is the most important part of IoT, which not only converges the servers but also processes on an increased processing power and analyzes the useful information obtained from the sensors and even provide good storage capacity (Xiaohui, 2013).

But this is just a beginning of unleashing the true potential of this technology. Cloud computing interfaced with smart objects using potentially millions of sensors can be of enormous benefits and can help IoT for a very large scale development so researches are being carried out since IoT will be totally dependent on the Cloud Computing.

iv. **Networking Technologies**: These technologies have an important role in the success of IoT since they are responsible for the connection between the objects, so we need a fast and an effective network to handle a large number of potential devices. For wide-range transmission network we commonly use 3G, 4G etc. but as we know, mobile traffic is so much predictable since it only has to perform the usual tasks like making a call, sending a text message etc. so as we step into this modern era of ubiquitous computing, it will not be predictable anymore which calls for a need of a super-fast, super-efficient fifth generation wireless system which could offer a lot more bandwidth (Vermesan and Friess, 2016). Similarly, for a short-range communication network we use technologies like Bluetooth, WiFi etc.

v. **Nano Technologies**: This technology realizes smaller and improved version of the things that are interconnected. It can decrease the consumption of a system by enabling the development of devices in nano meters scale which can be used as a sensor and an actuator just like a normal device. Such a nano device is made from nano components and

the resulting network defines a new networking paradigm which is Internet of Nano-Things (Akyildiz and Jornet, 2010).

vi. **Micro-Electro-Mechanical Systems (MEMS) Technologies**: MEMS are a combination of electric and mechanical components working together to provide several applications including sensing and actuating which are already being commercially used in many field in the form of transducers and accelerometers etc. MEMS combined with Nano technologies are a cost-effective solution for improvising the communication system of IoT and other advantages like size reduction of sensors and actuators, integrated ubiquitous computing devices and higher range of frequencies etc(Lubecke and Jung-Chih, 2000).

vii. **Optical Technologies**: Rapid developments in the field of Optical technologies in the form of technologies like Li-Fi and Cisco's BiDi optical technology could be a major breakthrough in the development of IoT. Li-Fi, an epoch-making Visible Light Communication (VLC) technology, will provide a great connectivity on a higher bandwidth for the objects interconnected on the concept of IoT. Similarly, Bi-Directional (BiDi) technology gives a 40G ethernet for a big data from multifarious devices of IoT.

4. APPLICATIONS

Most of the daily life applications that we normally see are already smart but they are unable to communicate with each other and enabling them to communicate with each other and share useful information with each other will create a wide range of innovative applications (Abdmeziem and Tandjaoui, 2006). These emerging applications with some autonomous capabilities would certainly improve the quality of our lives. A few of such applications are already in the market, let's take the example of the Google Car which is an initiative to provide a self-driving car experience with real-time traffic, road conditions, weather and other information exchanges, all due to the concept of IoT. There are a number of possible future applications that can be of great advantage. In this seminar, we present few of these applications.

i. **Smart Traffic System:**Traffic is an important part of a society therefore all the related problems must be properly addressed. There is a need for a system that can improve the traffic situation based on the traffic information obtained from objects using IoT technologies. For such an intelligent traffic monitoring system, realization of a proper system for automatic identification of vehicles and other traffic factors is very important for which we need IoT technologies instead of using common image processing methods. The intelligent traffic monitoring system will provide a good transportation experience by easing the congestion. It will provide features like theft-detection, reporting of traffic accidents, less

environmental pollution. The roads of this smart city will give diversions with climatic changes or unexpected traffic jams due to which driving and walking routes will be optimized (Rafiullah*et. al.,* 2012). The traffic lighting system will be weather adaptive to save energy. Availability of parking spaces throughout the city will be accessible by everyone.

ii. **Smart Environment:** Prediction of natural disasters such as flood, fire, earthquakes etc will be possible due to innovative technologies of IoT. There will be a proper monitoring of air pollution in the environment.

iii. **Smart Home:**IoT will also provide DIY solutions for Home Automation with which we will be able to remotely control our appliances as per our needs. Proper monitoring of utility meters, energy and water supply will help saving resources and detecting unexpected overloading, water leaks etc. There will be proper encroachment detection system which will prevent burglaries. Gardening sensors will be able to measure the light, humidity, temperature, moisture and other gardening vitals, as well as it will water the plants according to their needs.

iv. **Smart Hospitals:** Hospitals will be equipped with smart flexible wearable embedded with RFID tags which will be given to the patients on arrivals, through which not just doctors but nurses will also be able to monitor heart rate, blood pressure, temperature and other conditions of patients inside or outside the premises of hospital. There are many medical emergencies such as cardiac arrest but ambulances take some time to reach patient, Drone Ambulances are already in the market which can fly

to the scene with the emergency kit so due to proper monitoring, doctors will be able to track the patients and can send in the drone to provide quick medical care until the ambulance arrive.

v. **Smart Agriculture:** It will monitor Soil nutrition, Light, Humidity etc and improve the green housing experience by automatic adjustment of temperature to maximize the production. Accurate watering and fertilization will help improving the water quality and saving the fertilizers respectively.

vi. **Smart Retailing and Supply-chain Management:**IoT with RFID provides many advantages to retailers. With RFID equipped products, a retailer can easily track the stocks and detect shoplifting. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover, the retailer can even generate the sales chart and graphs for effective strategies.

vii. **Logistics:**IoT tries to simplify real world processes in business and information systems (Ferreira*et. al.,* 2010). The goods in the supply chain can be tracked easily from the place of manufacture to the final places of distribution using sensor technologies such as RFID and NFC. Real time information is recorded and analyzed for tracking. Information about the quality and usability of the product can also be saved in RFID tags attached with the shipments.

viii. **Energy Conservation:**The smart grid is information and communication technology enabled modern electricity generation,

transmission,distribution, and consumption system (Karnouskos, 2010).To make electric power generation, transmission, and distribution smart, the concept of smart grids adds intelligence at each step and also allows the two-way flow of power (back from the consumer to the supplier). This can save a lot of energy and help consumers better understand the flow of power and dynamic pricing. In a smart grid, power generation is distributed. There are sensors deployed throughout the system to monitor everything. It is actually a distributed network of microgrids.

ix. **Social Life and Entertainment:** Social life and entertainment play an important role in an individual's life. Many applications have been developed, which keep track of such human activities. The term "opportunistic IoT" Guo (2013) refers to information sharing among opportunistic devices (devices that seek to make contact with other devices) based on movement and availability of contacts in the vicinity. Personal devices such as tablets, wearables, and mobile phones have sensing and short range communication capabilities. People can find and interact with each other when there is a common purpose.

4.1 SECURITY AND PRIVACY CHALLENGES

IoT makes everything and person locatable and addressable which will make our lives much easier than before; however, without a lack of confidence about the security and privacy of the user's data, it's more unlikely to be adopted by many. So for its ubiquitous adoption, IoT must have a strong security infrastructure. Some of the possible IoT related issues are as followed:

i. **Unauthorized Access to RFID**: An unauthorized access to tags that contains the identification data is a major issue of IoT which can expose any kind of confidential information about the user so it needs to be addressed. Not just the tag can be read by a miscreant reader but it can even be modified or possibly be damaged. In this context, summarized some of the real life threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and SpeedPass Hack.

ii. **Sensor-Nodes Security Breach**: WSNs are vulnerable to several types of attacks because sensor nodes are the part of a bi-directional sensor network which means other than the transmission of data, acquisition of data is also possible. Some of the possible attacks that includes Jamming, tampering, Sybil, Flooding and some other kinds of attacks, which are summarized as followed:

   - Jamming obstructs the entire network by interfering with the frequencies of sensor nodes.

- Tampering is the form of attack in which the node data can be extracted or altered by the attacker to make a controllable node.
- Sybil attack claims multiple pseudonymous identities for a node which gives it a big influence.
- Flooding is a kind of a DOS attack caused by a large amount of traffic that results in memory exhaustion.

iii. **Cloud Computing Abuse:** Cloud computing is a big network of converged servers which allow sharing of resources between each other. These shared resources can face a lot of security threats like Man-in-the-middle attack (MITM), Phishing etc. Steps must be taken to ensure the complete security of the clouding platform. Cloud Security Alliance (CSA) proposed some possible threats among which few are Malicious Insider, Data Loss, Accounts Hijacking and Monstrous use of Shared Computers etc. which are summarized as followed:

- Malicious Insider is a threat that someone from the inside who have an access to the user's data could be involved in data manipulating.
- Data Loss is a threat in which any miscreant user who has an unauthorized access to the network can modify or delete the existing data.
- Man-in-the-middle (MITM) is a kind of Account Hijacking threat in which the attacker can alter or intercept messages in the communication between two parties.

- Cloud computing could be used in some monstrous ways because if the attacker gets to upload any malicious software in the server e.g. using a zombie-army (botnet), it could get the attacker a control of many other connected devices.

5. CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the concept of Internet of Things will soon be inexorably developing on a very large scale. This emerging paradigm of networking will influence every part of our lives ranging from the automated houses to smart health and environment monitoring by embedding intelligence into the objects around us. In this paper we discussed the vision of IoT and presented a well-defined architecture for its deployment. Then we highlighted various enabling technologies and few of the related security threats. And finally we discussed a number of applications resulting from the IoT that are expected to facilitate us in our daily lives. Researchers are already being carried out for its wide range adoption, however without addressing the challenges in its development and providing confidentiality of the privacy and security to the user, it's highly unlikely for it to be an omni-present technology. The deployment of IoT requires strenuous efforts to tackle and present solutions for its security and privacy threats.

REFERENCES

Abdmeziem,R. andTandjaoui,D. (2006) ”Internet of Things: Concept, Building blocks, Applications and Challenges, Computers and Society, Cornell University” London.

Akyildiz,I.and Jornet, J. (2010) ”THE INTERNET OF NANOTHINGS,” *IEEE Wireless Communications*, Volume: 17 Issue: 6, pp. 58-63.

Atzori, L., Iera, A. and Morabito,G. (2014) ”The Internet of Things: A survey,” *in Computer Networks* - Science Direct.

Benjamin, K., (2011) ”RFID as an Enabler of the Internet of Things: Issues of Security and Privacy,” *in Internet of Things (iThings/CPSCom),* pp. 709- 712.

Debasis, B. andJaydip, S. (2016) ”Internet of Things-Applications and Challenges in Technology and Standardization” *in Wireless Personal Communications*, Volume 58, Issue 1, pp. 49-69.

De-Li, Y., Feng, L. and Yi-Duo, L., (2010) ”A Survey of the Internet of Things”, *in International Conference on E-Business Intelligence* (ICEBI).

Ferreira, P., Martinho,R. andDomingos,D. (2010) “Iot-aware business processes for logistics: limitations of current approaches,” *in Proceedings of the Inforum Conference*, vol. 3, pp. 612–613.

Guicheng, S. and Bingwu, L., (2011)” The visions, technologies, applications and security issues of Internet of Things,” *in E-Business and E-Government* (ICEE), pp. 1-4.

Guo, B., Zhang, D.,Wang, Z., Yu, Z. and Zhou, X. (2013) “Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things,” *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1531–1539.

Harald, S., Patrick, G., Peter, F. and Sylvie, W., (2016) ”Vision and challenges for realizing the Internet of Things,” *Publications Office of the European Union*.

Hui, S., Jiafu, W., Caifeng, Z. andJianqi, L. (2012) ”Security in the Internet of Things: A Review,” *in Computer Science and Electronics Engineering* (ICCSEE), pp. 648-651.

Jian, A., Xiao-Lin, G. and Xin, H. (2012) ”Study on the Architecture and Key Technologies for Internet of Things,” *in Advances in Biomedical Engineering*, Vol.11, IERI, pp. 329-335.

Karnouskos,S. (2010) “The cooperative internet of things enabled smart grid,” *in Proceedings of the 14th IEEE International Symposium on Consumer Electronics* (ISCE '10), pp. 7–10.

Lan, L. (2005) ”Study of Security Architecture in the Internet of Things,” *in Measurement, Information and Control* (MIC),, Volume: 1, pp. 374- 377

Lubecke, V. M. and Jung-Chih, C. (2000) ”MEMS technologies for enabling high frequency communications circuits,” *in Telecommunications in Modern Satellite, Cable and Broadcasting Services*, Volume: 2, pp. 382-389

Ma,H.D. (2011)” Internet of things: Objectives and scientific challenge,” *in Journal of Computer Science and Technology*, pp. 919-924.

Miao, W., Ting-lie, L., Fei-Yang, L., ling, S. and Hui-Ying, D. (2010) ”Research on the architecture of Internet of things,” *in Advanced Computer Theory and Engineering* (ICACTE), pp. 484-487.

Nich, H., (2015)” What the Internet of Things means for you”. It can be accessed at: http://www.techrepublic.com/blog/europeantechnology/what-the- internet-of-things-means-for-you

Peña-López, I.(2005) Internet Report 2005: The Internet of Things.

Rafiullah, K., Sarmad, U. K., Rifaqat, Z. and Shahid, K., (2012)” Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges,” *in Proceedings of Frontiers of Information Technology* (FIT), p p . 257-260.

Rao,B.B. P.,Saluia,P., Sharma,N.,Mittal,A. and Sharma,S.V. (2012) ”Cloud computing for Internet of Things & sensing based applications,” *in Sensing Technology* (ICST), Sixth International Conference, IEEE.

Ronda, H. (2007) ” ARPANET to the Internet”- *TCP Digest (UUCP).* Retrieved 2016-06-05 It can be accessed at: http://www.columbia.edu/ r h 1 2 0 / other/tcpdigest paper.txt

Sohraby, K., Minoli, D., Znati, T. (2007) ”Wireless sensor networks: technology, protocols, and applications”, *John Wiley and Sons,*ISBN 978-0-471-74300-2, pp. 15-18.

Vermesan, O. and Friess,P. (2016) ”Internet of Things ? From Research and Innovation to Market Deployment,” *River Publishers*, pp. 74-75.

Vermesan, O. and Friess, P. G., (2011) “Internet of things strategic research roadmap*,” in Internet of Things: Global Technological and Societal Trends*, vol. 1, pp. 9–52.

Wang, C. (2012) ”AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS,” *in Cloud Computing and Intelligent Systems* (CCIS), 2012, pp.

Xiaohui, X. (2013) ”Study on Security Problems and Key Technologies of The Internet of Things,” *Computational and Information Sciences* (ICCIS), pp. 407-410.

Xu, C., Minghui, Z., Fuquan, S., (2012) ”Architecture of internet of things and its key technology integration based-on RFID*,” in Fifth International Symposium on Computational Intelligence and Design*, pp. 294-297.

Ying, Z., (2011) ”Technology Framework of the Internet of THings and Its Application,” *in Electrical and Control Engineering* (ICECE), pp. 4109- 4112.

Zhang,H. and Zhu,L. (2011)”Internet of Things: Key technology, architecture and challenging problems”, *in Computer Science and Automation Engineering* (CSAE), 2011, Volume: 4, pp. 507-512.