Internet of Things (IoT) and Its Applications

Ashish Kumar[1], Ansh Jhawar[2], Deepak Bisht[3], Pius Alex[4]
[1,2,3,4]*B. tech Student, Department of Computer Science & Engineering, Dronacharya Group of Institution, Greater Noida, India*

***Abstract* - The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and plays.**

Internet, a revolutionary invention, is always transforming into some new kind of hardware and software making it unavoidable for anyone. 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 paper aims to provide a comprehensive overview of the IoT scenario and reviews its enabling technologies and the sensor networks. The paper concludes with a discussion of social and governance issues that are likely to arise as the vision of the Internet of Things becomes a reality.

***Index Terms* - Internet of Things, IoT Vision, IoT applications, RFID, Iot security.**

INTRODUCTION

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency Identification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that Cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere.

The concept of IoT dates back to 1982 when a modified coke machine was connected to the Internet which was able to report the drinks contained and that whether the drinks were cold Later, in 1991, a contemporary vision of IoT in the form of ubiquitous computing was first given by Mark Weiser However in 1999, Bill Joy gave a clue about Device to Device communication in his taxonomy of internet. In the very same year, Kevin Ashton proposed the term ”Internet of Things” to describe a system of interconnected devices. The basic idea of IoT is to allow autonomous exchange of useful information between invisibly embedded different uniquely identifiable real world devices around us, fueled by the leading technologies like Radio-Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) which are sensed by the sensor devices and further processed for decision making, on the basis of which an automated action is performed.

Vision: 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. 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. 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. 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.

IoT 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. 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 section, we present few of these applications.

A. Personal and Home(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. The sensor information collected is used only by the individuals who directly own the network. Usually WiFi is used as the backbone enabling higher bandwidth data (video) transfer as well as higher sampling rates (Sound). Ubiquitous healthcare has been envisioned for the past two decades. IoT gives a perfect platform to realize this vision using body area sensors and IoT backend to upload the data to servers. For instance, a Smartphone can be used for communication along with several interfaces like Bluetooth for interfacing sensors measuring physiological parameters. So far, there are several applications available for Apple iOS, Google Android and Windows Phone operating system that measure various parameters. However, it is yet to be centralized in the cloud for general physicians to access the same.

An extension of the personal body area network is creating a home monitoring system for aged-care, which allows the doctor to monitor patients and elderly in their homes thereby reducing hospitalization costs through early intervention and treatment. Control of home equipment such as air conditioners, refrigerators, washing machines etc., will allow better home and energy management. This will see consumers become involved in the IoT revolution in the same manner as the Internet revolution itself . Social networking is set to undergo another transformation with billions of interconnected objects. An interesting development will be using a Twitter-like concept where individual Things‘ in the house can periodically tweet the readings which can be easily followed from anywhere creating a Tweetot. Although this provides a common framework using cloud for information access, a new security paradigm will be required for this to be fully realized.

B. Mobile:

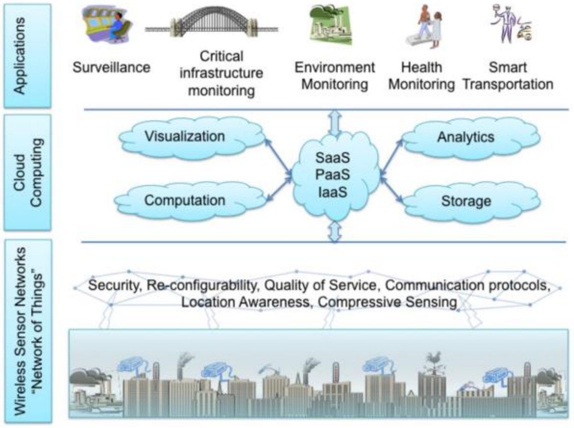
Smart transportation and smart logistics are placed in a separate domain due to the nature of data sharing and backbone implementation required. Urban traffic is the main contributor to traffic noise pollution and a major contributor to urban air quality degradation and greenhouse gas emissions. Traffic congestion directly imposes significant costs on economic and social activities in most cities. Supply chain efficiencies and productivity, including just-in-time operations, are severely impacted by this congestion causing freight delays and delivery schedule failures. Dynamic traffic information will affect freight movement, allow better planning and improved scheduling. The transport IoT will enable the use of large scale WSNs for online monitoring of travel times, origin-destination (O-D) route choice behavior, queue lengths and air pollutant and noise emissions. The IoT is likely to replace the traffic information provided by the existing sensor networks of inductive loop vehicle detectors employed at the intersections of existing traffic control systems. They will also underpin the development of scenario-based models for planning and design of mitigation and alleviation plans, as well as improved algorithms for urban traffic control, including multi-objective control systems. Combined with information gathered from the urban traffic control system, valid and relevant information on traffic conditions can be presented to travelers.

The prevalence of Bluetooth technology (BT) devices reflects the current IoT penetration in a number of digital products such as mobile phones, car hands-free sets, navigation systems, etc. BT devices emit signals with a unique Media Access Identification (MAC-ID) number that can be read by BT sensors within the coverage area. Readers placed at different locations can be used to identify the movement of the devices. Complemented by other data sources such as traffic signals, or bus GPS, research problems that can be addressed include vehicle travel time on motorway and arterial streets, dynamic (time dependent) O-D matrices on the network, identification of critical intersections, and accurate and reliable real time transport network state information. There are many privacy concerns by such usages and digital forgetting is an emerging domain of research in IoT where privacy is a concern .

Another important application in mobile IoT domain is efficient logistics management. This includes monitoring the items being transported as well as efficient transportation planning. The monitoring of items is carried out more locally, say, within a truck replicating enterprise domain but transport planning is carried out using a large scale IoT network.

C. Cloud centric Internet of Things:

The vision of IoT can be seen from two perspectives – Internet‘ centric and Thing‘ centric. The Internet centric architecture will involve internet services being the main focus while data is contributed by the objects. In the object centric architecture, the smart objects take the center stage. In our work, we develop an Internet centric approach. A conceptual framework integrating the ubiquitous sensing devices. In order to realize the full potential of cloud computing as well as ubiquitous Sensing, a combined framework with a cloud at the center seems to be most viable. This not only gives the flexibility of dividing associated costs in the most logical manner but is also highly scalable. Sensing service providers can join the network and offer their data using a storage cloud; analytic tool developers can provide their software tools; artificial intelligence experts can provide their data mining and machine learning tools useful in converting information to knowledge and finally computer graphics designer can offer a variety of visualization tools. The cloud computing can offer these services as Infrastructures, Platforms or Software where the full potential of human creativity can be tapped using them as services. This in some sense agrees with the ubicomp vision of Weiser as well as Rogers human centric approach. The data generated, tools used and the visualization created disappears into the background, tapping the full potential of the Internet of Things in various application domains. As can be seen from Figure 4, the Cloud integrates all ends of ubicomp by providing scalable storage, computation time and other tools to build new businesses. In this section, we describe the cloud platform using Manjrasoft Aneka and Microsoft Azure platforms to demonstrate how cloud integrates storage, computation and visualization paradigms. Furthermore, we introduce an important realm of interaction between cloud which is useful for combining public and private clouds using Aneka. This interaction is critical for application developers in


Applications
Surveillance
Critical infrastructure monitoring
Environment Monitoring
Health Monitoring
Smart Transportation
Cloud Computing
Visualization
Analytics
SaaS
PaaS
IaaS
Computation
Storage
Wireless Sensor Networks "Network of Things"
Security, Re-configurability, Quality of Service, Communication protocols, Location Awareness, Compressive Sensing

order to bring sensed information, analytics algorithms and visualization under one single seamless framework.

D. 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. The traffic lighting system will be weather adaptive to save energy. Availability of parking spaces throughout the city will be accessible by everyone.

E. 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.

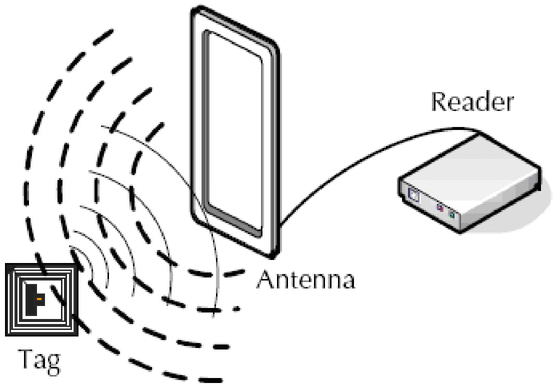
F. Smart Retailing and Supply-chain Management:

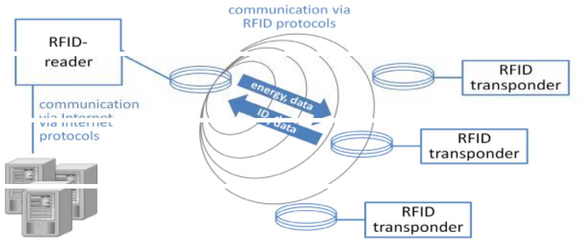
IoT with RFID provides many advantages to retailers. With RFID equipped products, a retailer can easily track the stocks and detect shoplifting. It can keep a track of all the items in a store and to prevent them from going out-of-stock, it places an order automatically. Moreover the retailer can even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

Radio Frequency Identification (RFID):

RFID (Radio Frequency Identification) is primarily used to identify objects from a distance of a few meters, with a stationary reader typically communicating wirelessly with small battery-free transponders (tags) attached to objects. As well as providing two important basic functions for an Internet of Things – identification and communication – RFID can also be used to determine the approximate location of objects provided the position of the reader is known. At the end of the 1990s, RFID technology was restricted to niche applications such as animal identification, access control and vehicle immobilizers. High transponder prices and a lack of standards constituted an obstacle to the wider use of the technology. Since then, however, its field of application has broadened significantly, mainly thanks to MIT’s Auto-ID Center, which was founded in 1999. The Auto-ID Center and its successor organization EPCglobal have systematically pursued a vision of cheap, standardized transponders identifying billions of everyday objects, and they have developed the necessary technology jointly with commercial partners. The use of RFID technology in the supply chains of retail giants such as Wal-Mart and Metro is the result of these efforts. While the adoption by major retailers represents a remarkable success, the evolution of RFID and its associated infrastructure technologies in recent years also highlights challenges involved in realizing an Internet of Things in the broader sense of the term.

RFID is the key technology for making the objects uniquely identifiable. Its reduced size and cost makes it integrable into any object. 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 more costly than the Passive tags however they have a wide range of useful applications. 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. 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.





Depending on the type of application, RFID frequencies are divided into four different frequencies ranges, which are given below:
(1) Low frequency (135 KHz or less)
(2) High Frequency (13.56MHz)
(3) Ultra-High Frequency (862MHz 928MHz)
(4) Microwave Frequency (2.4G, 5.80)
Bar Code is also an identification technology which has almost the same function as an RFID, but RFID is more effective than a Bar Code due to a number of its benefits. RFID being a radio technology does not require the reader to be physically in its vision while Bar Code is an optical technology which cannot work unless its reader is placed in front of it. Moreover, an RFID can work as an actuator to trigger different events and it has even modification abilities which Bar codes clearly do not have.

Internet of Things (IoT) Security and Privacy:
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 is 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:
1. 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 cellphone and SpeedPass Hack.

2. 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. Described some of the possible attacks that includes Jamming, tampering, Sybil, Flooding, and some other kinds of attacks, which are summarized as followed:
(1) Jamming obstructs the entire network by interfering with the frequencies of sensor nodes.
(2) Tampering is the form of attack in which the node data can be extracted or altered by the attacker to make a controllable node.
(3) Sybil attack claims multiple pseudonymous identities for a node which gives it a big influence.
(4) Flooding is a kind of a DOS attack caused by a large amount of traffic that results in memory exhaustion.

3. 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:
(1) Malicious Insider is a threat that someone from the inside who have access to the user's data could be involved in data manipulating.
(2) 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.

(3) 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.
(4) Cloud computing could be used in a monstrous way 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.

4. Social and Political issues:
The Internet has long since changed from being a purely informational system to one that is socio-technological and has a social, creative, and political dimension. But the importance of its non-technological aspects is becoming even more apparent in the development of an Internet of Things since it adds an entirely new quality to these non-technological aspects. So, in addition to the positive expectations mentioned above, several critical questions need to be asked with regard to possible consequences. Much of the public debate on whether to accept or reject the Internet of Things involves the conventional dualisms of "security versus freedom" and "comfort versus data privacy". In this respect, the discussion is not very different from the notorious altercations concerning store cards, video surveillance and electronic passports. As with RFID, the unease centers primarily on personal data that is automatically collected and that could be used by third parties without people's agreement or knowledge for unknown and potentially damaging purposes. And personal privacy is indeed coming under pressure. Smart objects can accumulate a massive amount of data, simply to serve us in the best possible way. Since this typically takes place unobtrusively in the background, we can never be entirely sure whether we are being "observed" when transactions take place. Individual instances of observation might seem harmless enough, but if several such instances were to be amalgamated and forwarded elsewhere, this could under certain circumstances result in a serious violation of privacy. Irrespective of the data protection issues, there is also the question of who would own the masses of automatically captured and interpreted real-world data, which could be of significant commercial or social value, and who would be entitled to use it and within what ethical and legal framework. Another critical aspect is that of dependence on technology. In business and also in society generally we have already become very dependent on the general availability of electricity – infrequent blackouts have fortunately not yet had any serious consequences. But if everyday objects only worked properly with an Internet connection in the future, this would lead to an even greater dependence on the underlying technology. If the technology infrastructure failed for whatever reason – design faults, material defects, sabotage, overloading, natural disasters, or crises – it could have a disastrous effect on the economy and society. Even a virus programmed by some high-spirited teenagers that played global havoc with selected everyday objects and thus provoked a safety-critical, life-threatening, or even politically explosive situation could have catastrophic consequences. Remotely controlled things could also cause us to become dependent and lose our supremacy on a personal level. And even with no ill intent, our own smart objects might not behave as we would wish, but rather as they "believe" is best for us – presaging a subtle type of technological paternalism. Although these extreme opinions are not representative, it must be said that for an Internet of Things to be truly beneficial requires more than just everyday objects equipped with microelectronics that can cooperate with each other. Just as essential are secure, reliable infrastructures, appropriate economic and legal conditions, and a social consensus on how the new technical opportunities should be used. This represents a substantial task for the future.

CONCLUSION

The proliferation of devices with communicating-actuating capabilities is bringing closer the vision of an Internet of Things, where the sensing and actuation functions seamlessly blend into the background and new capabilities are made possible through access of rich new information sources. The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps.

Presented here is a user-centric cloud-based model for approaching this goal through the interaction of private and public clouds. In this manner, the needs of the end-user are brought to the fore. Allowing for the necessary flexibility to meet the diverse and sometimes competing needs of different sectors, we propose a framework enabled by a scalable cloud to provide the capacity to utilize the IoT. The framework allows networking, computation, storage, and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. In proposing the new framework associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable. The consolidation of international initiatives is quite clearly accelerating progress towards an IoT, providing an overarching view for the integration and functional elements that can deliver an operational IoT.

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. Researches 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

[1] K. Ashton, That ―Internet of Things‖ Thing, RFiD Journal. (2009).

[2] J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.

[3] Adelmann, R., Langheinrich, M., Floerkemeier, C.: A Toolkit for Bar Code Recognition and Resolving on Camera Phones – Jump-Starting the Internet of Things. Proc. Workshop Mobile and Embedded Interactive Systems. In: Hochberger, C., Liskowsky, R. (eds.) Informatik 2006 – GI Lecture Notes in Informatics (LNI) 94, pp. 366–373 (2006).

[4] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan," Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in Proceedings of Frontiers of Information Technology (FIT), 2012, pp. 257-260.

[5] Ling-yuan Zeng," A Security Framework for Internet of Things Based on 4G Communication," in Computer Science and Network Technology (ICCSNT), 2012, pp. 1715-1718.

[6] European Commission: Internet of Things – An action plan for Europe. COM (2009) 278, http://eur-lex.europa.eu/LexUriServ/site/en/com/2009/com2009_0278en01.pdf (2009).

[7] M. Weiser," The computer for the 21st century", Sci. Amer., 1991, pp.66 -75.

[8] R. Caceres, A. Friday, Ubicomp Systems at 20: Progress, Opportunities, and Challenges, IEEE Pervasive Computing 11 (2012) 14–21.

[9] Guinard, D., Trifa, V., Wilde, E.: Architecting a Mashable Open World Wide Web of Things. TR CS-663 ETH Zürich, www.vs.inf.ethz.ch/publ/papers/WoT.pdf (2010).

[10] " The Internet of Things," ITU Report, Nov 2005.

[11] V. Mayer-Schönberger, Failing to Forget the ―Drunken Pirate, ‖ in: Delete: The Virtue of Forgetting in the Digital Age (New in Paper), 1st ed, Princeton University Press, 2011: pp. 3–15.

[12] Guinard, D., Trifa, V., Wilde, E.: Architecting a Mashable Open World Wide Web of Things. TR CS-663 ETH Zürich, www.vs.inf.ethz.ch/publ/papers/WoT.pdf (2010).

[13] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler," Transmission of IPv6 Packets over IEEE 802.15.4 Networks".

[14] D. Donoho, Compressed sensing, IEEE Transactions on Information Theory. 52 (2006) 1289–1306.

[15] D.B. Neill, Fast Bayesian scan statistics for multivariate event detection and visualization, Statistics in Medicine 30 (2011) 455–469.

[16] L.Atzori, A.Iera, G. Morabito, ”The Internet of Things: A survey,” in Computer Networks - Science Direct.