iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** XII **Month of publication:** December 2019

DOI: http://doi.org/10.22214/ijraset.2019.12071

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

Wireless Sensors Integration into Internet of Things and the Security Primitives

Alex. R. Mathew
Department of Cyber Security, Bethany College, USA

Abstract: ***The ordinary way of looking at the present smart systems in largely associated with a single concept, and this is the internet of things (IoT) where the whole physical structure is connected with intelligent communication and monitoring devices enabled by the wireless sensors. In such a vibrant and intelligent system, the sensors are interlinked to facilitate sensing of critical information and control the instructions through the sensor networks that are distributed all over the system. It has been shown that wireless sensors are easy flexibility and faster deployment of devices in contrary to the wired setup system. With the increased rate of technological development of sensors, wireless sensor networks are deemed to become the essential technology for IoT and as well become an invaluable resource for the realization of the vision put forth by the internet of things paradigm (IoT). Further, it is mandatory to consider whether there should be a complete integration of the sensors of the Wireless Sensor Networks into the IoT or should not. New challenges to security come up when heterogenous sensors are incorporated into the IoT. Security at global perspective should be considered and not only at the local scale. Therefore, this paper will give an overview of the integration of sensors into the IoT, with some major challenges to the security of systems and also several security primitives which can be adopted for the protection of data via the internet.***

Keywords: Internet of Things (IoT) Wireless Sensor Networks (WSN) Confidentiality, Integration, Privacy

I. INTRODUCTION

Presently, the Internet of Things has become in Itself a thing that is worth to talk about, from simple places like the discussions in universities about projects to meetings of massive companies. IoT has been identified as one of the technologies of the future that have emerged. IoT concept is simple from its core; being a connection if devices over the internet, and making the devices smart. IoT can be thought as a network experiencing expansion from being a network of computers to a network that incorporates the computers and things. The ideology is not new since the first thing that was connected to the internet was the Coke vending machine in 1982 by Carnegie Mellon University Students. The new concepts that have been added to this aspect is about the sensors, which are the tiny sensors that are embedded in this devices which are able to gather almost every kind of information within the surrounding environment including temperature, time, movement, sound, light, distance, speed and many more.

However, the term internet of things is not a new concept as it was devised by Ashton Kevin in 1999. Ashton was the co-founder and executive director of Auto-ID Center at MIT and he called it as uniquely identifiable objects that are virtually represented within a structure that is similar to internet. The increased advancement in technology has facilitated the reduction in the costs of these sensors, transmitters, and processors and consecutively the computational and processing powers of these devices have become high and have allowed them into any object of our daily life like in foods, clothing and medicine. The advancement in technology has facilitated the connectivity by addition of an extra dimension to it, and this is the connection of anything. For instance, Nike introduced a new line of athletics shoes which is able to track the progress of the wearers and be able to post the updates online. The “Smart dust” age has been talked about for many years and it is finally here and after developing a fully functional computers, with built-in wireless connectivity which are very minute and measuring approximately 1 cubic mm. The internet of things is deemed to transform everything in many industries including the retail, transportation, industrial, medical, communications and energy.

The revolutionization of technology is increasing every day. According to Cisco, it is expected that the number of connected devices will exponentially grow in 2020 to 50 billion. Also, Intel predicts optimistically that the number of connected devices will 200 million by 2020. The main driver for this is not the human population but rather owing to the fact that the devices that people use in their daily life as well as operational technologies like those that are found on the floor of will be more connected entities globally. The world is becoming a world of interconnected things where there is increasing interaction of humans with machines and machines have been modified to talk to other machines, this is here at the moment and it is here to stay.

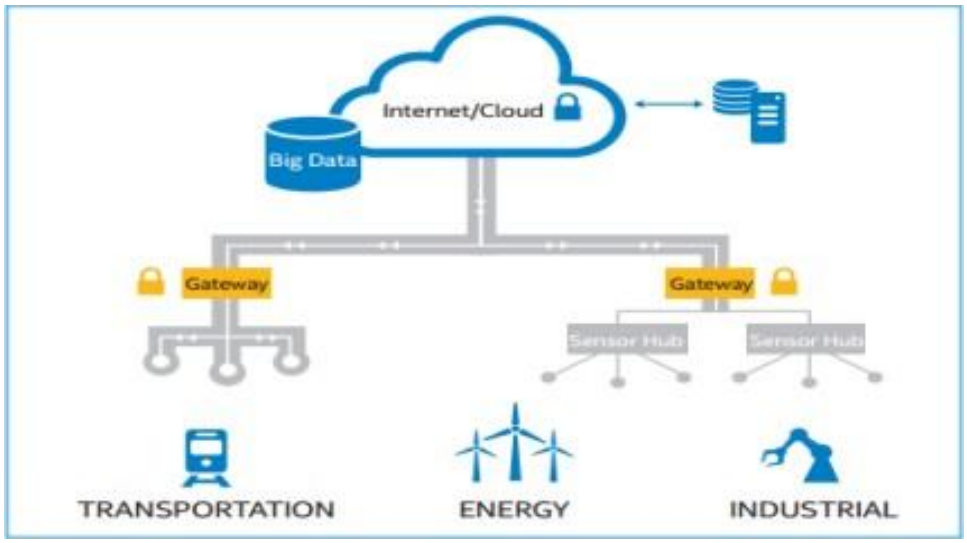
The shift from the consumer-based IPv4 internet of tablets and laptops which is basically the shift from IT to Operational Technology (OT) based IPv6 Internet of machine to machine interactions is one of the interesting trends that is contributing to the

growth of IoT. The shift includes the sensors, smart objects and clustered systems like the Smart Grid. IPv6 is a newly enabling technology which is an upgrade to the original fundamental internet protocol=Internet Protocol, that supports all communication on the internet. IPv6 is essential since the internet is running out of the IPv4 addresses.

The significant challenge in this is to make the IPv6 interoperable for the most IoT software which were developed for IPv4 and which are as well readily available. However, according to many experts they believe that IPv6 is the smartest connectivity option which will allow IoT to attain its potential.

Notwithstanding, there ae challenges that need to be addressed including the ways to communicate effectively and securely between the devices, ways of transmitting and store huge amounts of data, and the ways to protect the privacy. Though, a significant barrier to the realization of the full potential of IoT is that approximately 85% of the things that exist were not designed to connect to the internet and thus cannot share data with the cloud.

In addressing this issue, gateways from the mobiles, home and industry, while all are playing the part will become intermediaries between the cloud and legacy things. Thus, this will happen, not only by providing the required connectivity, but also the security and the manageability.



Things that can be connected to the internet have different characteristics. they range from small and static devices like the RFIDs to the huge mobile devices like vehicles.

The heterogeneity produces complexity and indicates the presence of a middleware which can mask this variability and thus promoting transparency. The Radio Frequency Identification (RFID) and the Wireless Sensor Networks (WSN) among other technologies are among the two most promising technologies that enable the implementation of the IoT infrastructure. RFID is a low-cost and low power technology which consists of passive or as well battery-assisted passive devices also known as tags, that can transmit data when they are powered by an electromagnetic field which is generated by an interrogator or reader. Simple passive RFID tags do not require any energy source for their operation and their lifetime can be measured in decades, and this makes RFID technology to be well suited in a variety of situations of application including in industries and healthcare. However, the main challenge for RFID are the non-uniform encoding, conflict collision and the RFID privacy protection.

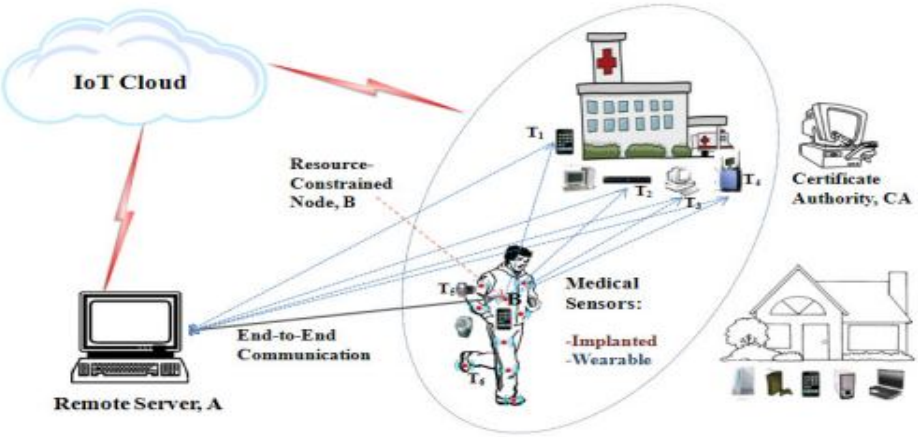
Comparatively, WSNs are generally self-organizing and hoc networks of small and cost-effective devices also known as motes which communicate in a multi-hop way to provide control and monitor functionalities in vital applications including military, industrial, automotive and the healthcare sectors.

Presently, most of the WSN motes are powered by battery computer systems integrating the analogue and digital sensors as well as the IEEE 802.15.4 radio which enable up o 100m range of outdoor communication. Unlike the other networks, WSNs ae particularly characteristic of the collection of sensed data, like temperature, pressure motion and fire detection and forwarding it to the base station. Despite that most of the WSNs were not designed for two-way communication, they should be able to receive information and send it to the sensors and as well be able to react on behalf of the commander like in the automation of home appliances.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue XII, Dec 2019- Available at www.ijraset.com

II. SENSOR NETWORKS IN A GLOBALLY CONNECTED NETWORK

The integration of the WSN into IoT is not a mere speculation since a number of big technology companies have supported and developed their IoT infrastructure around the WSN. For instance, it is noteworthy to mention about the "A Smarter Planet" by IBM, a strategy that considers sensors as fundamental pillars in the intelligent systems for water management as well as intelligent cities; the HP Labs CeNSE project, that is focused on the deployment of a sensor network that is worldwide so as to create Earths Central Nervous System. However, an important question is how the sensor networks should provide their services either directly or through a base station when connecting WSN to the internet. It is worth noting that the 'thing' that is connected to the internet is supposed to be locatable and addressable via the internet, though, this particular configuration might not be suitable in some situations. Some of such particular situations include those in SCADA systems where there is no need for a sensor node to provide its services directly as well other situations where a sensor node should be integrated into the internet entirely.



The IoT's evolution has its origins in the wireless technology convergence, the advancements of MEMS and the digital electronics where as a result of the miniature devices that have the ability to sense and compute can wirelessly communicate. However, having an IP connectivity does not guarantee that every sensor node should have a direct connection to the internet. There need to be a carefully consideration on some challenges and among those challenges, the most prevalent is security. During the IoT era, the interaction between humans and computers need to be more aggressive as machines have evolved and become more smarter and thus started handling tasks meant for humans. A thing therefore might be a patient having a medial implant that facilitates real-time monitoring in the healthcare application or as well an accelerometer for movement that is attached to an animal within a dairy environment. In such a situation therefore, humans are required to trust these machines and feel safe about them.

III.IOT SECURITY AND PRIVACY

The projections of the IoT application predicts for a safer, smarter and efficient world while some observers display concerns it might become a darker world for surveillance, security and privacy violations, as well as a consumer lock-in. The IoT scale and context make it a compelling target for those that might want to harm companies, nations, networks, organizations and individual entities as people. As the IP systems are continually being adopted, the IoT application have become a significant target for attacks and this might become more sophisticated and grow more in magnitude. The nature in which the IoT devices are interconnected means that every poorly secured device that is connected online has a potential, of affecting the global internet resilience and security. The weakest link is a definition of the overall security level of the entire infrastructure. Besides, the challenges herein are proliferated by the considerations like the mas-scale homogenous deployment of the IoT devices, the ability of some of the devices connecting to other devices, and the likelihood of fielding the devices in an unsecure environment. The coming of IoT presents with it challenges to the architects of networks and security. Smarter security systems including managed threat detection, anomaly detection and predictive analysis need to evolve. Further, various challenges are experienced in the designing of security solutions in the IoT because of the characteristics of the network including the heterogeneity of the devices, constraint in resources, unreliable links for communication, and the distribution nature. In the conventional TCP/IP networks, security is developed to enhance protection of confidentiality, availability and integrity of the network data. It makes the system reliable and as well protects the system from malicious attacks which might lead to system malfunctioning as well as information disclosure. The IoT requires multi-

facet security solutions where there is secure communication with confidentiality, authentication and integrity services; in this case the network is protected from any intrusion and disruptions; and the sensor node like in the WSN, with imposed security protection and user privacy depending on the scenario for application.

With the IPv6, there are enough IP addresses that can connect to billions of 'things' facilitating the formation of the new IoT world but whether these things will be secure enough to ensure individual privacy and rights and secure systems form malicious attacks. There is need for algorithms to become highly efficient, low power, low energy realizations especially for the devices that are passively powered or operated via battery. In many practical applications, there is need for the gateway to send periodic messages for control, notifications as well as sensitive confidential data to all the wearable devices where there needs to be a common secret key for encryption or decryption on such smart devices with their hardware integration supporting them as well. Although, when the number of devices that are connected has become too high, it becomes infeasible to exchange the symmetrical keys and the need to have an efficient scalable key establishment protocol becomes vital. Another approach is to key distribution via asymmetrical key cryptography, however, this requires computational costs, which is the main concern for resource-constrained devices. Therefore, the heterogenous nature of the sensors makes it impossible to apply the conventional security primitives (either implanted, wearable of on-body) low resources and systems architecture of the healthcare systems that are IoT based.

IV. IOT SECURITY PRIMITIVES

Devices can only be regarded to be smart if they include technology that provides security and privacy. When IoT devices are poorly secured, they might serve as entry points for cyber-attacks by allowing malicious individuals to re-program a device or as well cause malfunctioning of a device. Furthermore, unique to the cryptographic implementation is that they as well require protection against physical interference either passive or active. These therefore means that there is need to include the countermeasures in the design process. IoT security must ensure that there is secrecy and integrity of communication as well as the messages that are being exchanged are authenticated.

From the perspective of the end-users, it is not easy to possibly modify these smart devices; security primitives must be pre-embedded into the system. The integration of the sensors into the internet require that interoperability, transparency and flexibility are ensured. However, the sensor nodes might inherently have constrained resources; since small batteries are the primary source of energy for the sensor nodes which requires longer periods of operation. Hence energy efficiency becomes an important factor besides security and the issues of privacy. There are different approaches being employed in the E2E communication in the WSNs and the IoT. These can be classified into the major directions of research as follows; centralized approaches, protocol-based extensions and optimizations, alternative delegation and architecture and solutions that require special purpose hardware modules. There is need as well to understand the techniques for attack in order to rationalize security mechanisms in the protocol of communication. Some of the significant attacks in respect to IoT include; eavesdropping, impersonation, MITM Attack, and the DoS Attack. The conventional security primitives are not applicable because of the sensors' heterogenous nature, resource insufficiency, and the system architecture of the systems that are based on IoT. Any use of data that is unauthorized or privacy concerns may restrict people to utilize applications that are IoT-based. Therefore, to mitigate these privacy and security threats, there is need for a strong network security infrastructure. Peer authentication and end-to-end protection of data are crucial requirements for the prevention of eavesdropping on the sensitive data or malicious triggering of harmful actuating tasks. Some of the security primitives that need to be considered include; securing of device identity and the mechanisms to authenticate it, protection of the initial configuration and provisioning of devices from tempering, theft and other forms of compromise throughout usage life, application of geographic location and privacy levels of data, strong identities, strengthening of other network-centric methods like the Domain Name system and adoption of other protocols that are more tolerant to delay or transient connectivity.

V. IS INTERNET OF THINGS REAL?

It is evident that internet of things is coming. It is no longer a matter of if or whether, but it is all about when and how. The primary question as well is where humans will be placed into this exponential expansion of growth of IoT? Technological innovations are mostly emerging from the society needs of humans. IoT, as todays to emerging technology, that is focused on proficient monitoring and controlling various activities will have an impact on the human society including the daily life of the ordinary people. Ultimately, people might become part of the IoT through the specific devices like the medical implants, without even knowing that they have become part of this present technology.

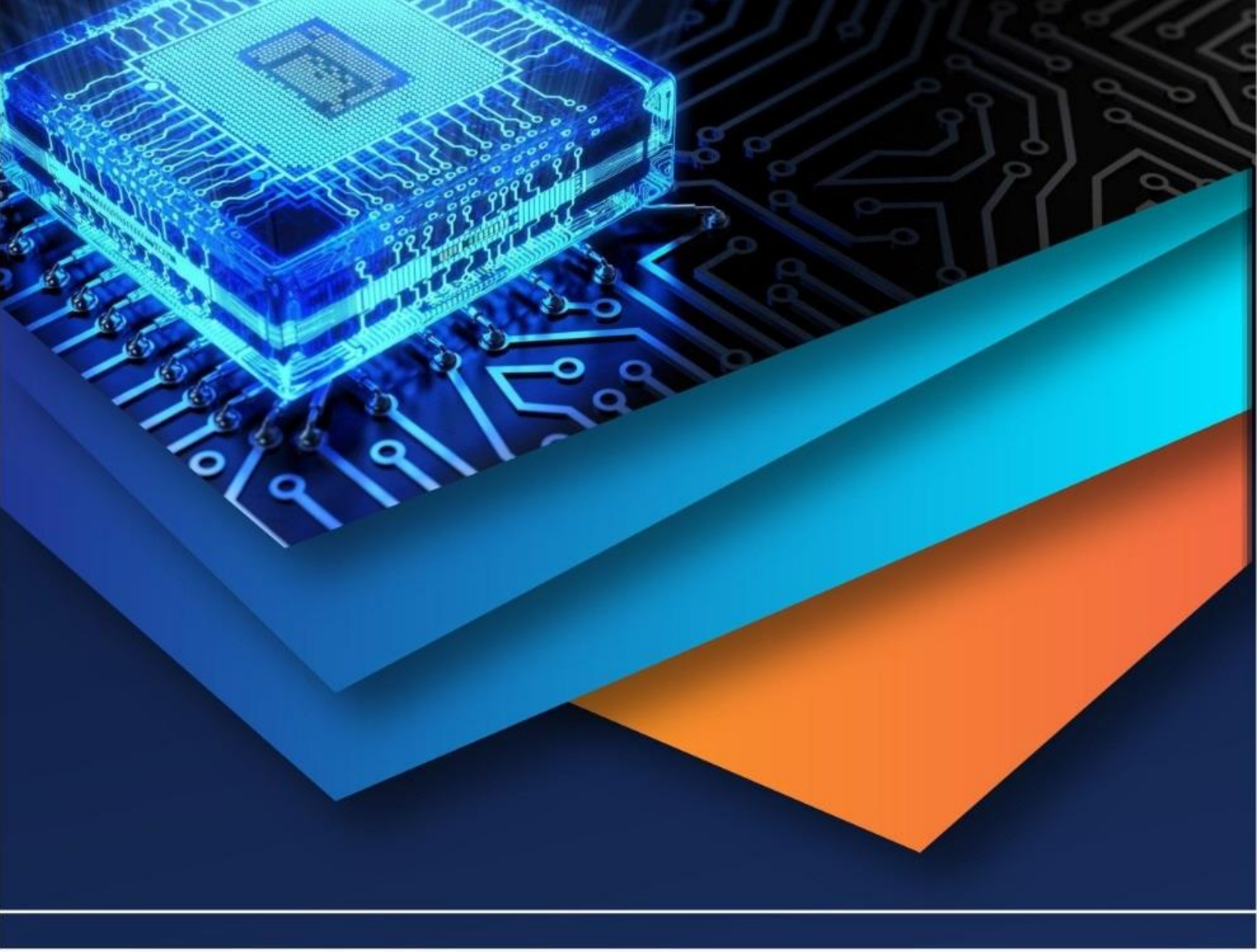
American paper, back in 1991. "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it".

VI. CONCLUSIONS

From this paper, we get an overview of how wireless sensors are integrated into the Internet of Things, the security challenges facing this as well as the security primitives that might be taken to protect the data of the sensors. The available approaches are focused on the pre-deployed pre-shared keys, on both ends whereas the certificate-based authentication is generally considered to be infeasible for the constrained resource sensors. Any unauthorized use of data or concerns on privacy may become a restriction to people in the utilization of applications that are IoT-based. Peer authentication and protection of data are critical requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating activities. Besides, other challenges need to be solved if there is integration of the sensor nodes into the infrastructure of the internet and the complete integration of the sensor networks and the internet still remain as an open issue. Distribution of secret key for the heterogenous sensors in the IoT becomes a challenge due to the inconsistencies in the cryptographic primitives as well as the computational resources of the various applications. Highly constrained sensors are not able to provide sufficient resources that are required for the heavy computational operations. The paper analyzes the interactions between sensor networks and the internet from the security point of view of identifying both the challenges to security and the primitives.

REFERENCES

[1] Nacer Khalil, Mohamed Riduan Abid, Driss Benhaddou, Michael Gerndt, (2014) “Wireless Sensors
[2] Networks for Internet of Things”, IEEE Ninth International Conference on Intelligent Sensors, Sensor
[3] Networks and Information Processing (ISSNIP) Symposium on Public IoT
[4] Jameson Berkow (2011) “Is the Internet leaving humanity behind?” Financial post
[5] Muhammad A. Iqbal, Dr. Magdy Bayoumi (2016) “Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IoT” The 2016 IEEE International Conference on High Performance Computing and Simulation (HPCS 2016) Innsbruck, Austria
[6] “Internet of Things: An overview by Internet Society” https://www.internetsociety.org/sites/ default/files/ISOC-IoT-Overview- 20151014_0.pdf
[7] Kashyap Kompella, “A Guide to the Internet of Things”
[8] Azmi Jafarey, “The Internet of Things & IP Address Needs”
[9] Phillip Howard, (January 2015) “The Internet of Things Reference Model” Bloor
[10] Therese Sullivan, (November 2014) “The Cutting-Edge of IoT, how does the IoT really change the future of commercial building operations?” Automated buildings
[11] Jim Duffy, (January 2016) “AT&T allies with Cisco, IBM, Intel for city IoT” Network World International Journal of Computer Networks & Communications (IJCNC) Vol.8,
No.6, November 2016 37.
[12] Bruce Ndibanje, Hoon-Jae Lee, and Sang-Gon Lee, “Security Analysis and Improvements of Authentication and Access Control in the Internet of Things”.
[13] Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman, “Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?” University of Malaga, Spain
[14] Securing the Internet of Things: A Proposed Framework by Cisco.
[15] White Paper Internet of Things Intel Corporation (2014). “Developing Solutions for the Internet of Things”
[16] Intel corporations, USA. Intel® Gateway Solutions for the Internet of Things.
[17] D. E Vans, (2011)“The Internet of Things: How the Next Evolution of the Internet is Changing Everything”, Cisco Internet Business Solutions Group (IBSG).
[18] H. Shafagh and A. Hithnawi, “Poster Abstract: Security Comes First, A Public-key Cryptography Framework for the Internet of Things”, 2014 IEEE International Conference on Distributed Computing in Sensor Systems, (2014), pp. 135-136.
Muhammad A. Iqbal, Dr. Magdy Bayoumi, (2016) “A Novel Authentication and Key Agreement Protocol for Internet of Things Based Resource-constrained Body Area Sensors” The IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) 2016 Vienna, Austria



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY