Available online at www.worldscientificnews.com

World Scientific News

An International Scientific Journal

WSN 41 (2016) 83-91 EISSN 2392-2192

Study: Protocols and Challenging Issues in IoT

G. Bhavani*, S. Sangeetha, S. Sivakumari

Department of Computer Science and Engineering,
Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India

*E-mail address: bhavanigb16@gmail.com

ABSTRACT

The aim of Internet of Things (IoT) is to enable the integration and interconnection of the existing physical components, internet and the people. This paper deals with the different protocols and its related challenges and its security issues in IoT. This paper is a general study of the protocols present in the Internet of Things along with an analysis of the challenges and security issues that an end-user shall face as an effect of the spread of IoT. The major of the study concentrates on the protocols, its challenging areas and also the security and privacy issues on the Internet of Things. No corrective action had been proposed for the security drawbacks have been examined in the paper.

***Keywords*:** IoT, MQTT, XMPP, DDS, AMQP, Security, Privacy

1. INTRODUCTION

The Device to Device (D2D) communication technology of the Internet of Things (IoT) explains the concept of free flow of information in the various embedded computing devices using the internet. The term "Internet of Things" aims at providing advanced mode of communication between the different systems and devices as well as facilitating the interaction of humans with the virtual environment. The Internet of Things with all its advanced capabilities in the information exchange area is a flawed concept from the security viewpoint and proper steps has to be taken in the initial phase itself before going for further development of IoT for an effective and widely accepted adoption.

(Received 01 February 2016; Accepted 10 February 2016; Date of Publication 11 February 2016)

2. PROTOCOLS IN IOT

In a system all the devices must communicate with each other (D2D). The data from a device should be collected and sent to the infrastructure on the server (D2S) which in turn has to share device data (S2S), by providing it back to devices, to analyze programs, or to the people.

- MQTT: a protocol for Device-to-Server communication (D2S)
- XMPP: a protocol for a special case of the D2S pattern, to connect people to the servers
- DDS: a bus for Device-to-Device communication (D2D)
- AMQP: a queuing system for Server-to-Server communication (S2S)

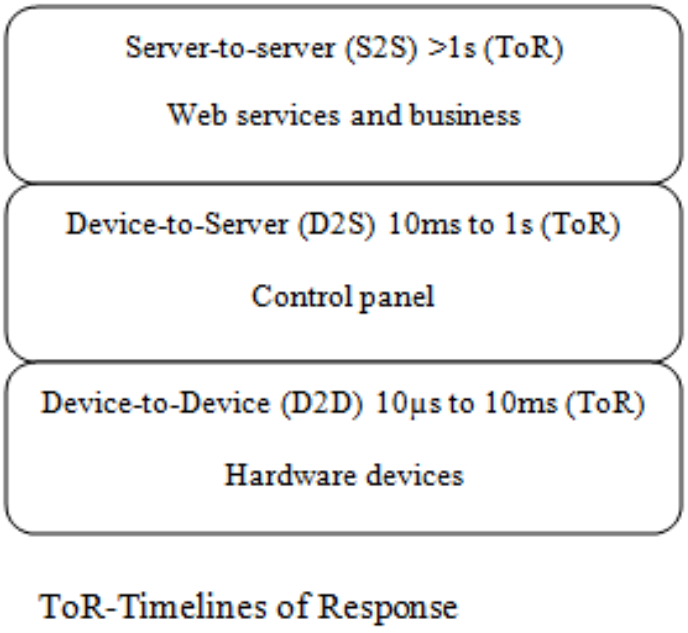


Fig. 1. IoT protocols with respective response time

2. 1. MQTT

Message Queue Telemetry Transport (MQTT) targets device data collection. Its main purpose is telemetry (remote monitoring). It collects data from many devices and transports that data to the IT infrastructure and targets large networks of small devices that need to be monitored or controlled from the cloud.

MQTT enables Device-to-Server (D2S) transfer that has a simple, clear and compelling single application, which offers clear control options. A hub-and-spoke architecture is natural for MQTT. Since the IT infrastructure uses the data, the entire system is designed to transfer data into enterprise technologies like ActiveMQ and Enterprise Service Buses (ESBs) in an easy manner.

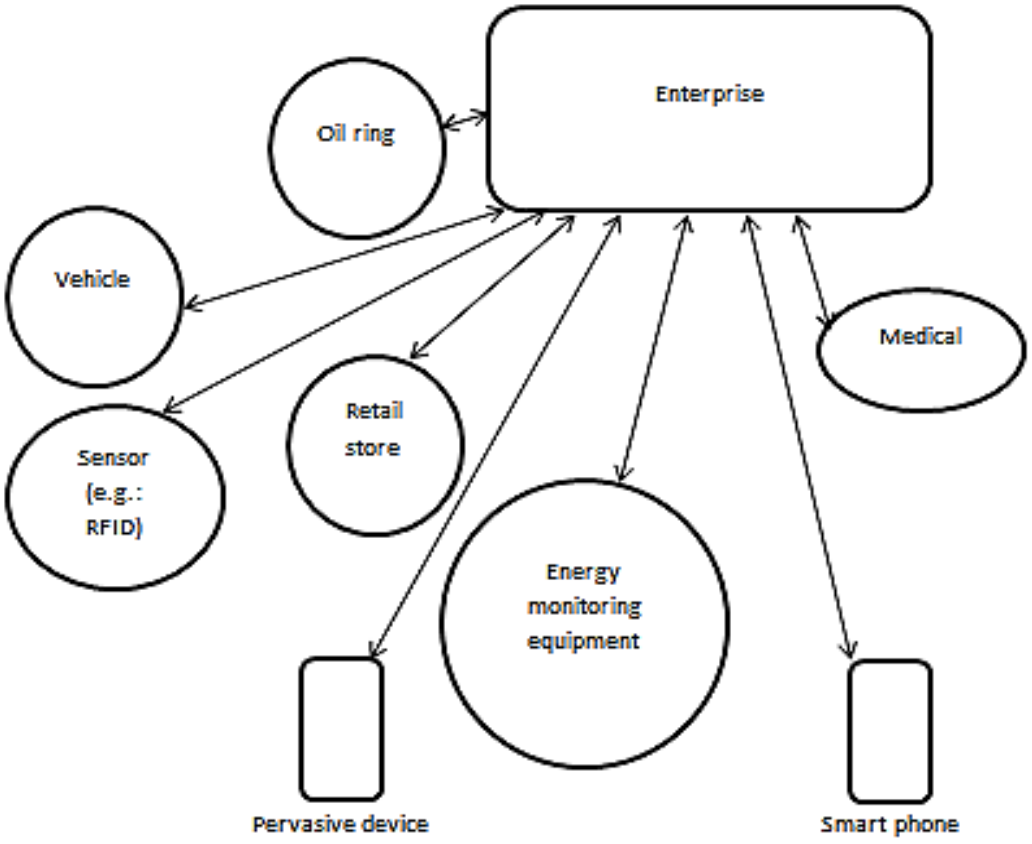


Fig. 2. Message Queue Telemetry Transport (MQTT) implementing a hub-and-spoke system

The Fig. 2 is an application for MQTT for monitoring a huge oil pipeline for leaks. The sensors analyses a location. The system identifies the problem and performs action to rectify that problem. MQTT can be applied to power usage monitoring, lighting control, and even intelligent gardening that shares a need for collecting data from many sources and making it available to the IT infrastructure.

2. 2. XMPP

eXtensible Messaging and Presence Protocol (XMPP) was developed for instant messaging (IM) to connect people to other people via text messages. XMPP provides a great way to connect a home thermostat to a Web server so one can access it from one phone. Its strengths in addressing, security, and scalability make it ideal for consumer-oriented IoT applications.

XMPP uses the XML text format as its native type, making person-to-person communications natural. XMPP runs over TCP, or over HTTP on top of TCP. The key strength is a <name@domain.com> addressing scheme that helps connect the needles in the huge Internet haystack. XMPP offers an easy way to address a device. It is not designed to be fast. Most implementations use polling, or checking for updates which is done only on demand. The "real time" to XMPP is on human scales, measured in seconds.

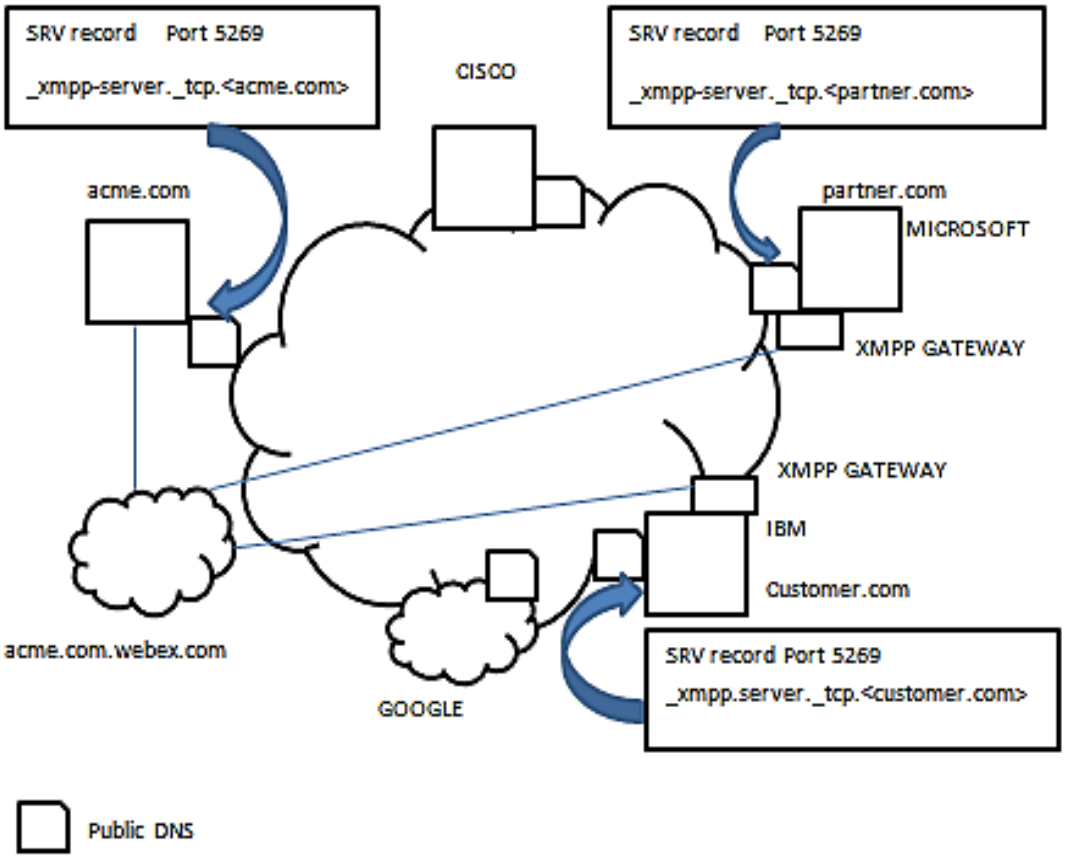


Fig. 3. The Extensible Messaging and Presence Protocol (XMPP) provides text communication between points

XMPP provides a great way, for instance, to connect one home thermostat to a Web server so one can access it from one phone. Its strengths in addressing, security, and scalability make it ideal for consumer-oriented IoT applications.

2. 3. DDS

The **Data Distribution Service** (DDS) targets devices that directly use device data. It distributes data to other devices (Fig. 5). The aim of DDS is to establish connection between devices. It is data-centric middleware standard with origin in high-performance defense, embedded, and industrial applications. DDS can efficiently deliver millions of messages per second towards many simultaneous receivers.

The data demands in devices are very different. The performance of devices is fast. DDS are measured in microseconds. DDS provides multicast, configurable reliability, detailed quality-of-service (QoS) control and pervasive redundancy. DDS provides efficient methods to filter and select accurately which data goes where. Lightweight versions of DDS are used for small devices in constrained environments.

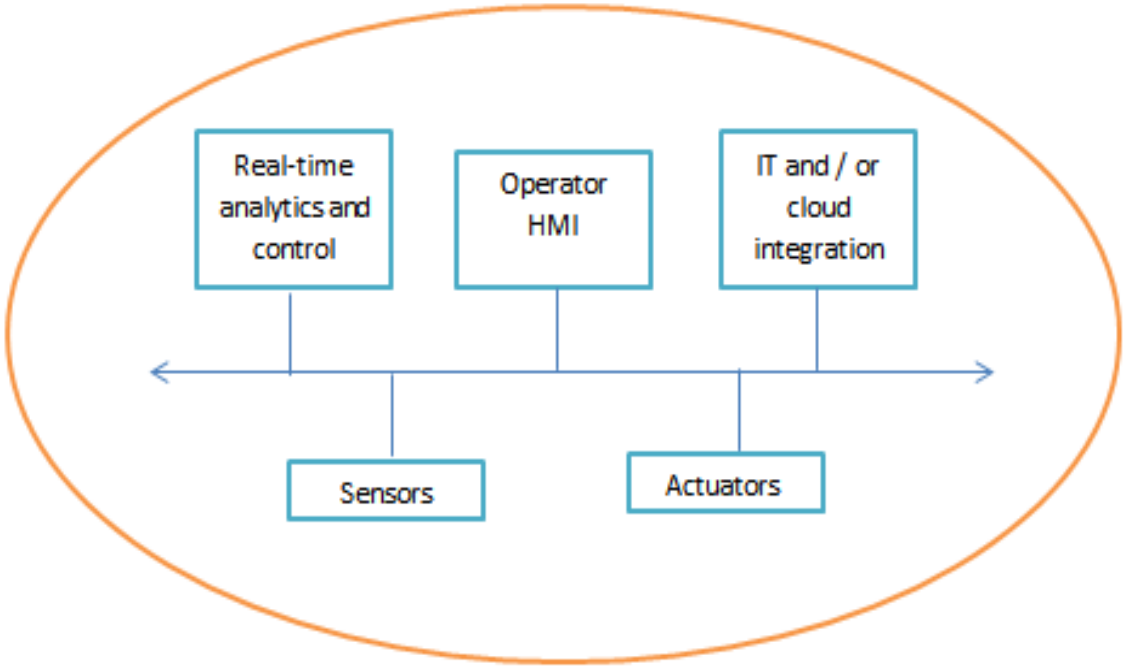


Fig. 4. Data Distribution Service (DDS) implements a publish/subscribe architecture

DDS implements direct bus communication between devices with the presence of a relational data model. The direct bus is a database as it is the networking, analog to a database. The high-performance devices should work together as one system in order to store the data in an efficient database. DDS delivers the reliability, flexibility, and speed necessary to generate real-time, complex applications. Applications include wind farms, military systems, medical imaging, hospital integration, asset-tracking systems, and automotive test and safety.

2. 4. AMQP

The **Advanced Message Queuing Protocol** (AMQP) is all about queues *(Fig. 5) that* sends transactional messages between servers. It is a message-centric middleware that is developed from the banking industry that can process thousands of reliable queued transactions.

AMQP is mostly used in business messaging. It usually defines “devices” as mobile handsets communicating with back-office data centers. AMQP is best suitable for the server-based analysis functions or control plane.

AMQP focuses on the message transaction without any loss of data. Communications from queues to subscribers use TCP and from the publishers to exchanges which provides strictly reliable point-to-point connection. The endpoints must acknowledge acceptance of each message. The standard also describes an optional transaction mode with a formal multiphase commit sequence. AMQP middleware focuses on tracking all messages and verifying every message is delivered as intended, without any failures or reboots.

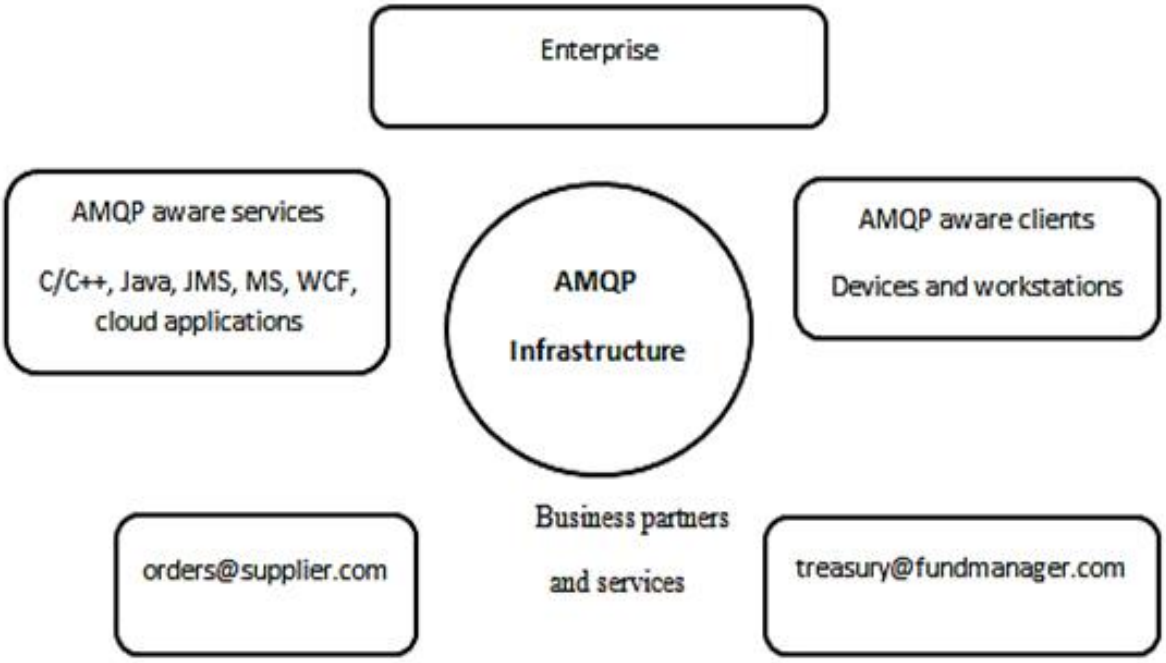


Fig. 5. The Advanced Message Queuing Protocol (AMQP) from the banking industry

3. CHALLENGING AREAS

3. 1. Security: IoT connects more devices and transfers the entry points for malware. Less expensive devices are more subject to tampering. API and Machine-to-Machine communication, Integration middleware, more layers of software, creates more complexity and new security risks.The booting of security is done when the integrity and authenticity of the software on the device is verified using cryptographically generated digital signatures.

3. 2. Trust and Privacy: A core use case for the IoT is monitored with remote sensors that will be heightened for sensitivity to controlling access and ownership of data. Compliance will continue to be a major issue in medical and assisted-living applications, which could have life and death issue. New compliance frameworks to address the IoT's unique issues will evolve. Social and political concerns in this area may also hinder IoT adoption.

3. 3. Complexity, confusion and integration issues: The IoT system with multiple platforms, numerous protocols and large numbers of APIs lacks in integration and testing which leads to confusion around evolving standards. Reduced adoption and unanticipated development resource requirements will result in slip schedules and slow time to revenues will require additional funding for IoT projects and longer runways for startups.

3. 4. Evolving architectures, protocol wars and competing standards: The IoT with many players are bound to be ongoing conflict as legacy companies seek to protect their corrective system's merits and open systems supporters try to set new standards. There may be multiple standards that evolve based on different requirements determined by device class, power

requirements, capabilities and uses which presents opportunities for platform vendors and open source advocates to contribute and influence future standards.

3. 5. Concrete use cases and compelling value propositions: Lack of clear use cases or strong Return On Investment examples will reduce adoption of the IoT. Although technical specifications, theoretical uses and future concepts may suffice for some early adopters, mainstream adoption of IoT will require well-grounded, customer-oriented communications and messaging around "what's in it for me." Detailed explanations of a specific device or technical details of a component won't cut it when buyers are looking for a "whole solution" or complete value-added service. IoT providers will have to explain the key benefits of their services or face the proverbial "so what."

3. 6. Access control: Different forms of resource and access control are applied. Role-based access controls are developed into the operating system limit the privileges of device components and applications so they access only the resources they need to do their jobs. If a component is proved to be compromised, then the access control ensures that the intruder has as minimal access to other parts of the system. Device-based access control mechanisms are analogous to network-based access control systems like Microsoft Active Directory.

3. 7. Device authentication: The device authentication is plugged into the network, which authenticates itself prior to receiving or transmitting data. The user authentication permits a user to access a corporate network based on user name and password, machine authentication allows a device to access a network based on a similar set of credentials that has been stored.

3. 8. Firewalling and Intrusion Prevention System: The device requires a firewall in order to control traffic that is destined to end at the device. The embedded devices should have unique protocols, which should differ from enterprise IT protocols. The smart energy grid acquires its own set of protocols assessing the devices talk to each other. Industry-specific protocol filtering and deep packet inspection capabilities are required to identify malicious payloads hiding in non-IT protocols.

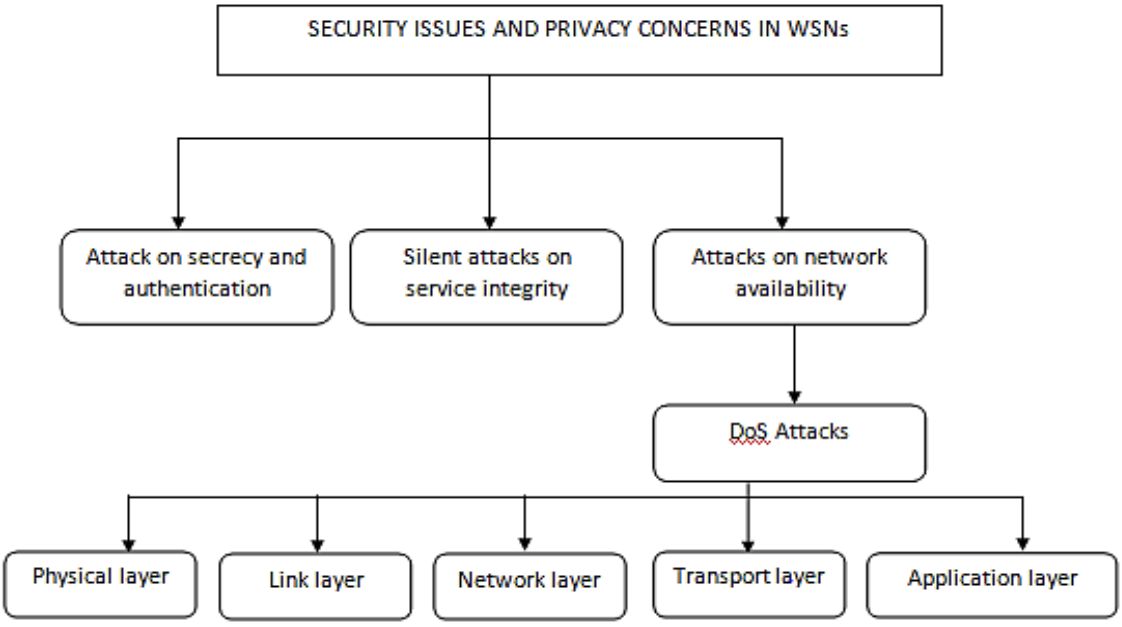
3. 9. Updates and patches: The device in operation should receive hot patches and software updates. The operators should roll out patches and authentication should be provided by the devices which should consume lesser bandwidth or impair the functional safety. The software updates and security patches must be delivered in a way that conserves the intermittent connectivity and limited bandwidth of an embedded device and exactly eliminates the possibility of compromising functional safety.

4. SECURITY AND PRIVACY ISSUES

Gartner's views on IoT Challenges:

- **Security:** Increased digitization and automation creates new security disquiet
- **Enterprise:** Security issues could pose safety risks
- **Consumer Privacy:** Potential of privacy contravention
- **Data:** Lots of data will be generated, both for big data and personal data

- **Storage Management:** The cost-effective data should be identified by the industries
- **Server Technologies: The investments** should be increased
- **Data Centre Network:** Human interface applications are optimized by WAN links, in which IoT is expected to create pattern change by automatic data transmission.



5. CONCLUSION

In this paper, we have studied all the protocols and its associated challenges in Internet of Things. The four protocols outlined here vary with techniques which are categorized based on Quality of Service, addressing, and application. QoS control represents data delivery flexibility in which the complex QoS system may be harder to implement, but it solves more application based demands. These protocols are critical to the rapid evolution of the IoT. The Internet of Things is a big place, with room for many protocols. In the conclusion, the study of the protocols and the challenging issues results in choosing the efficient and effective protocols for the future work.

References

[1] Borgohain, T., U. Kumar and S. Sanyal. Survey of Security and Privacy Issues of Internet of Things. ArXiv abs/1501.02211 (2015): n. pag.

[2] Stan Schneider, Understanding The Protocols Behind The Internet Of Things, 2013. https://www.electronicdesign.com/technologies/iot/article/21798493/understanding-the-protocols-behind-the-internet-of-things

[3] Chris Kocher, Gray Heron, The Internet of Things: Challenges and Opportunities, 2014. https://sandhill.com/article/the-internet-of-things-challenges-and-opportunities/

[4] Singla, Aashima, R. Sachdeva and S. Guru. Review on Security Issues and Attacks in Wireless Sensor. (2013). Corpus ID: 14492338

[5] Sen, Jaydip. Security and Privacy Challenges in Cognitive Wireless Sensor Networks. Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks, edited by Natarajan Meghanathan and Yenumula B. Reddy, IGI Global, 2013, pp. 194-232. http://doi:10.4018/978-1-4666-4221-8.ch011

[6] J. Sen, A Survey on Wireless Sensor network Security. *International Journal of Vommunication Networks and Information Security* Vol 1, No 2, pp. 55 - 78, August 2009. arXiv:1011.1529