International Journal of Information System Modeling and Design
Volume 9 • Issue 3 • July-September 2018

A Survey, Design and Analysis of IoT Security and QoS Challenges

M Kesavan, Research Scholar, SITE, VIT University, Vellore, India
J Prabhu, VIT, Vellore, India

ABSTRACT

IoT is a technological exemplar with a vision of "Everything is connected" enabling everyone to publish their generated data collected from different heterogeneous and homogenous systems onto the web. The basic concept of IoT is connectivity, a set of physical objects that use network support to exchange data. These objects can be software, boards, sensors, etc. In the real end to end network deployment, IoT is a platform and cloud is one part of it. In order to turn the IoT vision into reality high reliability, security and QoS are required to support the communications between the homogenous and heterogeneous networks. The security and QoS are critical factors in the real End to End topology. In this article, the authors proposed the various challenges for IoT security, and IoT routing between the edge and cloud.

KEYWORDS

Integration, Interoperability, Quality of Service [QoS] Cloud, Security

1. INTRODUCTION

Internet plays a very important role for the devices to communicate with the help of protocols. In recent technological fields, Each IoT devices has unique identity and unique Identifier (Ip address and Url). Most of the IoT devices has an interface allows users to query the devices, monitor and control them remotely (Weber, 2010). These devices communicate to the other smart things wirelessly thus connecting them to internet and making them establish their ID and identifier status on the web. Eventually an IoT is formed, which is in turn used as an IoT application by human users. These devices can be used as tool for tracking, observing and influencing the real world. Miniatures of these devices are created and attached to other objects such as people, desk are rooted into places like home, office etc. A wireless network of these devices are formed. A good example is RFID tags.

The entity is brought from origin to a destination by routing the packets without losing the Integrity. These devices can either be an IoT or an Internet device. This approach involves routing and better security in the layers.

1.1. Background of IoT

The IoT is simply the network of interconnected things which are embedded with sensors, software, and network connectivity and embedded devices that enable them to collect and exchange data making them accessible over the Internet. IoT brings useful applications like home automation, smart health monitoring, security, automated devices monitoring and management of daily tasks. Every sector like Energy, Computing, Management, Security and transportation are going to be benefited with

DOI: 10.4018/IJISMD.2018070103

this new paradigm (IEEE Internet of Thing Journal Evaluating critical security issues of the IoT world: Present and Future challenges of IoT, n.d.). Development of sensors, actuators, smart phones, RFID tags makes it possible to materialize IoT which interact and co-operate each other to make the service better and make accessible at any time, from anywhere using any network. Wireless sensor technology allows objects to provide real-time environmental information and context. IoT allows objects to become more intelligent which can think and communicate among them.

As the number of devices connected to the internet is growing in rate, the concept of IoT has gained power. Survey has revealed that there will be billions of devices connected to IoT serving various purposes in day to day life (Al-Fuqaha et al., 2015). This results in development of applications in various domains, whereas the application depends on QoS requirements.

The QoS requirements classified are Best effort, Differentiated services and guaranteed services. The guaranteed services known as hard QoS should use suitable mechanism at each layer of IoT architecture. A delay in any layer could lead to unacceptable QoS, in order to provide guaranteed services it is important to know QoS has been addressed properly at each layer (Ahsan et al., 2016).

In the real deployment, IoT is connected to different backend systems with different Vendors. Due to high heterogeneity and scalability upgrading the devices for various Malware, virus scanning, and software Functionality is highly challenging. Numerous vendors and integrators likely would be involved over the lifetime of the device, requiring a collaborative mix of standards-based, proprietary and open-sourced components (Stoimenovic & Wen, 2014; Qu &Chan 2016).

As a result, security solutions for the devices are indeed with strong hardware-based security, and legacy devices should be protected behind purpose-built gateways (Khari et al., 2016).

Also, there is no single, perfect level of security. Various devices at different companies have varying risk profiles. Creating just the right security level is achievable, through evaluating the risk, use and capability of every device. IoT security focus is more on data than the device. Due to immense use and importance of the Internet of Things, it has become paramount to secure it. IoT security is so critical because private information could be stolen from the use of connected devices.

2. ANALYSIS ON IOT

As mentioned in the introduction, the IoT is nothing but devices communicate through the internet when they are enabled and don't communicate if they are disabled. Example: Smart TV, Online games through computer/Xbox etc. The best example of this is the RFID tags, which enables each device to communicate with each other over any network connectivity altogether resulting in exchange of information in a better and smarter manner (Al-Fuqaha et al., 2015).

IOT has given a concept of Machine to-Machine (M2M) communication. Implementing strategy to capitalize on the Internet of Things so that you can just stop your business and starts making it thrive. IOT is going to have huge impact on home automation and building automation system where every convenience will be taken care of by the interconnected devices on IOT.

The major characteristics of IoT objects are to sense, tiny in size, limited capability, and limited energy, connected to the physical world, intermittent connectivity and mobility, managed by devices and not by People (Aljawarneh, 2012).

2.1. IoT Architecture

There is no single agreement on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers (Gubbi et al., 2013; Han et al., 2016; Hao, 2015) based on the use cases. Earlier researchers identified the three layer architecture as key for the Internet of Things (Desai et al., 2015; Van der Veer & Wiles, 2008). When we deep dive for many user deployment, the IoT architecture is decoupled and the layers are well augmented for better understanding and requirements. This could be one of the reasons that the five layered architectures are proposed (IEEE Internet of Things Journal Evaluating critical security issues of the IoT world: Present and Future

challenges of IoT, n.d.) which furthermore includes the processing and business layers (Hussain, 2016; Aljawarneh, 2017).

1. Three layer Architecture
2. Five-Layer Architectures
3. Cloud and Fog Based Architectures

2.2. Three Layer Architecture

The three layers are Application, Transportation and perception as described in figure 1

1. To deal with the physical layer, the perception layer plays a key role. The sensors defined in this layer, will sense and gather information about the environment. This will basically identify other smart objects in the environment.
2. Interconnection of smart things, network devices and servers are achieved through the network layer. It also holds the responsibility of transmitting and processing sensor data.
3. All the specific services to the user are delivered by the application layer. Example deployments are Smart health and cities.

2.2.1. Five Layer Architecture

The five layers are perception, transport, processing, application, and business layers. The role of the perception and application layers is the same as the architecture with three layers. A swift of remaining layers can be defined as follows.

1. Transport layer grabs the sensor information (data) by following any of the below medium like Bluetooth, NFC, RFID, wireless and LAN from perception layer to the processing layer and vice versa.
2. As the name defines, processing layer holds the following responsibility- Store, Analyze and process massive amount of data from transport layer.
3. The layer holds the complete responsibility of user's privacy and profit model is completely managed by business layer and controls the whole IoT system.

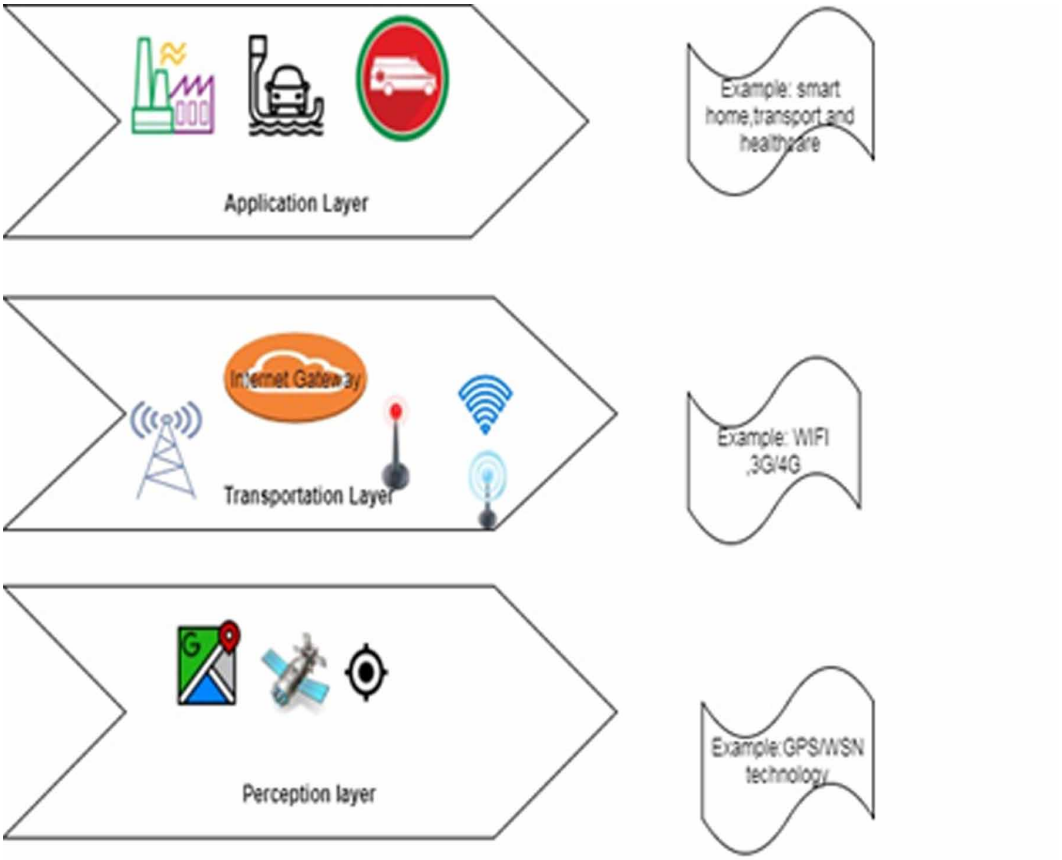
IoT uses the RFID readers/Sensors, which is an identification technique. This RFID/Sensors targets the devices and collects information through radio frequency (Aijaz et al., 2015; Pinto et al., 2017) and it uniquely identifies the object and collects the information. All these are done without human intervention.

IoT encompasses of several devices connected to each other, a uniform architecture should be maintained. Figure 1 represents the architecture of IoT, where it is classified into 2 tiers – edge and platform tiers. The gateway node connects the two dissimilar networks that exist between IoT and Internet devices (Ahsan et al., 2016).

2.2.2. Cloud and Fog Based Architectures

Based on the data generated by different IoT devices, we need some mechanism to preprocess the data. In some system architectures the data processing is done in a large unified fashion by cloud computers. Such a cloud centric architecture keeps the cloud at the center, applications above it, and the network of smart things below it (Stoimenovic & Wen, 2014). Cloud compromises lot of flexibility and scalability. It also supports for services such as the core infrastructure, platform, software, and storage. Developers can provide their storage tools, software tools, data mining, and machine learning tools, and visualization tools through the cloud.

Figure 1. Layers of IoT



The enhancement of cloud gave a new architecture namely; fog computing (Bonomi et al., 2014; Stoimenovic & Wen, 2014), where the sensors and network gateways do a part of the data processing and analytics.

2.2.3. Protocol Stack

The information is exchanged through layers as stated in Figure 1. The main layers are data link, network and application layer. The data link layer servers as medium for allocating channels for data transmission among smart devices. The best example of the IoT technology is ZigBee. The ZigBee technology (Sarkar & Kundu, 2016) is fast responsive when compared with Bluetooth.

In application layer, many new protocols are introduced to adapt with immense volume and large network of IoT devices. Machine-to-machine (M2M) communication Message Queue measure Transport (MQTT) is meant for IoT devices of little size that have low information measure, high cost, low process power and unreliable networks such they'll communicate cleanly among them.

The XMPP protocol is proposed (Ahsan et al., 2016) for communication in IoT world, precisely designed for instant messaging that are based on XML.

The interoperability is achieved between smart devices in IoT by using the Data-Distribution Service (DDS) protocol (Schoop et al., 2006). For IoT applications, this protocol offers great Performance and, Scalability.

2.2. IoT Protocols (Hussain, 2016)

The IoT protocols are listed in Table 1.

Message Queuing Telemetry Transport (MQTT) is a lightweight messaging protocol designed for sensor and wireless networks. The protocol is widely deployed for M2M (machine to machine) communication. It uses send or publish method. MQTT Performs well when there is bandwidth limitation.

Constrained Application Protocol (CoAp) is specifically designed for constrained (limited) Hardware. This protocol is widely used when the hardware doesn't support HTTP or Tcp/Ip. It is a lightweight protocol that needs low power IOT application like for communication between battery powered IOT devices. This also uses client-server architecture.

Extensible Messaging and Presence Protocol (XMPP) is an XML based messaging protocol. It was used in messaging, Presence, voice and video. XML is a markup language used for both human and machine readable. The use of XMPP for IOT allows real-time and scalable networking between devices or things.

Based on MQTT, Secure Message Queue Telemetry Transport (SMQTT) protocol is an encryption based light weight messaging protocol. It follows setup, encryption, publish and decryption. It works similar to MQTT, except both subscriber and publisher need to register with the broker using a secret master key for security purpose.

DDS - Designed by Object Management Group (OMG), This also works in MQTT pattern. Data Distribution Service is a M2M application layer protocol for real-time systems without any networking middleware.

AMQP - Like XMPP, Advanced Message Queue Protocol (AMQP) is also an open standard application layer protocol for message-oriented middleware. It is used for passing business messages between applications or organizations.

RPL is the distance vector routing protocol for Low Power and Lossy Networks developed in ROLL IETF Working Group - RPL Control Messages are used to build a network topology.

6LoWPAN is acronym that combines the latest version of the Internet Protocol (IPv6) and Low-power Wireless Personal Area Networks (LoWPAN). 6LoWPAN, therefore, allows for the smallest devices with limited processing ability to transmit information wirelessly using an internet protocol.

CRB-RPL: A Receiver-Based Routing Protocol for Communications in Cognitive Radio Enabled Smart Grid.

(LTE-Machine Type Communication) - Standards-based family of technologies supports several technology categories, such as Cat-1 and CatM1, suitable for the IoT.

LoRaWAN - Network protocol intended for wireless battery-operated Things in regional, national or global network.

Z-Wave It is a proprietary protocol, with two basic types of devices: controlling and slave devices. This is effective non-scale deployments and where the message seconds > 200 millesec or more.

3. CHALLENGES IN IOT

There are several challenges and research issues in IoT.

3.1. Heterogeneity

The major issue as well as the critical issue of IoT is heterogeneity of the devices. Unlike the traditional devices, the IoT devices are subjected to different conditions (Al-Fuqaha et al., 2015). The heterogeneity may be due to the below reasons.

Table 1. Protocols used in IoT

Application Layer	XMPP (Ungurean & Gaitan, 2015), CORE, AMQP (Iova et al., 2016), MQTT (Ghosh et al., 2010), HTTP, IFTF, SSH, CoAP (Whitmore et al., 2015), smqtt (Xu et al., 2016), dds (Shirgahi et al., 2017)
Network Layer	RPL (Pinto et al., 2017), 6LowPAN (Neiva et al., 2016), IPv4, IPv6 (Ungurean & Gaitan, 2015), 6TiSCH (Dandelski et al., 2015), CoRP CRB-RPL (Qu & Chan, 2016), IETF ROLL
Data Link Layer	LTE-A (Al-Fuqaha et al., 2015), 802.11g/ac/ad/ah (Ronen et al., 2017), NFC, ANT?, sIGfOX (Bonomi et al., 2012), LoRaWAN (Bonomi et al., 2014), 802.15.4, rfid, ble, z-Wave

1. Operative conditions: The detector devices operate in several conditions like- temperature, pressure, and voltage (Ahsan et al., 2016).
2. Functionality: The IoT devices could either deliver information sporadically or on demand basis (Aijaz et al., 2015).
3. Resolutions: The target of IoT devices could also be following, monitoring, actuating, etc.
4. Hardware platform: The hardware platform varies per their design and style. Supported this, the supporting in operation systems and applications also are different (Hussain, 2016), packet size, etc.
6. Implementations: Completely different programming languages are used to develop IoT applications using different operation systems, like Android, IOS, etc (Hussain, 2016).
7. Interaction modes: The interaction between IoT devices and also the remote user are often request/response or command type (Bravo & Velazquez, 2008).

As IoT deals with different applications and domain, adhering to single protocol isn't an easy task in IoT, Hence the concept of interoperability has come into picture to handle the heterogeneity.

3.2. Interoperability (IoP)

As said earlier there are several devices in different technologies which does not communicate in the same way as the conventional computer devices does it.

We have different levels of interoperability like Devices/connectivity, platform and Services.

Consider the smart home system, in which all lights, ovens, washing machines/dryers are connected and controlled through internet/web interface (Bravo & Velazquez, 2008). An addition of any of new device from different vendor should not affect the entire set up.

The devices which are heterogeneous in nature should be able to communicate with each other and work together and this is achieved by integration of IoT system. Because of the interoperability issues still 60% of the system faces IoP issues. These various categories of IoP issues are provided in the IoT context (Pinto et al., 2017).

The various interoperability issues which has to be addressed for seamless communication (Asuncion & Van Sinderen, 2011)

1. Technical Interoperability: When communication technologies and protocols used for exchange of information are incompatible, technical interoperability results. This can help only in low level information exchange.
2. Syntactic Interoperability: This results when information and knowledge are represented by different structures by different people or systems.
3. Semantic Interoperability: It deals with different meaning of the same content which is being exchanged. It deals with human rather than the system. It is the most important barrier as it involves in the exchange of information and this info doesn't have defined semantics.
4. Pragmatic Interoperability: The rapidity in the messages which is exchanged between the sender and receiver is explained here. The Pragmatic interoperability is still largely disconcerted, as

defined by the proposed definitions (Al-Fuqaha et al., 2015; Aljawarneh, 2012; Van der Veer & Wiles, 2008)

5. Organizational Interoperability: Lacks in exchanging information among organization when they have wide variety of information over different system, this interoperability come into picture. This ensures that all the industries are organized in same pattern.

Achieving IoP among all the heterogeneous devices across completely different communication technologies is indispensable. Some attainable approaches are mentioned below (Ahsan et al., 2016).

1. Protocol Version: The proprietary protocols are converted to TCP/IP and vice versa using the gateway because of its low complexity and its low cost. Since there is no common standards protocol translation are isolated in IoT applications.
2. IPV6 over WSN: WSN can use IPv6 by squashing the header and using the stateless auto-configuration of IPV6. As IoT things have size variants, further inputs are required to make the protocol stack adaptable to the devices.
3. Using Device Ontology: Ontology helps in sharing the common understanding of the structure of information among people. It also provides Meta information, knowledge and information about the devices. Devices might not adapt to the ontology as they have different context.
4. Web of Things (WoT): The client can access any device in the network as they run a web server. The main cons of this is that, they are user-centric i.e., the device actions is always originated by users.
5. Service Oriented Middle-ware (SOM): Here services are the data generated from the device. Creator and end user interaction is done by the registry.
6. Designing a Generic Protocol Stack: By combining all the low power technologies a protocol stack can be designed. This stack can provide interoperability at different aspects. The aspect are the physical and application integration which is for interconnecting the devices and executing different applications in tandem respectively.

3.3. Scalability

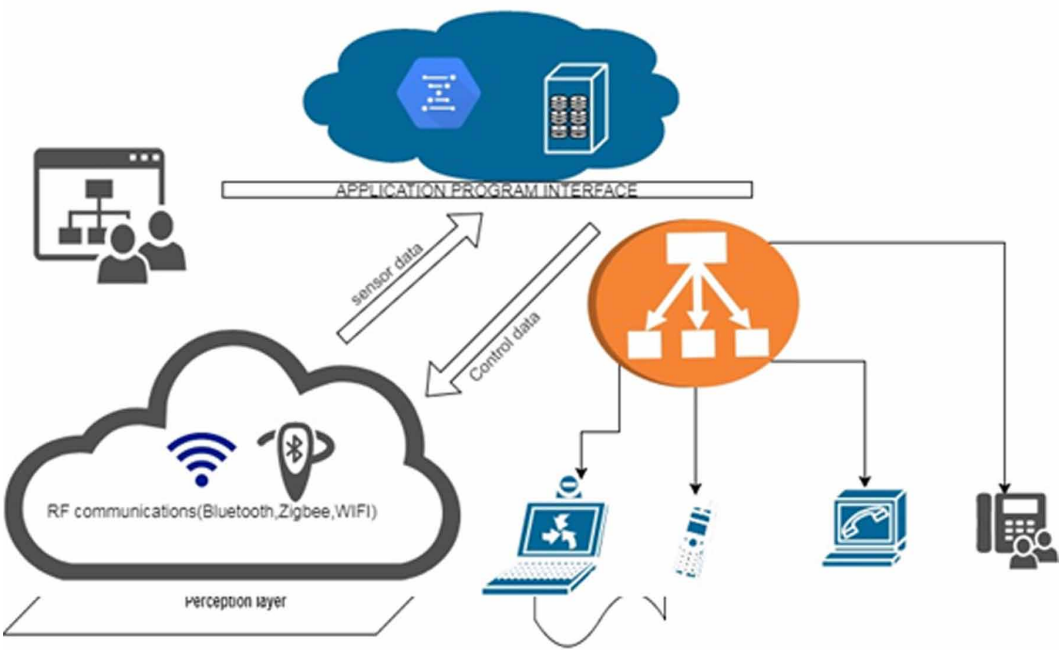
Scalability is the best option to handle the fiery growth. Figure 2 represents the relative growth of components to the growth of nodes. Scalability is the ability of a device to adapt to the changes in the environment and meet the changing needs in the future. It is essential feature of any system which has the capability to handle the growing amount of work. It is a desirable attribute of a system or a network whose lack can cause a poor system performance and the necessity of reengineering of the whole system. The IoT applications should be capable to hold up increasing number of devices without any deprivation in the QoS (Hussain, 2016). Also, the number of resources is proportional to the number of devices increasing, as we need resources to manage these devices

We have two types of scalability, vertical and horizontal scalability

3.3.1. Vertical Scalability

It is also referred to as scaling up which is the ability to increase the capacity of existing hardware or software by adding more resources to it. For ins1.tance, we add processing power to a server to increase its speed. Moreover, we can scale a system vertically by expanding it by adding more processing, main memory, storage, and network interfaces to the node in order satisfy more requests per system. Hosting services companies surmount by increasing the number of processors. It means to add resources to a single node in a system which involves the addition of CPUs or memory to a single computer (Ahsan et al., 2016). Such vertical scaling of current systems facilitates them to utilize virtualization technology more productively.

Figure 2. Nodes in scalability



The main advantage of vertical scalability is that it consumes less power if we compare to running multiple servers, reduces administrative efforts as we need to handle and manage only one system (Hussain, 2016). Moreover, the implementation is easier, reduces software costs and application compatibility is retained. As there are advantages there are also disadvantages to this type of scaling which include greater risk of hardware failure which will cause bigger outages, severe vendor lock in and the cost of the overall implementation is high (Hao, 2015; Bonomi et al., 2012; Ahsan, 2016).

3.3.2. Horizontal Scalability

It is also referred to as scaling out which is the ability to increase the capacity by connecting the multiple hardware or software entities so that they can work together as a single unit. Horizontal scalability can be achieved by adding more machines (Kaur & Mir, 2015) into the group of resources and adding more nodes to a system for instance adding a new computer to a distributed software application.

The examples of this can be SOA systems and web servers which scale out by adding more and more servers to the load-balanced network so that the incoming requests can be distributed between all of them. Cluster is a familiar term for describing a scaled-out processing system.

3.4. Cloud and Server Platform

The amount of connections and data produced by the devices are proportional to the increase of the devices. Handling the massive growth of devices along with the connections and data is a big hurdle. Some of the solutions of IoT are openIoT, Compose, Clout and Kaa (Shirgahi et al., 2017; Karnouskos et al., 2014; Qin et al., 2016).

Different approaches are adopted to augment scalability can be listed as follows

1. Proper scheduling mechanisms should be developed to handle the reliability issues. The services in a cloud should take the responsibility to enable automated bootstrapping, registration, monitoring, and upgrade.

2. Data processing pipeline: This technique is needed to collect, clean, enrich and change on streaming data

Scalability of IoT can be achieved by breaking the application into multiple autonomous functional units. Multiple data storage units have to be adopted. The database technology should be tied with analytics algorithms.

3.5. Network and Communication Protocol

In the IoT communication there may be transmission occurring between thousands of devices. Many devices may connect to a single network for a special purpose. Networking and communication with insufficient channel band is exigent (Pinto et al., 2017). Different strategies for providing scalability are

1. New modulation and coding patterns are mandatory for refining network capacity.
2. MAC protocols should be able to take control over the argument and collision over the public wireless medium.
3. Finally comes the addressing scheme IPV4 and IPV6 which are distinctive. IPV4 has been switched to IPV6 due to the limited address space. IPV6 can give unique routable address.
4. The next aspect of provisioning scalability is to control the protocol overhead as the network size and the physical layer capacity increases.
5. The devices are limited in nature and it is very vital that the protocols are optimized to munch through very low power (Neiva et al., 2016; Pinto et al., 2017).
6. Redundant data is dealt with the help of data aggregation. It combines all the superfluous and interrelated data into valid high-quality information which is in turn transmitted to the sink through the intermediate nodes. This can reduce the repetitive routes (Hussain, 2016).

3.6. Security and Privacy

Security and Privacy is the most important aspect in IoT as the devices are connected globally and accessibility is provided to anyone. The security architectural diagram for the End to End flow is referred as below in Figure 3.

Information can be taken by anyone and this has to be restricted. Also, these devices are more prone to intruders. The communication will happen through radio waves which is another advantage for intruders. The real complexity in IoT arises, when exchange of information happens on heterogeneous devices which are geographically separated.

Also cloud computing (Chen et al., 2006) plays a role in information leakage. As a result, there is an increased demand in security and privacy techniques to ensure the info exchanged are less prone to vulnerability.

3.6.1. Security Challenges in IoT Deployment

According to standard IoT Architecture (Ghosh et al., 2010; Gubbi et al., 2013; Han et al., 2016) we have 3 layers Perception, Transportation and application layer. Figure 4 shows the security attacks in IoT layers.

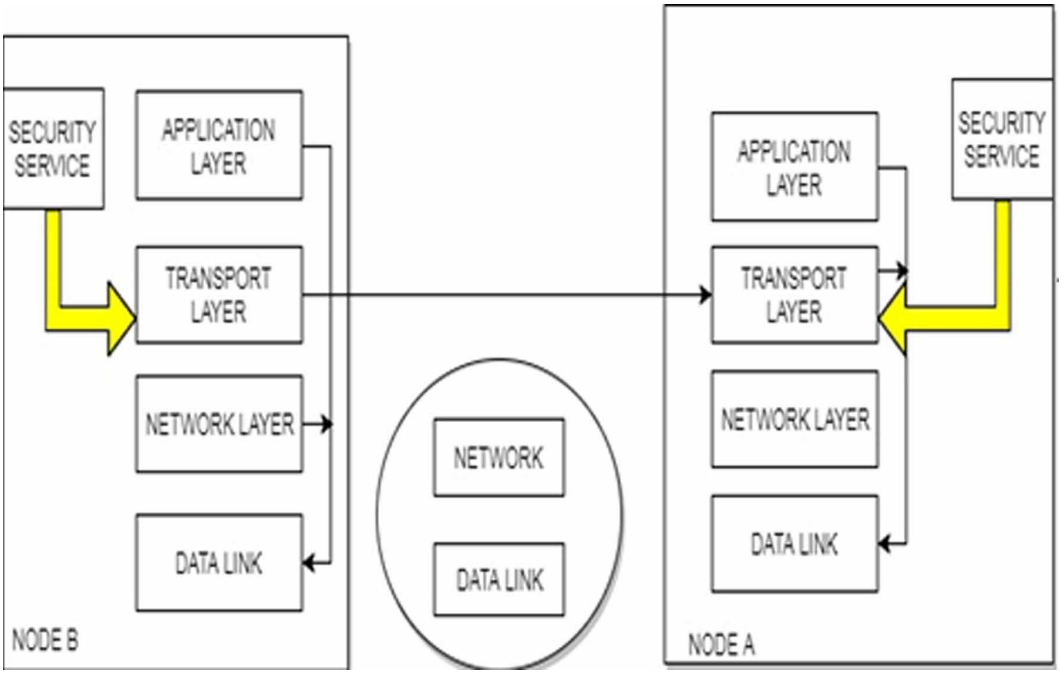
3.6.2. Requirements in Security for IoT

For a protected IoT deployment different systems and parameters should be figured with as portrayed underneath.

3.6.3. Integrity, Data privacy and Confidentially

As IoT information goes through numerous paths in a system, a legitimate encryption component is required to guarantee the classification of information, because of a various reconciliation of

Figure 3. Architectural diagram for end to end flow (Pinto et al., 2017)



administrations. The IoT gadgets vulnerable to assaults may cause an aggressor to affect the information honesty by altering the put away information for pernicious purposes.

3.6.4. Authentication, Authorization, Accounting

The decent variety of validation components for IoT exists chiefly due to the differing heterogeneous fundamental designs and situations which bolster IoT devices. A channelized deployment of authorization and authentication results in a reliable/Trust worthy environment which ensures a secure environment for communication.

3.6.5. Energy Efficiency

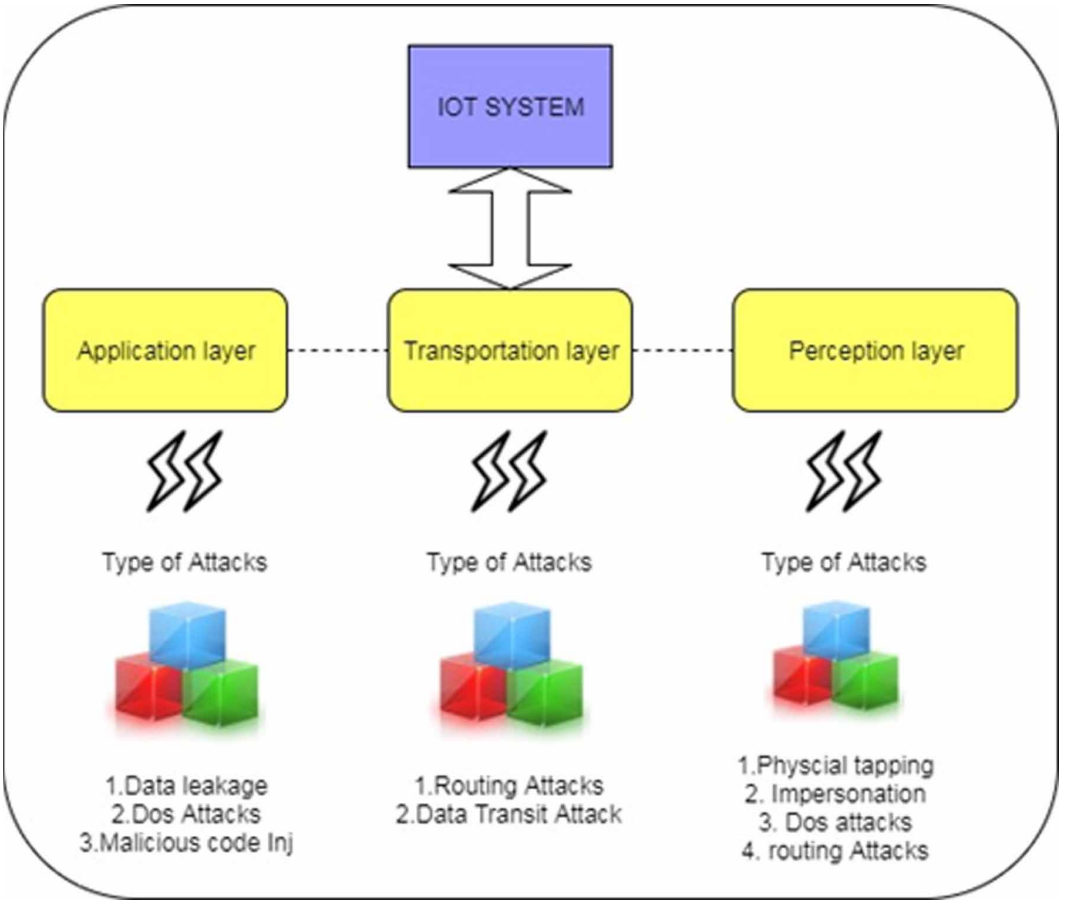
The IoT gadgets are regularly asset obliged and are portrayed with low power and less capacity. The assaults on IoT structures may bring about an expansion in vitality utilization by flooding the system and debilitating IoT assets through excess or produced benefit demands.

3.7. Security Challenges

Conventional techniques cannot be used in IoT because of the variety of standards and communication stacks involved. Hence the upcoming security and privacy feature should be a firewall for the information. Some of the upcoming research challenges (Hao, 2015) are listed below

1. Designing lightweight security for resource constraint networks and devices is a major task.
2. Common authentication: This is a network identity verification method that allows users to exchange information from one device to other. This can be implemented in IoT as well.
3. Controlling the access of an individual by identifying them in the system through their location and restricting their rights are very important.
4. Provisioning and protecting the data in a cloud is one of the key issues of the future IoT.

Figure 4. Security attacks in IoT layers



A summary of different type of Attacks and levels of threat and solutions (Shirgahi et al., 2017) are listed in Table 2

3.8. Quality of Service (QoS)

QoS has become the burning and sensational research topic in IoT. There are so many QoS topics which has to be addressed in IoT some are availability, reliability, mobility, performance, scalability, interoperability, security, management, and trust (Ungurean & Gaitan, 2015). Figure 5 defines the components of QoS.

3.8.1. QoS in IoT

Figure 6 represents the industrial deployment of IoT, where QoS plays a major role. Smart Nuclear reactor monitoring system, and it is a must to be monitored continuously. For example, a nuclear reactor in production should be monitored constantly with thermal images. This will help us to catch the problem signs and anomalies. These reports are provided to the monitoring station in real time to save lot of people life. In such instances providing data to the Monitoring stations accurately and without any delay is important. Various protocols are industrialized to afford QoS to IoT deployment.

Table 2. Security Attacks and the solutions

Type of attack	Threat level	Actions	Solution
Passive	Low	Usually breach data confidentiality.	Ensure confidentiality of data and do not allow an attacker to fetch information.
Man in the Middle	Low to Medium	Alteration and eavesdropping are the examples of this attack.	Apply data confidentiality and proper integration on data to ensure integrity
Active	High	Effects confidentiality and integrity of data.	Ensure both confidentiality and integrity of data.
Imitation	High	It impersonates for unauthorized access.	To avoid from spoofing and cloning attacks, apply identity
Privacy	High	Sensitive information of an individual or group may be dis-closed	Transmit sample data instead of actual data

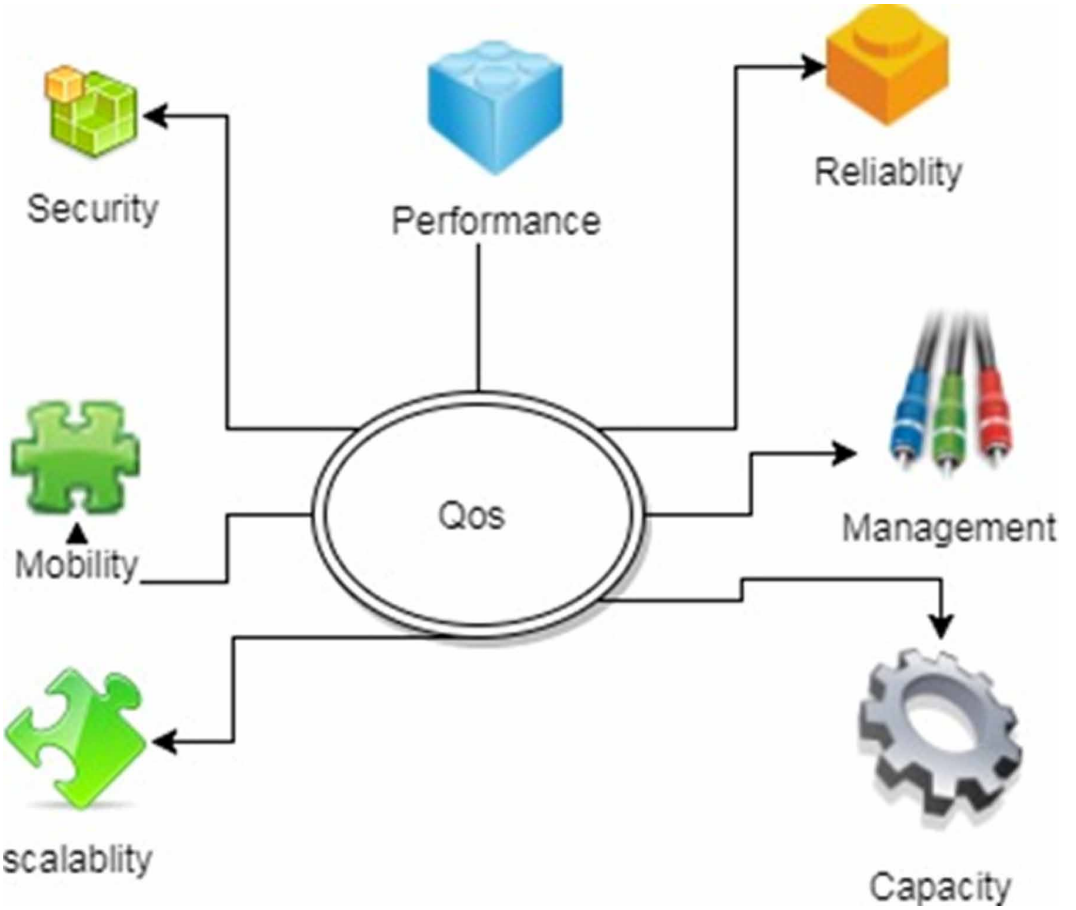
The data provided in Table 3 represents several IoT applications and the QoS parameters (Ahsan et al., 2016) to define the need for better services. QoS has its own challenges as it has numerous devices in the network and these challenges are given below (Sarkar & Kundu, 2016).

1.Resource–constraint devices: Sensor based devices in IoT are positioned at remote zones due to this there are power constraints as well as some other drawbacks like bandwidth, buffer size, memory issue also hits the system.
2.Traffic Load: As the sink node which is responsible for collecting large amount of data for numerous sensors are scattered in the environment. Due to this there is great hit in traffic, which ultimately hits the QoS.
3.Data Redundancy: As cited in the second point, the sink node which are scattered, receives data from several sensors and this may be redundant as well. Due to these redundant data the QoS may be affected. With the use of some data fusion or data aggregation techniques, data redundancy can be avoided.
4.Scalability: Scalability is a major factor as number of users in IoT keeps on increasing day by day. This rise in the usage should not affect the working of an application.
5.Fault Tolerance: The node or link failure is the big issue in provisioning QoS in IoT.
6.Heterogeneity: This is another major factor which affects QoS.
7.Multiple receiver and traffic types: Each application has its own set of receivers and these receivers rely on different traffic models which is again a hurricane to the QoS in IoT.

In General, we can categorize QoS solutions to some IoT applications can be achieved in following ways (Hussain, 2016)

1. QoS architecture for specific application.
2. Designing effective MAC protocol to deal with energy efficiency, throughput, and delay.
3. Optimizing the resource utilization.
4. Defining service models for IoT.

Figure 5. Components of quality of service



3.8.2. Routing Protocol

The Routing Protocol for Low power and Lossy Networks (RPL) which is the IPV6 routing protocol for Low power and Lossy Networks (LLNs) was standardized by IEFT. Meanwhile IoT emerged and had the global connectivity factor; hence it gained its priority for acquiring RPL protocol.

Figure 7 represents that the success of RPL in IoT. It is witnessed when the companies' part of ZigBee Alliance adopted the technology. There are few challenges in RPL must face to remain on the vanguard of technology.

3.8.3 RPL in a Casing

RPL usually has its topology in the form of Destination-Oriented Directed Acyclic Graph (DODAG), where DODAG is a directed graph without cycle formation and it orients towards a root node. Border router may be termed as example for the same.

For multipoint-to-point communication in RPL, this is the schematic representation of several parent nodes send packet upwards to the root node whereas the other nodes are kept for the purpose of serving as backup routers. The topology is created and maintained via control packets called DODAG Information Objects (DIO). The packet contains the routing metric and an objective function which is used by each node, to select their parents among the neighbors.

Figure 6. Monitoring the system

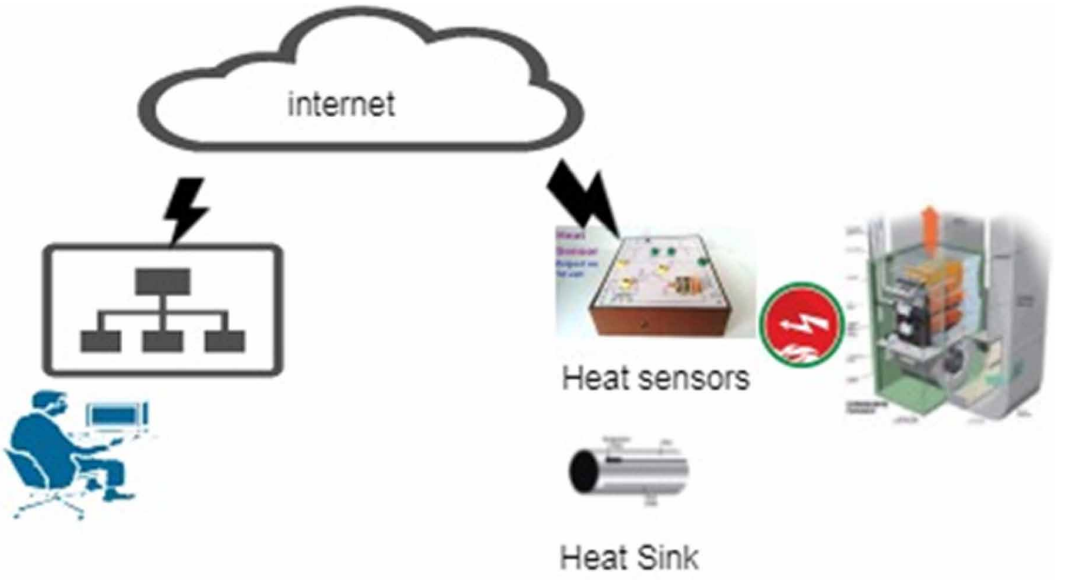


Table 3. QoS Requirement for various IoT deployments (Ahsan et al., 2016; Stoimenovic & Wen, 2014)

Deployment	Priority	Reliability	Data type	Availability
Smart Industrialization	High	High	Continuous	Low
Medical Domain	High	High	Continuous	High
Fire Service	High	High	Event	High
Smart Home	High	High	Query and Event	Moderate
Social Networking	Low	Moderate	Query	Moderate
Traffic control	High	High	Continuous	High

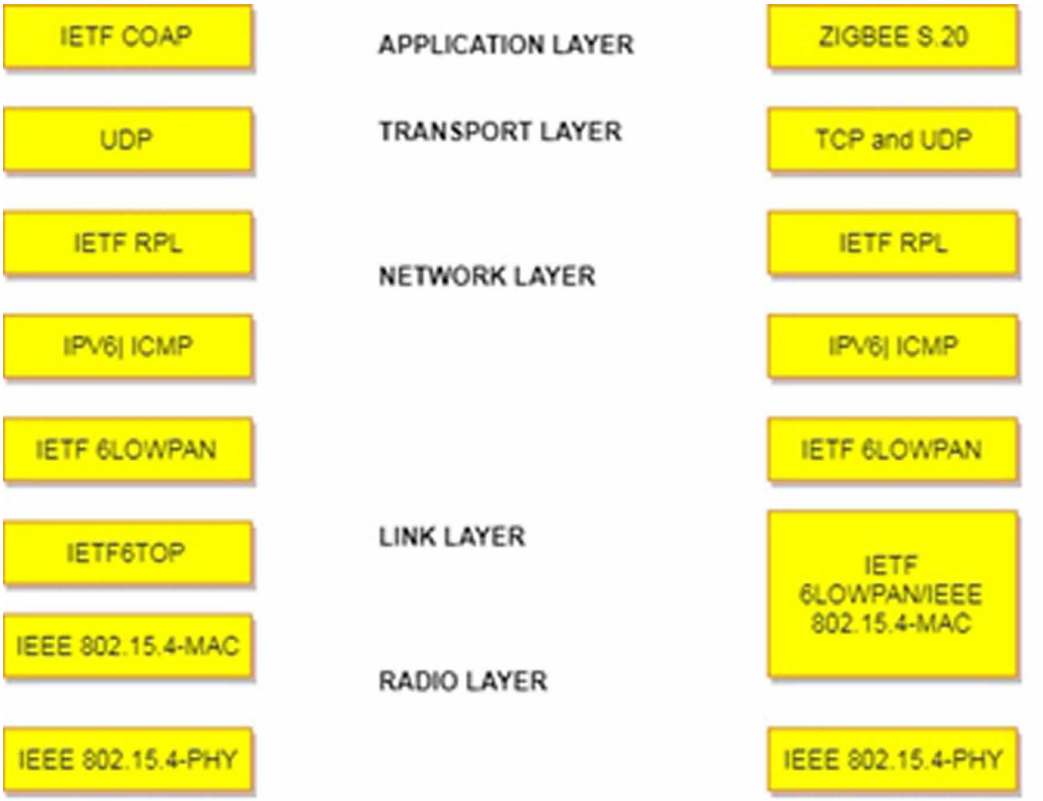
The Trickle algorithm is used to rebroadcast the DIO packets which strike a trade-off between reactivity to topology changes and energy efficiency. Trickle ensures that DIOs are publicized hostilely when the network is unhinged and instead rebroadcast at an increasingly slow pace while the network is stable.

To support point-to-multipoint communication in RPL, which is dual traffic pattern from the root to the devices the standard requires additional control messages and routing state. Destination Advertisement Object (DAO) control packets and it should be sent by all the node in the network to the root as a possible destination. Figure 8 represents the flow of these upwards messages in the DODAG topology thereby establishing downward route along the way.

3.8.4. RPL for IoT: The Future Challenges (Iova et al., 2016)

3.8.4.1. Prevailing Pattern on Traffic

Figure 7. IoT protocol Stack



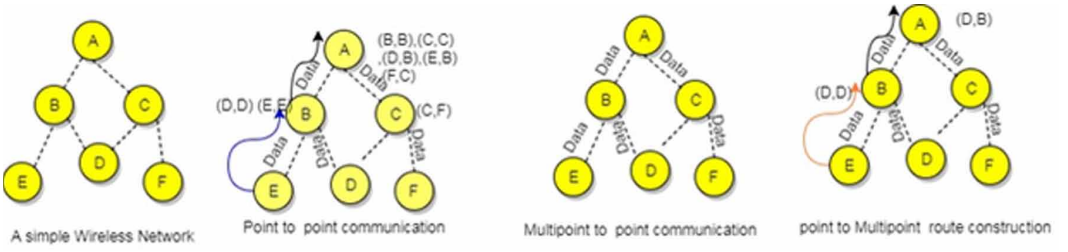
Point-to-multipoint and point-to-point communication received significantly less attention in RPL, yielding implementations with poor performance; this might forestall future adoption of RPL (Qu & Chan, 2016) within the ever-increasing IoT applications.

3.8.4.2. Mobile Devices

RPL deployment on Mobility is not satisfactory, which eventually pull down the Performance. The contact aware routing needs to be considered for future developments.

3.8.4.3. Advanced methods for Network Stack Design

Figure 8. RPL Routing Topology (Iova et al., 2016)



New approaches with considerably higher performances have emerged since the RPL customary was defined, and will so receive attention

3.8.4.4. Advanced/Innovative Wireless Technology

The scenarios nurtured by IoT are generating a new wave in wireless technologies that can significantly redefine the goals and eventually the mechanisms of RPL as well.

3.8.4.5. RPL Routing Attack

The Eaves dropping, Man in middle attack are the key implications as per (Dvir et al., 2011; Le et al., 2013) and the proposed solutions are hashing and Signature based Authentication.

3.8.5. Forthcoming RPL

To remain fruitful in the IoT domain, RPL needs a re-pointing. However, standardization bodies must keep up with the latest developments. The respective working groups (e.g., IETF ROLL), in an effort to create a "standard ecosystem" around RPL and weave it into state-of-the-art approaches from related research communities.

4. CONCLUSION

Internet has witnessed drastic changes which cannot be avoided and eventually the readiness of the internet has increased. Sensor technologies are well advanced and hardware is also available at a cheaper rate in market (Ahsan et al., 2016). Due to this, it has been possible to attach the sensors to this hardware and make them communicate with each other without the human activity coming into picture. This paper provides a brief thought to the Features, Main Concepts, Protocol stacks, Objectives and challenges of IoT. This paper analyzed the objectives and challenges of IoT technology by identifying some of the credible areas that needs to be well focused. This work will help us to understand and provide a theoretical Foundation of IoT concepts and challenges that can be specifically taken to develop the IoT framework for large scale Systems. The survey also highlights the 6Lowpan and RPL (traditional routing protocols) and the possible security Attacks. This will pave a way to develop effective security mechanism and better QoS for IoT systems.

REFERENCES

Ahsan, M., Talib, M. R., Sarwar, M. U., Khan, M. I., & Sarwar, M. B. (2016). Ensuring interoperability among heterogeneous devices through IoT middleware. *International Journal of Computer Science and Information Security*, *14*(4), 251.

Aijaz, A., Su, H., & Aghvami, A. H. (2015). CORPL: A routing protocol for cognitive enabled AMI networks. *IEEE Transactions on Smart Grid*, *6*(1), 477–485. doi:10.1109/TSG.2014.2324022

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376. doi:10.1109/COMST.2015.2444095

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials*, *17*(4), 2347–2376.

Aljawarneh, S. (2012). *Cloud computing advancements in design, implementation, and technologies*. Hershey, PA: IGI Global.

Asuncion, C. H., & Van Sinderen, M. (2011). *Towards pragmatic interoperability in the new enterprise—a survey of approaches*. Springer. doi:10.1007/978-3-642-19680-5_12

Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). *Fog computing: a platform for internet of things and analytics. In Big Data and Internet of Things: A Road Map for Smart Environments* (pp. 169–186). Springer.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the 1st ACM MCC Workshop on Mobile Cloud Computing* (pp. 13–16). doi:10.1145/2342509.2342513

Bravo, M., & Velazquez, J. (2008). *Discovering Pragmatic Similarity Relations between Agent Interaction Protocols*. Springer. doi:10.1007/978-3-540-88875-8_32

Chen, D., & Daclin, N. (2006, March). Framework for enterprise interoperability. In *Proc. of IFAC Workshop EI2N* (pp. 77-88). doi:10.1002/9780470612200.ch6

Dandelski, C., Wenning, B. L., Perez, D. V., Pesch, D., & Linnartz, J. (2015). Scalability of dense wireless lighting control networks. *IEEE Communications Magazine*, *53*(1), 157–165. doi:10.1109/MCOM.2015.7010529

Desai, P., Sheth, A., & Anantharam, P. (2015). Semantic gateway as a service architecture for IoT interoperability. In IEEE international conference on mobile services (pp 313–319).

Dvir, A., Holczer, T., & Buttyan, L. (2011). Vera - version number and rank authentication in rpl, In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems* (pp. 709–714). doi:10.1109/MASS.2011.76

Dvir, A., Holczer, T., & Buttyan, L. (2011). Vera - version number and rank authentication in rpl. In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems* (pp. 709–714). doi:10.1109/MASS.2011.76

Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, *5*(4), 2483–2495. doi:0.1109/JIOT.2017.2767291

Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., & Thomas, T. (2010). LTE-advanced: Next-generation wireless broadband technology. *IEEE Wireless Communications*, *17*(3), 10–22. doi:10.1109/MWC.2010.5490974

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Han, G., Shu, L., Chan, S., & Hu, J. (2016). Security and privacy in internet of things: Methods, architectures, and solutions. *Security and Communication Networks*, *9*(15), 2641–2642. doi:10.1002/sec.1497

Hao, Y. F. S. J. J. (2015). A scalable cloud for internet of things in smart cities. *Journal of Computers*, *26*(3), 1–13.

Hussain, M. I. (2017). Internet of Things: challenges and research opportunities. CSI transactions on ICT, 5(1), 87-95. doi:10.1007/s40012-016-0136-6

Iova, O., Picco, P., Istomin, T., & Kiraly, C. (2016). RPL: The Routing Standard for the Internet of Things... Or Is It? *IEEE Communications Magazine*, *54*(12), 16–22.

Karnouskos, S., Marrn, P. J., Fortino, G., Mottola, L., & Martinez deDios, J. R. (2014). *Applications and Markets for Cooperating Objects. In Springer Briefs in Electrical and Computer engineering* (pp. i–xiv, 1–120). Springer. doi:10.1007/978-3-642-45401-1

Kaur, S., & Mir, R. N. (2015). Quality of service in WSN-a review. *International Journal of Computers and Applications*, *113*(18).

Khari, M., Kumar, M., Vij, S., & Pandey, P. (2016, March). Internet of Things: Proposed security aspects for digitizing the world. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 2165-2170). IEEE.

Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., & Chai, M. (2013). The impact of rank attack on network topology of routing protocol for low-power and lossy networks. *IEEE Sensors Journal*, *13*(10), 3685–3692. doi:10.1109/JSEN.2013.2266399

Neiva, F. W., David, J. M. N., Braga, R., & Campos, F. (2016). Towards pragmatic interoperability to support collaboration: A systematic review and mapping of the literature. *Information and Software Technology*, *72*, 137–150. doi:10.1016/j.infsof.2015.12.013

Pinto, S., Gomes, T., Pereira, J., Cabral, J., & Tavares, A. (2017, January-February). IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices. *IEEE Internet Computing*, *21*(1), 40–47. doi:10.1109/MIC.2017.17

Qin, Y., Sheng, Q. Z., Falkner, N. J. G., Dustdar, S., Wang, H., & Vasilakos, A. V. (2016). When things matter: A survey on data-centric internet of things. *Journal of Network and Computer Applications*, *64*, 137–153. doi:10.1016/j.jnca.2015.12.016

Qu, Y., & Chan, P. (2016). Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network Based IoT Systems. In *Proc. IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity)*, New York, NY (pp. 42-48). doi:10.1109/BigDataSecurity-HPSC-IDS.2016.63

Qu, Y., & Chan, P. (2016). Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network Based IoT Systems. In *Proc. IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity)*, New York, NY (pp. 42-48). doi:10.1109/BigDataSecurity-HPSC-IDS.2016.63

Ronen, E., Shamir, A., Weingarten, A. O., & Flynn, C. O. (2017). IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *Proc. IEEE Symposium on Security and Privacy (SP)*, San Jose, CA (pp. 195-212). doi:10.1109/SP.2017.14

Sarkar, S., & Kundu, A. (2016). An indexed approach for multiple data storage in cloud. In *Information systems design and intelligent applications* (pp. 639–646). Springer. doi:10.1007/978-81-322-2755-7_66

Schoop, M., Moor, A., & Dietz, J. L. G. (2006). The pragmatic web: A manifesto. *Communications of the ACM*, *49*(5), 75–76. doi:10.1145/1125944.1125979

Shirgahi, H., Mohsenzadeh, M., & Haj Seyyed Javadi, H. (2017). Trust estimation of the semantic web using semantic web clustering. *Journal of Experimental & Theoretical Artificial Intelligence*, *29*(3), 537–556. doi:10.1080/0952813X.2016.1199601

Stojmenovic, I., & Wen, S. (2014). The fog computing paradigm: scenarios and security issues. In *Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS '14)*, Warsaw, Poland (pp. 1–8). IEEE. doi:10.15439/2014F503

Ungurean, I., & Gaitan, N. C. (2015). Data distribution service for realtime systems-a solution for the internet of things environments. *Annals of the University Dunarea de Jos of Galati: Fascicle II, Mathematics, Physics, Theoretical Mechanics*, *38*(1), 72–76.

Van der Veer, H., & Wiles, A. (2008). Achieving technical interoperability. *Eur. Telecommun. Stand. Inst.*, *3*, 1–30.

Vasco Lopes, N., Pinto, F., Furtado, P., & Silva, J. (2014) IoT architecture proposal for disabled people. In *IEEE 10th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 152-158). doi:10.1109/WiMOB.2014.6962164

Vinoski, S. (2006). Advanced message queuing protocol. *IEEE Internet Computing*, *10*(6), 87–89. doi:10.1109/MIC.2006.116

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The internet of things—a survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274. doi:10.1007/s10796-014-9489-2

Xu, K., Qu, Y., & Yang, K. (2016). A tutorial on the internet of things: From a heterogeneous network integration perspective. *IEEE Network*, *30*(2), 102–108. doi:10.1109/MNET.2016.7437031

Yang, Z., Ping, S., Sun, H., & Aghvami, H. (2016). CRB-RPL: A receiver based routing protocol for communications in cognitive radio enabled smart grid. *IEEE Transactions on Vehicular Technology*, *65*, 1–10. doi:10.1109/TVT.2016.2546948