International Journal of Engineering &Technology, 7 (1.7) (2018) 15-20

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Review paper

Internet of things (IoT): a survey on protocols and security risks

R H Aswathy [1] *, N Malarvizhi [2]

[1] *Research Scholar, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India*
[2] *Professor, Department of Computer Science and Engineering, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai-62, TamilNadu, India*
**Corresponding author E-mail: rhaswathy@gmail.com*

Abstract

A dramatic change by the growth of new ubiquitous computing, our globe is moving towards the fully connected paradigm called Internet of Things (IoT). The world is being connected and interlinked with the exponential growth of this pervasive technology. It plays a significant role in many fields such as healthcare, manufacturing industry, agriculture, transportation, smart homes etc and reinforces our everyday life. It acts as an aegis for covering all the factors such as protocols, key elements, technologies etc. IoT includes many capabilities and numerous mechanisms but protection hassle that slow down the era. In this paper we discussed about essential protocols and security issues of IoT.

Keywords: Internet of Things (IoT); Constrained Application Protocols (CoAP); DoS (Denial of Service); Bandwidth Constraint; Node Capture.

1. Introduction

IoT is a dynamic system foundation in which articles, individuals or creatures are furnished with UID and capacity to impart, gather and trade the information over system with H2H or H2M association. IoT is initially begat by Kevin Ashton in 1999 and well known to Auto-ID focus, MIT [1]. IoT is the achievement unrest of portable correspondence and it has AI that demands the articles to sense and convey together to share data and to take choices. It totals the accessible innovation, for example-sensor, RFID, EPC and so on. IoT enhances the world economy by method for business applications and it makes regular life simple by appealing home apparatuses and it contributes the Quality of life [2].

For case: In synthetic industry 1milli second is likewise significant, in light of the fact that it surpasses edge esteem, the whole unit will impact. In Smart-homes, it consequently opens the entryway while going into the home, planning espresso, control AC, TV and different machines. IoT empowered elements demonstrates more noteworthy than human and it works in many risky environments which people can't. In Japan after the atomic debacle, robots were utilized to investigate the harmed atomic force plants because of overwhelming radiation [3]. The computing technologies and expansive sensor communication develops a vertical applications which interest closely with horizontal entities [4].Smart technologies are needed with customary communication of internal and external environment [5].

IoT gadgets globally deployed around 212 billion entities at the end of 2020[6].The entire monetary effect is made by IoT is assessed $2.7 trillion to 6.2 trillion by 2025[7].In paper [8] creator demonstrates the expectation of future associated gadgets over IoT by 2050.The framework of the commitment of the paper is clarified as takes after. In section 2, we display the most vital conventions go about as the spine of IoT, for example, MQTT, XMPP, AMQP and CoAP with its nitty-gritty design. In section 3 we distinguished the most vital security issues confronted by IoT.

2. IoT protocols

2.1. Message queue telemetry transport (MQTT)

MQTT is presented by Andy Stanford clark of IBM and Arlan nipper of Arcom in 1999.The communication of this protocol is predicated on machine-to-machine level, sanctioned in 1999[9]. It is a publish/subscribe form of light-weight protocol flowing over TCP/IP with reliable bi-directional message distribution. Multiple consumers receive messages which is published once by publish/Subscribe messaging protocol. It provides disjoin between the publisher and subscriber. A publisher sends the message on the topic and subscriber consumes a message on a corresponding topic. A message server matches publications to subscriptions. If one or more matches found at the event, the message is delivered to corresponding subscriber and the message is discarded if no matches found. The MQTT is designed for constrained networks. The protocol has bit-wise headers and variable length fields. The packet size is 2 bytes [1] [9].Figure 1 shows the overall functionality of MQTT.

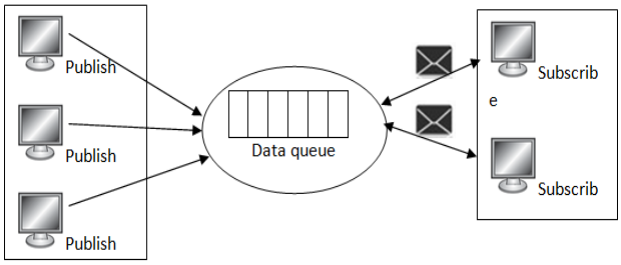


Fig. 1: Architecture of MQTT.

Copyright © 2018 R H Aswathy, N Malarvizhi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The publish-subscribe methods in MQTT is shown in Figure 2.

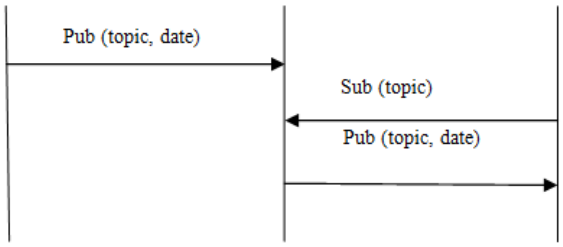


Fig .2: Publish-Subscribe Methods.

Bit	7	6	5	4	3	2	1	0
byte 1	MQTT Control Packet type				Flag - Each MQTT Control Packet			
byte 2…	Remaining Length							

Fig. 3: MQTT Control Packets with Fixed Header.

It sends from client that Server to publish a message and Server that Client to send the messages. The Table I shows the control packet types of MQTT.

Table 1: Control Packet Types of MQTT

Types	Mneumonics	Description
Connection Management	Connect	Client Request To Connect Server
	Connact	Connection Acknowledgement
	Disconnect	Client Is Disconnecting
	Pingreq	Ping Request
	Pingresp	Ping Response
Subscription Management	Subscribe	Client Subscribe Request
	Suback	Subscribe Acknowledgement
	Unsubscribe	Client Unsubscribe Request
	Unsuback	Unsubscribe Acknowledgement
Message Delivery	Publish	Publish Message
	Puback	Publish Acknowledgement
	Pubrec	Publish Received
	Pubrel	Publish Release
	Pubcomp	Publish Complete

The QOS field indicates the level of assurance for delivery of an application service.The QOS level is listed in Table 2.

Table 2: QoS Levels

Qos value	Bit 2	Bit 1	Description
0	0	0	At most once <=1
1	0	1	Atleast once >=1
2	1	0	Exactly once =1
3	1	1	Reserved

In MQTT, most control packets have a corresponding acknowledgement. The term 'Connect' restarts the previous session.The MQTT control packet consists of 3 parts such as Fixed header,Variable header and Payload.The MQTT control packet contains fixed header format is shown in figure 3.

2.2. Extensible messaging and presence protocol (XMPP)

In the year 1999, Jabber open source Community developed the rudimentary syntax and semantics of XMPP [10]. The Jabber protocol that would appropriate for IETF instant messaging (IM) and presence technology in the year 2002[10].The XMPP is implemented by a client-server architecture is shown in figure 4. The client and server architecture are Request/response over TCP Connections. XMPP act as a gateway and it bridge the communication between peregrine networks [11].

The server manages the connection from different entities in the form of XML streams. Xml stanzas are routes and addressed by XML Streams. Clients utilize TCP Connection to communicate with server. Multiple users/resources can connect simultaneously to server with the avail of resource identifier of an XMPP address. Client and server communicate through gateway. Message passing is the primary function of server side special purpose service.

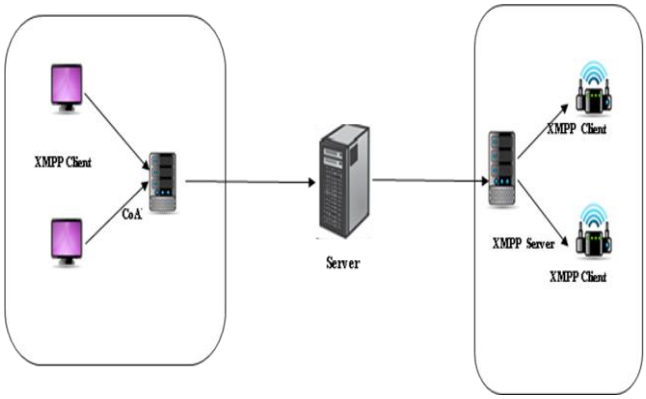


Fig. 4: Architecture of XMPP.

The addressing schemas are identified by identifiers. The most prevalent identifiers are Domain identifier, Node identifier and Resource identifier [10]. The representation of network gateway or primary server to indicates the association of entity is done by Domain identifier. It is addressed as a sub domain of a server. Node identifier: optional secondary identifier associated with multiuser chat service, called bare JID. Resource identifier: optional tertiary identifier represents a concrete session, connection (example: Device or location) or object.

XML Streams is a container, mainly deployed for the exchange of XML elements between any two entities over a network.

XML stanza is a discrete semantic unit of structured information and separated into three components: (i) Message stanza,(ii) Presence stanza and (iii)IQ stanza [2] [10]. Message stanza includes single messages. The types are chat, Error, group chat, headline etc. Presence stanza express entities current availability status.IQ stanza works predicated on Request/response mechanism. Types of IQ are get, set, result, and error etc. The structure of XML stanza is shown in Figure 5.

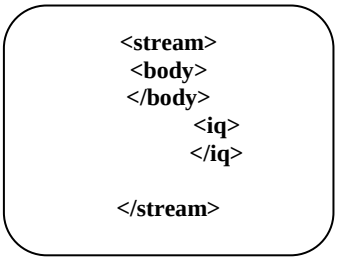


Fig. 5: Structure of XMPP Stanza.

2.3. Constrained application protocol (CoAP)

CoAP is an application layer protocol designed for resource constrained environment. It is specialized web transfer protocol categorically intended to low power sensors, components and switches that need to be controlled and supervised remotely. This protocol is designed for machine to machine communication. CoAP provides a request /response model between applications. A CoAP request is sent by a client to request a concrete action. The server then sends a response using response code. CoAP bind with UDP and fortifies unicast and multicast request. It interchanges messages asynchronously. CoAP defined 4 types of messages: CON (Confirmable message), ACK (Acknowledgement), Reset (Reset message) [2] [6]. The CoAP architecture is shown in figure 6.

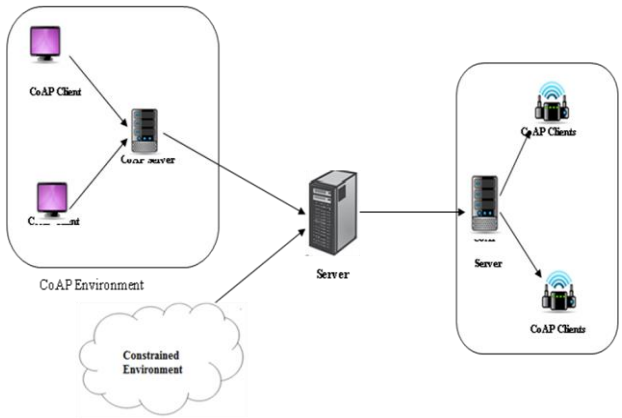


Fig. 6: Architecture Diagram of CoAP.

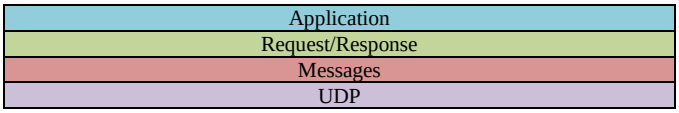


Fig .7: Layering of CoAP.

This protocol run on the top of TCP, it fortifies both unicast and multicast communication, while HTTP runs in the UDP, it fortifies only unicast so it works with group communication. The CoAP messaging model is predicated on exchange of messages over UDP. It has a fine-tuned binary header of 4 bytes. The messages are carried out by request and response [12].The layering of CoAP is shown in figure 7. CoAP works with reliable and unreliable message transmission. The reliable message transmission is marked as CON (Confirmable), it returns an ACK within timer expires (timeout).

The unreliable message transmission does not require any Acknowledgement. This protocol works under the three types of responses named Piggybacked, separate response and Non-confirmable request/response. Request and response are carried by Confirmable and Non-confirmable messages. The confirmable message is carried by ACK. This is called as piggyback response shown in figure 8 [12].

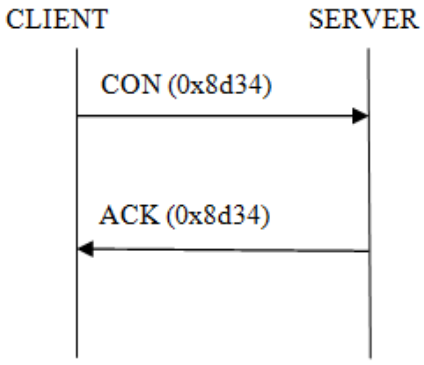


Fig. 8: GET Request with Piggyback Response.

The request is carried out by confirmable message and server is not able to respond immediately to the particular request, it responds with empty ACK message [12]. The client can stop the retransmitting request. Once the request is yare, the server sends the confirmable message, called separate response shown in the figure 9.

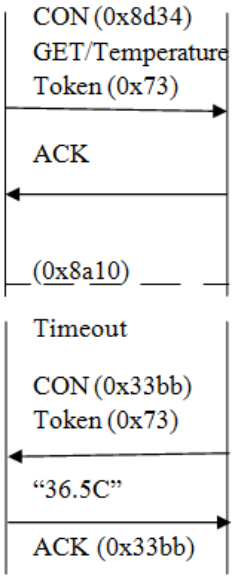


Fig. 9: GET Request with Separate Response.

If the request is non confirmable message, it does not need and ACK. The server sends a Non-confirmable message instead of confirmable message. CoAP fortifies with four methods: GET, POST, PUT and DELETE [2] [12]. GET is the method which regains the information which is identified by requested URI. The respond message with 200(OK) is sent, if the request is processed precisely. The server is to create the new subordinate resource under the desired pared URI by using POST method. The server should reply with 201(created) once the resource has been created. The new message does not created, the servers responds with 201(OK), once the 'POST' done successfully. The resource URI be updated or created with the message body by using PUT method. The message body will consider the modified version of that resource and 200(OK), If the resource subsists at the corresponding URI. The server creates new resource with URI 201(created), if no resource exits. The error response code is displayed if the code is created or modified anonymously. The response code 200(Ok) should send URI is deleted by DELETE method

2.4. Advanced message queuing protocol (AMQP)

AMQP is an open standard application layer protocol with MOM (Message-oriented middleware) architecture. AMQP provide a full functional interoperability between and middleware servers (brokers). AMQP defines both server side accommodations and network protocol. In network protocol, the AMQ model has defined rules for coalescing the components together and consist of set of components that store and route messages within the broker service. The architecture of AMQP is shown in figure 10. In a protocol level, AMQ have set of rules when client application interacts with AMQ model.

The AMQP protocol guarantees the interoperability between AMQP components. The components in the architecture which are connected parallel in the server to accomplish the desired functionality. The components are exchange, message Queue, publisher, consumer and binding [13].

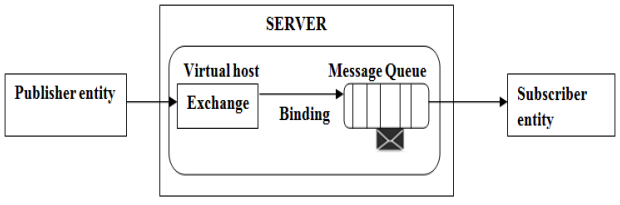


Fig. 10: Architecture of AMQP.

The publisher entities who publish the messages, the data server accept the message and send them to different consumers depending upon the routing address. If consumers are diligent it buffers them in memory or disk. In Exchange, it accepts the messages and routes them top message queue. The message queue stores the messages and forwards to the end user or consumer entity. Binding is the interface between exchange and message queue. There are number of exchange types. Depending upon the application, it creates the own exchange instances are withal denominated. It designates how to bind Queues and publish messages.

AMQP works with two things in runtime programmable semantics [13]. First it engenders arbitrary exchange and message queue types via protocol. Second it wires the exchanges and message queue together to engender any message processing system through protocol.

Routing key is a virtual address that exchange and decide how to route the messages. Two routing keys are discussed here. First, P2P routing key, it is same as that of message Queue name. Second, Publish/subscribe routing, the routing key is a topic hierarchy value

The AMQP is split into two layers: Functional layer and transport layer [2] [13]. Functional layer grouped into logic class of functionality and work together. The transport layer routes the method from application to server and it handles data representation, channel multiplexing, context encoding, framing and Error handling [14].The AMQP model was driven by many factors such as QoS, interoperability, consistent, explicit in naming, complete configuration of server etc. Likewise the transport layer of AMQP is driven by many factors such as Binary encoding, handles messages of any size(without any limit),carries multiple channels across single connection, long lived, no limitations, Asynchronous command, scalable, version upgrade, repairable, neutral with programming languages and code generation process.

The message queue in the AMQP store messages in disk or memory and routes to consumer applications. The message queue is act as storage and distributers of messages. Each message queue is independent to one another. The paramount properties of message queue are private/shared, durable/temporary and client/server. Predicated on the properties, the user can utilize the message queue to deploy the standard middleware entities: store and forward Queue, private reply Queue and private subscription queue. A store and forward queue holds messages and distribute the messages between consumers on round robin substructure [13]. These queues are very flexible and durable while messages shared between multiple consumers. Private reply queue holds and forward messages to single consumers. It is an ephemeral queue, server denominated and private to only one consumer. A private subscription queue holds messages collected from amassed sources and forward to a single consumer. Table III shows IoT protocols and its desired features.

Table 3: Protocol and Its Features

S. No	Protocols	Features
1	CoAP	Asynchronous Message Transfer, Lower Overhead, Parsing Complexity, Simple Proxy, Datagram Transport Layer Security, Satisfy M2m Requirement
2	MQTT	Resource Discovery, Resource Observation, Store And Forward, Prioritize, Interacting With Http, Providing Qos, Security
3	XMPP	Instant Messaging, Presence Protocol, Block Communication, Message Subscription And Message Item
4	AMQP	Standard Wired Protocol, Routing Key, Message Persistence, Request And Response, Redelivery/Acknowledgement

3. Security risks in IoT

The breathtaking open door for entrepreneurs and industrialist is given by IoT to build up new product and offers an assortment of administrations to satisfy the consumer loyalty. Number of IoT gadgets develops each day, the security danger and potential difficulties are likewise develops alongside that. Amid the correspondence between the gadgets in IoT environment, the webs likewise have numerous securities hazard specifically DoS, Eavesdropping, Unauthorized access, Tampering gadgets and privacy risks. It is constantly hard to actualize the cryptographic calculation and security conventions in IoT gadget. Since IoT is universal it requires fitting confirmation and approval measures [15] [16].

Table 4: Performance Measures of IoT Protocols

Protocols/parameters	MQTT	XMPP	CoAP	AMQP
Transport	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Communication	Publish-Subscribe	Peer-to-Peer	Request-Reply	Peer-to-Peer
Data transfer	Device-cloud Cloud-Cloud	Device-cloud Cloud-Cloud	Device-Device	Device-Device Device-cloud Cloud-Cloud
QoS	Medium	Low	Medium	Medium
Error Tolerance	Broker in SPoF	Server in SPoF	Decentralized	Implementation specific
Interoperability	Basic level	Structural	Semantic	Structural
Low power and Lossy data	Good	Fair	Excellent	Good

3.1. Distribution and denial-of-service attacks

DoS are a cyber attack launched against IoT. Amid this assault the system asset is inaccessible to the purposive client. It makes the site is in disengaged mode or some potential operational disappointments. Malicious attacker involves the whole system foundation and makes more disorder [16]. In automotive device IoT works with the standard of M2M correspondence. It is utilized as a part of most delicate industry like substance industry, DoS fall the whole unit. It is a detrimental consequence of a delicate industry. In corporate site, the clients are attempting to get to the information, the information is distracted the client get baffled and it prompts incredible misfortune and disappointment of clients.

3.2. Node capture and eavesdropping

The attacker physically finds the information specifically environment and store the information away element for future work. One sort of passive attack, the assailant assaults the correspondence channel to discover the information. Keeping in mind the end goal to get the data, the passive attacker extricates the data that moving inside that specific base.

3.3. Controlling the data

This is a an active attack as opposed to Eavesdropping or node catch the attacker pick up an incomplete or full control over the IoT gadget. The harm brought on by aggressor taking into account (a) the significance of information (b) benefits that are given by specific substance [16].

3.4. Complexity of vulnerability

System information assurance can be minimized by attacker due to vulnerability. It can be shaped by utilizing three components that is (a) System defect (b) attacker access to that flaw and (c) attacker ability to use the flaw. In delicate robotization industry this prompts decimation. To minimize the danger in IoT gadget, the gadget must plan with high security and secure firmware. Se-

curity can be authorized in HSF segment amid the configuration of IoT based supplies. Vulnerability management is an imperative piece of IoT, it is coordinated with system and PC security. The imperative stride in Vulnerability management is to distinguish, arrange and resolve vulnerabilities in HSF segment. Firmware upgrade takes additional time and exertion and it is a dangerous task.WAP or different gadgets in IoT are given in-build web server, it interfaces remotely. User can sign in by utilizing user ID and secret key. Before deploying the IoT gadget, it can give with specific set of information and maps with right arrangement of yield. The IoT gadget can be nearly observed with certain period before moving into this present real world scenario.

3.5. Bandwidth constraint

Research found that bandwidth is a critical limitation, which is utilized for transmitting a signal in addition network traffic is hopped 700% [17].Due to P2P application, high streaming media and person to person communication. More gadgets are associated in the web, the association needs to expand the Bandwidth and control the movement in the system. The Security model of IoT can be clarified by 3C's ie, Computation, Communication and Control [18]. The intelligent power grid is the most important and biggest instantiation of IoT system [19].Resource allocation is an important during this bandwidth, this can be narrated by author Sungwook Kin in paper [20].

3.6. Access attacks and privacy attacks

The intruder or unauthorized entity gain access to hardware components or network with no privilege to access. Access attacks can be categorized as two. The First one is physical access: unapproved entity access to physical device. The next is remote access, the intruder attacks the IP connected device [21].Protecting the private data is more challenging due to simple accessibility of extensive volume of information through remote access mechanism. The most recognized attacks are:

Data mining-The process of access the information from the database

Cyber espionage: It works with the spy or cracking technique of mystery data of individual, association or government organization.

Tracking: The intruder monitor every last minute utilizing one of an unique identifier (UID).this will uncover the elements definite area and exercises.

Table 5: Protocols with Security Measures [3] [4] [5] [22]

Protocols/parameters	MQTT	XMPP	CoAP	AMQP
Transport	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Communication	Publish-Subscribe	Peer-to-Peer	Request-Reply	Peer-to-Peer
Data transfer	Device-cloud Cloud-Cloud	Device-cloud Cloud-Cloud	Device-Device	Device-Device Device-cloud Cloud-Cloud
QoS	Medium	Low	Medium	Medium
Error Tolerance	Broker in SPoF	Server in SPoF	Decentralized	Implementation specific
Interoperability	Basic level	Structural	Semantic	Structural
Low power and Lossy data	Good	Fair	Excellent	Good

Password attacks: Intruders use copy passwords to assault the gadget or system. Two sorts of attacks are conceivable. The first one is Dictionary attack-attack happen with conceivable blend of letters and numbers to access client record or data. The second one is brute force attack-It is an application program with experimentation strategy used to get information such as client PIN or secret word. The attack will proceed until a right watchword is found with various conceivable key mixes.

4. Conclusion

This new innovation assuming a noteworthy part while advance regular life to expand profitability, enhance productivity in all fields like mechanical, medicinal services, home computerization, logistics and numerous more brilliant applications. In this article, we present the overview of the key components, protocols, which driven IoT, different applications for our solace living and difficulties, which confronted by research communities. Additionally the articles provide awesome ground work for researchers to overcome from issues faced by IoT communities. Security of information is the key point of any connected network, so our research moves towards make a more secure system than the existing and plays vital role in digital world.

References

[1] Ashton k. That ‘Internet of Things’ thing. RFID Journal, vol. 22, no. 7, pp. 97–114, 2009.

[2] Ala Al-Fuqaha,Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari and Moussa Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications” Vol. 17, No. 4, Fourth Quarter 2015.

[3] G. Brumfiel, "First Eyes inside Nuclear Plant May Be A Robot's," NPR, March 23, 2011.

[4] Winnie Kurien,”Internet of Things (IoT) & It’s Challenges” (IJARCET) Volume 5, Issue 5, May 2016

[5] Open Auto Alliance, Oct. 20, 2014. Available: http://www. openautoalliance.net

[6] J. Gantz and D. Reinsel, “The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east,” IDC iView: IDC Anal. Future, vol. 2007, pp. 1–16, Dec. 2012.

[7] J. Manyika et al., Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy. San Francisco, CA, USA: McKinsey Global Instit., 2013.

[8] Mahmoud Shuker Mahmoud, Auday A. H. Mohamad,” A Study of Efficient Power Consumption Wireless Communication Techniques/ Modules for Internet of Things (IoT) Applications”, AIT, Vol.6 No.2, April 2016http://creativecommons.org/licenses/by/4.0

[9] D. Locke, “MQ telemetry transport (MQTT) v3.1.1 protocol specification,” IBM developerWorks, Markham, ON,Canada, Tech. Lib., 2010.[Online].Available:Http://Www.Ibm.Com/Developerworks/Webservices/Library/Ws-Mqtt/Index.Html

[10] P.Saint Andrea,Ed,Jabber ”Extensible Messaging Presence Protocol(XMPP)”software foundation,October 2004. https://xmpp.org/rfcs/rfc3920.html

[11] M. T. Jones, "Meet the Extensible Messaging and Presence Protocol (XMPP)," developerWorks, 2009. https://www.ibm.com/developerworks/library/x-xmppintro/index.html.

[12] Z. Shelby, K. Hartke ” The Constrained Application Protocol (CoAP) “ ISSN: 2070-1721 C. BormannInternet Engineering Task Force (IETF) , https://tools.ietf.org/html/rfc7252.

[13] ” Advanced Message or Queuing Protocol” AMQP-Protocol specification Version 0-9-1, 13 November 2008, https://www.rabbitmq.com/resources/specs/amqp0-9-1.pdf

[14] OASIS Standard, "OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0," 2012. http://docs.oasis-open.org/amqp/core/v1.0/os/amqp-core-complete-v1.0-os.pdf

[15] Sye Keoh,Sandeep S Kumar and Hannes Tschofenig,”Securing the Internet of Things:A Standardization perspective,IEEE Internet of Things Journal,VOL 1,No 3,June 2014

[16] Rodrigo Roman,Jianying and Javier Lopez,”On the features and challenges of security and privacy in distributed Internet of Things” Volume: 1, Issue: 3, June 2014, Page(s): 265 – 275, ISSN: 2327 4662, http:\\www. elsevier. com/locate/comnet.

[17] Josh Broch David A. Maltz David B. Johnson Yih-Chun Hu Jorjeta Jetcheva,”A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols” ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’98), October 25–30, 1998, Dallas, Texas, USA. http:// www.monarch.cs.cmu.edu.

[18] YANG Jin-cui,FANG Bin-xing,”Security model and Key technologies for Internet of Things,ScienceDirect, 2011 December. www.sciencedirect.com/science/journal/10058885. https://doi.org/10.1016/S1005-8885(10)60159-8.

[19] Mitali Mahadev Raut, 2Ruchira Rajesh Sable, 3 Shrutika Rajendra Toraskar,"Internet of Things (IOT) Based Smart Grid,", (IJETT) – Volume 34 Number 1- April 2016,ISSN:2231-5381.

[20] Sungwook Kim,"Asymptotic shapley value based resource allocation scheme for IoT services", Computer Networks 100 (2016) 55–63,www.elsevier.com/locate/comnet,2016. https://doi.org/10.1016/j.comnet.2016.02.021.

[21] Mohamed Abomhara and Geir M. Køien,"Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks" 17 April 2015; Journal of Cyber Security, Vol. 4, 65–88. https://doi.org/10.13052/jcsm2245-1439.414.

[22] Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash," Security Analysis of the Constrained Application Protocol in the Internet of Things", IEEE FGCT,17 March 2013, https://www.researchgate.net/publication/259869307. https://doi.org/10.1109/FGCT.2013.6767217.