МЕЃУНАРОДЕН ЦЕНТАР ЗА СЛАВЈАНСКА ПРОСВЕТА - СВЕТИ НИКОЛЕ

«МЕЃУНАРОДЕН ДИЈАЛОГ: ИСТОК - ЗАПАД»
(ЕКОНОМИЈА, БЕЗБЕДНОСНО ИНЖЕНЕРСТВО, ИНФОРМАТИКА)

С П И С А Н И Е
на научни трудови

ДВАНАЕСЕТТА МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА „МЕЃУНАРОДЕН ДИЈАЛОГ: ИСТОК - ЗАПАД“
МЕЃУНАРОДЕН СЛАВЈАНСКИ УНИВЕРЗИТЕТ „ГАВРИЛО РОМАНОВИЧ ДЕРЖАВИН“ СВЕТИ НИКОЛЕ - БИТОЛА

Година VIII ***Број 1*** ***Април 2021***

- СВЕТИ НИКОЛЕ, Р. СЕВЕРНА МАКЕДОНИЈА -
- 2021 -

Издавач: Меѓународен центар за славјанска просвета - Свети Николе

За издавачот: м-р Михаела Ѓорчева, директор

Наслов: «МЕЃУНАРОДЕН ДИЈАЛОГ: ИСТОК - ЗАПАД» (ЕКОНОМИЈА, БЕЗБЕДНОСНО ИНЖЕНЕРСТВО, ИНФОРМАТИКА)

Компјутерска обработка и дизајн: Адриано Панајотов, Маја Маријана Панајотова, Благој Митев

ISSN (принт) 1857-9299
ISSN (онлајн) 1857-9302

Адреса на комисијата: ул. Маршал Тито 77, Свети Николе, Р. Сверна Македонија

Контакт телефон: +389 (0)32 440 330

Уредувачкиот одбор им се заблагодарува на сите учесници за соработката!

Печати: Печатница и книжарница „Славјански“, Свети Николе

Тираж: 100

МЕЃУНАРОДЕН ДИЈАЛОГ

ИСТОК - ЗАПАД

ЕКОНОМИЈА, БЕЗБЕДНОСНО ИНЖЕНЕРСТВО,
ИНФОРМАТИКА

ОБЛАСТ

ИНФОРМАТИКА

004.77.057.4-047.44

Ognen Firfov, PhD
Makedonski Telekom, Republic of North Macedonia

Cvetan Angjelkovski
UACS, Republic of North Macedonia

Viktor Denkovski, MSc
UACS, Republic of North Macedonia

Irena Stojmenovska, PhD
UACS, Republic of North Macedonia

COMPARATIVE ANALYSIS OF STANDARD IP AND IOT NETWORKING

ABSTRACT: In the past years we believed that IoT will be the future of the Internet and now we can easily say that we live in the future. The Internet of Things has rapidly expanded and is expected to continue expanding even faster in the following years. This paper gives an overview of the most common Web protocols and IoT protocols and provides a comparison between the IoT Stack and Web Stack seen through prism of various layers assisting you in deciding the most suitable set of protocols for your IoT device.

KEYWORDS: Internet of Things, TCP/IP, IoT protocols vs Web protocols, IoT Stack vs Web Stack

INTRODUCTION

The Internet of Things (IoT) refers to a complex network of "Things" – devices, embedded with software, sensing and other technologies that are able to connect and exchange information with other physical objects over the internet, through the use of standard message protocols [1].

The concept of the Internet of Things (IoT) was introduced in 1999 by Kevin Ashton at a presentation he made for Procter & Gamble (P&G) in 1999 [2]. Radio-frequency identification (RFID), nano and sensor technology as well as intelligence embedded technology are the most important technologies of the Internet of Things. RFID is at the heart of the construction of the Internet of Things, its foundation and networking core [3]. The development of RFID, WSN and cloud computing contributed to fast development of the communication among IoT devices and made it even more convenient than it was before [4].

Nowadays the internet no longer represents only a network of computers but also a network of all kinds of devices such as vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings. All of them being connected, communicating and sharing information based on protocols that allow smart restructurings, detecting, outlining, positioning, as well as, online monitoring and upgrade, control procedures and administration [1]. IoT gives us the possibility to connect and exchange information among billions of devices, services and people.

The IoT system can be divided in four sections [5]:

1. The Internet
2. The local network (this can include a gateway, which translates proprietary communication protocols to Internet Protocol)
3. The "Things" (meaning, the devices)
4. Back-end services (enterprise data systems, or PCs and mobile devices)

IoT diverges in few main categories such as:

» Industrial IoT, where the local network is based on one of many different technologies. The transmission of data over the global internet is going through IoT devices.
» Commercial IoT, where local communication is typically either Bluetooth or Ethernet (wired or wireless). The IoT device will communicate only to devices in local area [6].
» Consumer IoT, where local communication through short-range communication and typically used technologies are Bluetooth, WiFi and ZigBee. These are suitable for small spaces like houses or offices [7].

With the growth of IoT, security became stronger and privacy risks minimized [8].

In this paper we are comparing the standard networking with the IoT networking through the most common protocols. Furthermore, some ideas for future researches are given

1. COMPARISON OF WEB AND IOT PROTOCOLS

A. The TCP/IP Protocol

At the core of the Internet is the TCP/IP protocol stack which can be presented using the OSI seven layer reference model. To simplify the model the lowest three layers, Physical and Data Link layer, Network layer, Transportation layer, are grouped together [9].

» *Physical and Data Link Layers*

The most common physical layer protocols used by embedded systems are [10]:

1. Ethernet (10, 100, 1G)
2. WiFi (802.11b, g, n)
3. Serial with PPP (point-to-point protocol)
4. GSM, 3G, LTE, 4G

» *Network Layer*

Network layer conducts communication between the physical devices, determines the best path among networks reassuring transmission of information through many communication protocols in an IoT system. MQTT and CoAP are the most common protocol for IoT. With the help of Wireless Sensors, the main objective of the network layer is to collect information that is obtained by the physical layer which is further sent to information processing unit. From every device in the IoT network private information is sent with the assistance of the wireless sensors [11]. The transfer of information on the IoT network is carried by the network layer, therefore secure transfer of data is done by this layer from physical layer to other layers [12].

» *Transport Layer*

TCP and UDP are transport protocols that can be found above the Network layer. The most used transport protocol for most of our human interactions with the Web is TCP, that is why, many people think that this is a reason why it should be the only protocol used at the Transport layer. TCP is a connection-oriented protocol [13]. It provides the function of establishing a connection with a mechanism to track data that has been sent and acknowledgement of what is received. This way, TCP can detect a missing packet and resend it accordingly, ensuring reliable transmission of data and flow control but for an embedded system, TCP can be overkill. This been said, connectionless UDP is now finding its spotlight in sensor acquisition and remote control even if it has been relegated to network services such as DNS and DHCP. UDP is often used for transmission of information such as audio and video [14].

B. The IoT Protocols

You can build an IoT system with familiar Web technologies but the result would not be as efficient as with the newer protocols [15].

» *HTTP*

HTTP was designed in the early 90s and it is an extensible protocol that has evolved over time [16]. HTTP runs on TCP protocol. It is the foundation of any data exchange and it is the foundation of the client-server protocol, equipped with lot of headers to actually reach their destination over the internet. Including only a client in your IoT device is a more secure method. Excluding a server means that your IoT device would not be receive connections but will only be able to initiate them. After all, this protects you from an outside access to your local network [17].

» *WebSocket*

WebSocket is a protocol that provides full-duplex communication over a single TCP connection between client and server meaning that it allows client and server to communicate in a more real-time manner. From the most part communication is headerless and lightweight except for the initial handshake which is in HTTP [18]. Much of the connection management and the complexity around bi-directional communication on the Web is simplified by the WebSocket.

» *XMPP*

XMPP (Extensible Messaging and Presence Protocol) is a good example of an existing Web technology finding new use in the IoT space. XMPP has its roots in instant messaging and presence information, and it offers a multitude of applications beyond traditional instant messaging and the distribution of presence data [19]. XMPP addresses scheme to recognise devices on the network and enables the discovery and availability of services residing locally or across the network. XMPP provides a lot of support for communication, making it well suited for use within the realm of the Internet of Things making it suitable for remote management of appliances such as air conditioners, refrigerators, dryers, washers and many more [20].

» *CoAP*

Web protocols can be used for IoT devices but even though they are available they are too heavy for most of the IoT applications. The Constrained Application Protocol (CoAP) was designed by the IETF for use with low-power and constrained networks. CoAP uses the same methods used by HTTP. CoAp is IoT client server protocol, much like HTTP, where a client makes a request and the server sends back a response. It is suitable choice of protocol for devices which operate on battery [21].

Here are some of the features of CoAP [22]:

1. CoAP uses UDP.
2. Because CoAP uses UDP, some of the TCP functions are reproduced in CoAP. CoAP can distinguish non-confirmable messages and confirmabale messages.
3. Requests and responses are exchanged asynchronously over CoAP messages.
4. All the headers, methods and status codes are binary-encoded, which reduces the protocol overhead.
5. Unlike HTTP, the ability to cache CoAP responses does not depend on the request method, but the Response Code.
6. CoAP fully addresses the need for an extremely lightweight protocol and the ability for a permanent connection. And if you have a Web background, using CoAP is relatively easy.

» *MQTT*

MQ Telemetry Transport (MQTT) is an open source protocol for constrained devices and low-bandwidth, high-latency networks. It is a standard IoT messaging protocol carrying out messaging using publish-subscribe model unlike the HTTP that uses the request-respond model. Unlike HTTP, MQTT enables messages to be pushed to clients. Being designed as lightweight, MQTT, it is ideal for connecting small devices to constrained network. The biggest IoT platforms, IoT cloud service providers and many IoT edge gateways and devices support connectivity with MQTT[23].

Some of the key benefits of MQTT are [24]:

1. Lightweight and Efficient – its clients are small and require minimal resources.
2. Bi-directional Communications - enables messaging between device to cloud and vice versa.
3. Scale to Millions of Things – it can scale to connect with millions of IoT devices
4. Reliable Message Delivery – delivery of the messages is very important in many cases and MQTT has defined three quality of service levels.
5. Support for Unreliable Networks - reduces reconnection time required over unreliable networks
6. Security Enabled – TLS encrypted messages and modern uthentication protocols.

C. Comparison of Web protocols and IoT protocols

The key problem with IoT standardization is the limitations of the environment of IoT characterized by low storage capacity, energy constrains, low available bandwidth and high packet loss because IoT does not allow TCP/IP protocol to reduce these losses [25].

Fig. 1 below, shows a comparison between the IoT stack protocols and Web stack protocols. To solve this challenge, there are hundreds of proprietary protocols in IoT, M2M (Machine to Machine) and smart home communication technologies such as ZigBee and BLE (Bluetooth Low Energy) or Bluetooth 4.0. These protocols are supported by huge number of product vendors. However, they are not standardized like TCP, IP, HTTP or SMTP [26].

Most international standardization associations such as IEEE, IETF or W3C have standardized protocols such as 6LowPAN or CoAP and it is believed that other IoT protocols will be standardized like the web standards used today [27]. The IoT might use several application layer protocols and the future of IoT lies in understanding the need of standardizing the protocols majorly used across the network stack. Number of protocols like CoAP, MQTT and 6LowPAN would eventually become as successful as the TCP/IP stack used across the Web and Internet [28].

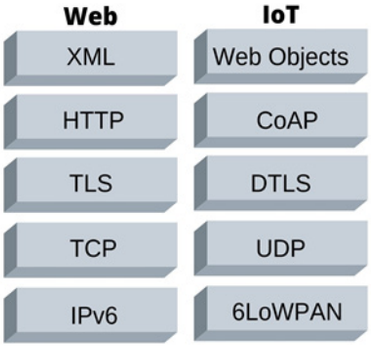

Fig.1 Web protocols vs IoT protocols

D. Comparison of the Web Stack and IoT Stack

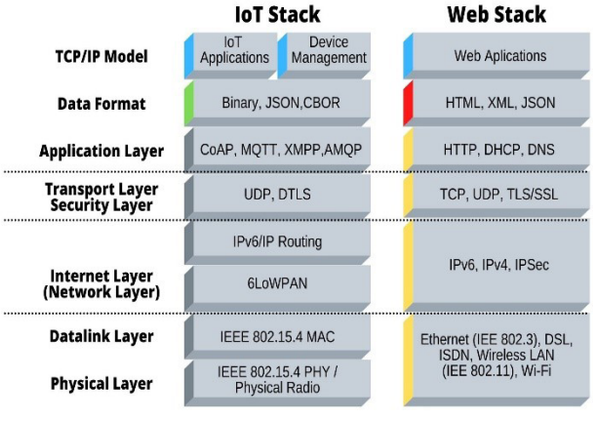

Fig.2 Web Stack vs IoT Stack

Fig.2 summarizes the differences between the IoT stack and the Web stack with an emphasis to the functionalities depending on the various layers.

Starting with the Physical Layer/Radio Frequency layer the IoT Stack uses wireless technologies like Bluetooth, ZigBee, Z-Wave etc. and it uses frequencies as per cellular

or indoor wireless technologies and country wide allocations for the same while, Web Stack has PHY layer and MAC Layer as per LAN or WLAN or DSL or ISDN technologies. Datalink or MAC layer in IoT stack, on the other hand, will use the same IoT wireless technologies as the Physical Layer (Bluetooth, Zigbee, Z-Wave etc.) but it takes care of medium access control and resource allocation and management [29].

Internet Layer (Network Layer) in IoT Stack uses 6LoWPAN to convert large IPv6 packets into small size packets to be carried on wireless medium as per Bluetooth, ZigBee etc. It also does header compression to reduce packet size. The Network Layer in Web Stack does not require protocols like 6LoWPAN. Fragmentation and reassembly is taken care by Transport Layer (i.e. TCP) itself [30].

As mentioned before in the Web Stack for the fragmentation and reassembly care is taken by the Transport Layer which is connection oriented and slower compared to UDP which is used in IoT Stack [26]. UDP is faster due to smaller header size therefore is lighter than TCP. The Security Layer uses Datagram Transport Layer Security (DTSL) in IoT Stack while Web Stack uses TLS/SSL protocols for the same.

The differences between IoT Stack and Web Stack in the Application Layer is in the protocols they use which are CoAP, MQTT, XMPP, AMQP for IoT Stack and HTTP, DHCP, DNS for Web Stack [27].

HTML, XML and JSON Data formats are used by Web Stack while IoT Stack uses CBOR Data format that is based on JSON and uses binary encoding for tiny messages.

IoT Stack is used in constrained network, having low power, low bandwidth and low memory requirements therefore it can transport tens of bytes and Web Stack is used in non-constrained network having no limits on power, bandwidth and memory that is why it can transport hundreds or even thousands of bytes [26].

The IP stack is extremely extensive and it requires big amount of power and memory from the IoT devices. In order for the devices to consume less power they may connect locally on non-IP networks and connect to the Internet through a smart gateway. Bluetooth and RFID are good examples of a non-IP communication with a low range up to few meters and this limits their applications to small personal area networks. To be able to increase the range of those small local networks a modification of the IP stack is needed [15].

2. DISCUSSION

By 2024 the industry, including retail, agriculture and manifacturing is expected to account over 70% of all IoT connections [31]. The number of industrial IoT units in service is expected to grow 180% over the next 4 years. IoT gives us huge advantages. It simplifies our life by providing access to data that otherwise would not be available to us.

The fast growth of the new technologies adobted by users will force the industrial IoT networks to develop rapidly so it can be able to follow and expand the services on their networks. The security issues will grow alongside the network growth, seeking scaling up of the security processes [32]. By knowing and being aware of the risks we can take proper actions to mitigate those risks and to protect ourselves.

IoT has the potential of becoming essential and its future has the opportunity to be limitless. The potential of becoming essential lies not just in enabling billions of devices simultaneously but supporting the huge volumes of actionable data that IoT can manage and through that enabling remote variety of business processes [31].

The design of IoT devices will depend of the selected network technologies and their proper selection requires compromise. What you will choose depends on many factors and priorities such as network range, data rate and power consumption which

are all directly conditionally related. The IoT device will require additional power to transmit the data if you increase the network range or volume of transmitted data [33].

The key point with an IoT device is to protect the network traffic. Typically, those devices use more often wireless network than wired network modules. This creates the demand to protect the transmission traffic between a sensor device and collecting point of data [34].

The rapid developments in Information Communication Technology (ICT) causes digital revolution in the healthcare sector. The top priority in healthcare sector is to provide secure and safer manners of accessing the patients' health and medical information throughout the whole process of medication prescribing process. Blockchain technology assumed to be among one of the suitable way of authentication, authorization and sharing the medication information. The potential of blockchain in e-prescription process is being realized by many involved stakeholders and its immense impact to improve the medication supply and enhanced healthcare economy and revenues. One of the vital on-going obstacle in the current e-prescribing systems is lack of mechanism for authentication and authorization and blockchain is the potential technology to handle this issue. The future of blockchain in the healthcare system seems to be quite prominent and visionary.

However, the practicality of the application for e-prescribing using blockchain is mostly untested yet. From these reasons, for the future, we plan to implement a functional prototype of the proposed architecture, shown in Section 3. A proposed system model are based on an open source community blockchain framework called Hyperledger Fabric. Future work includes implementation and testing of proposed system in closed environment, development of the necessary components of the system, demonstration of the upscaling of the system by allocation of architectural component to different parts of the system and goes to real implementation.

CONCLUSION

The continuous development the Internet of Things leads us believing that predictions for the next decade might become reality even faster than we have imagined. Every day more and more applications are developed in order to satisfy and take advantage of the blooming industry.

In this paper we a closer look at the most common communication technologies for short and medium range low power communication protocols such as RFID (Radio Frequency Identification) Bluetooth, Zigbee, and WiFi. Communication in the IoT world requires special networking protocols and mechanisms. Different set of protocols and standards may be used for communication on the network.

We provided comparison of the Web and IoT protocols and stacks leading us to the conclusion that the most suitable protocol is the one that has precise usage, can be widely deployed and accepted. Knowing the possibilities for each of the protocols will help to choose the best ones according to the corresponding IoT device and IoT application. Therefore, protocols proposed and implemented for each layer of the networking stack should be coordinated to the requirements imposed by the IoT devices.

We hope that this paper will help to the interested parties on choosing the right protocols for IoT deployment in their business, home and industrial applications. Additionally, in our future work and research as logical extension we would also focus on deeper security analysis and comparation of the IoT and standard IP Networking Stacks and threats which might occur due to protocol differences and possible inherent vulnerabilities.

REFERENCES

1. Keyur K Patel, Sunil M Patel , " Internet of Things – IOT : Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challanges", IJESC, vol.6, issue no.5, 2016.
2. Kevin Aston, That 'Internet of Things' Thing , RFID Journal, 2009
3. Xian-Yi Chen, Zhi-Gang Jin, "Research on Key Technology and Applications for Internet of Things", International Conference on Medical Physics and Biomedical Engineering, Physics Procedia 33, pp.561 – 566, 2012.
4. Khanna A., Kaur S., "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review", Wireless Pers Commun 114, pp.1687–1762 , 2020.
5. Jim Royal, "Making sense of the internet of things", video, 2015. [online] Available at: http://jimroyal.com/making-sense-of-the-internet-of-things/, Accessed: March 27, 2021.
6. Angelova Nadezhda, Kiryakova Gabriela, Yordanova Lina, "The great impact of internet of things on business", Trakia Journal of Science 15. pp.406-412, 10.15547/tjs.2017.s.01.068, 2017.
7. Alladi, Tejasvi & Chamola, Vinay & Sikdar, Biplab & Choo, Kim-Kwang Raymond " Consumer IoT: Security Vulnerability Case Studies and Solutions." IEEE Consumer Electronics Magazine. 9. 10.1109/MCE.2019.2953740. 2019.
8. Shaikh, Eman & Mohiuddin, Iman & Manzoor, Ayisha, "Internet of Things (IoT): Security and Privacy Threats." pp.1-6, 2019.
9. Muhammad Raza, OSI Model: The 7 Layers of Network Architecture 2018. [online] Available at https://www.bmc.com/blogs/osi-model-7-layers/, Accessed: March 27, 2021
10. Eltaeib, Tarik. "TCP/IP Protocol Layering". 3. 415-417. 2015.
11. Ansari, Danish Bilal & Rehman, Atteeq-Ur & Ali, Rizwan, "Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP." International Journal of Computer Applications. 179. pp. 9-14, 2018.
12. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.
13. Tschofenig H., Fossati T., "Transport Layer Security (TLS)/Datagram Transport Layer Security (DTLS)" Profiles for the Internet of Things, Internet Engineering Task Force (IETF); Fremont, USA, 2016.
14. Miry, Abbas. "Computer Network Chapter (8) Transport Layer: UDP and TCP" 10.13140/RG.2.2.26835.32809. 2020.
15. Pallavi Sethi, Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035
16. W. Shang et al. , " Challenges In IoT Networking Via TCP/IP Architecture ," NDN Technical Report NDN-0038 , 2016..
17. Tariq, M.A.; Khan, M.; Raza Khan, M.T.; Kim, D. Enhancements and Challenges in CoAP—A Survey. Sensors 2020, 20, 6391. https://doi.org/10.3390/s20216391., 2020.
18. Skvorc Dejan, Horvat Matija, Srbljic Sinisa, "Performance evaluation of Websocket protocol for implementation of full-duplex web streams" 1003-1008. 10.1109/MIPRO.2014.6859715. 2014.
19. Arslan Halil, "Extensible messaging and presence protocol's adaptation to business applications.", Global Journal of Computer Sciences: Theory and Research. 6. 10. 10.18844/gjcs.v6i1.1210., 2016.

20. Malik, Imran & McAteer, Ian & Hannay, Peter & Syed, Naeem & Baig, Zubair, "Security Vulnerabilities and Cyber Threat Analysis of the XMPP Protocol in an IoT Ecosystem", 2018.
21. Van den Abeele, F., Moerman, I., Demeester, P., & Hoebeke, J., "Secure Service Proxy: A CoAP(s) Intermediary for a Securer and Smarter Web of Things.", Basel, Switzerland, 2017. https://doi.org/10.3390/s17071609
22. Bhattacharjya, A.; Zhong, X.; Wang, J.; Li, X., "CoAP—Application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP.", In Digital Twin Technologies and Smart Cities; Springer: Cham, Switzerland, pp. 151–175, 2020.
23. Dan Dinculeană, Xiaochun Cheng, "Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices", MDPI Appl. Sci. 2019, 9, 848; doi:10.3390/app9050848, 2019.
24. PickData, "MQTT vs CoAP, the battle to become the best IoT protocol",https://www.pickdata.net/news/mqtt-vs-coap-best-iot-protocol, Acessed: March 27, 2021.
25. Soni,D., Makwana,A., "A survey: A protocol of internet of things (iot)". Power Analysis And Computing Techniques (ICTPACT-2017), Chennai, India, 2017.
26. C. Gomez, A. Arcia-Moret and J. Crowcroft, "TCP in the Internet of Things: From Ostracism to Prominence" in IEEE Internet Computing, vol. 22, no. 01, pp. 29-41, 2018. doi: 10.1109/MIC.2018.112102200
27. Amine Rghioui,Sendra Sandra , Lloret Jaime, Oumnad Abedlmajid, "Internet of Things for Measuring Human Activities in Ambient Assisted Living and e-Health. Network Protocols and Algorithms," ISSN 1943-3581, Vol. 8, No. 3, 2016.
28. Salman, Tara & Jain, Raj, "A Survey of Protocols and Standards for Internet of Things. Advanced Computing and Communications." 1. 10.34048/2017.1.F3., 2017.
29. Mocnej, Jozef & Pekar, Adrian & Seah, Winston & Kajáti, Erik & Zolotová, Iveta," Internet of Things Unified Protocol Stack" Acta Electrotechnica et Informatica. 19. 24-32. 10.15546/aeei-2019-0011, 2019.
30. Vijay Annamalaisamy,"Introduction to IoT Constrained Node Networks", 2019.
31. Sam Barker, Markus Rothmuller, "The Internet of Things: consumer, industrial & public services 2020-2024", Juniper Research, 2020
32. Abdur Razzaq, Mirza & Habib, Sajid & Ullah, Saleem," Security Issues in the Internet of Things (IoT): A Comprehensive Study." International Journal of Advanced Computer Science and Applications. 8. 10.14569/IJACSA.2017.080650. 2017.
33. Naser Hossein Motlagh, Mahsa Mohammadrezaei, Julian Hunt, Behnam Zakeri, "Internet of Things (IoT) and the Energy Sector, 2020.
34. Cvitić, Ivan & Zorić, Petra & Kuljanić, Tibor & Musa, Mario. (2019). "Analysis of Network Traffic Features Generated by Iot Devices." 2019