Applied Computing Journal https://doi.org/10.52098/acj.202126
ISSN: 2788-9688 Volume 1, Issue 2, pp 66-76, April 2021
Received: 26/4/2021 Revised: 27/5/2021 Accepted: 30/5/2021

DOA- A New Approach to Identify IoT Devices

Mahmood Al-Bahri[1*], Ruslan Kirichek[2], Dmitry Sazonov[2] and Wasin AlKishri[1]

[1] Faculty of Computing and Information Technology, Sohar University, Oman.
[2] The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation.

[*] Corresponding author: Mahmood Al-Bahri, mbahri@su.edu.om

Abstract

The analysis of the possibility of building a system for identifying the Internet of Things devices based on the Digital Object Architecture has been carried out. A model of the resolution handle system of Digital Object Identification as a queuing system is proposed. The analysis of the existing handle system is presented an identification system model based on digital object architecture. Based on the developed model of the queuing system, an optimization experiment was performed. The configuration of the resolution system was obtained, allowing to reduce the time for resolving the device identifier. The software of the existing handle system resolution was analyzed. The ways of improving the algorithms to reduce the time for identifier resolution were proposed.

Keywords: Internet of Things, Digital Object Architecture, Digital Object Identification, Handle System, queuing system, Global Handle Register.

Author(s) and ACAA permit unrestricted use, distribution, and reproduction in any medium, provided the original work with proper citation. This work is licensed under Creative Commons Attribution International License (CC BY 4.0).

1. Introduction

In modern society, a significant part of the market for technical systems is occupied by the Internet and Things. These devices find their place in many areas, ranging from simple household use, medicine and ending with military applications (Al-Bahri et al., 2019a). According to rough estimates, the number of IoT devices is about 28 billion and this figure is growing every year. A huge multitude of IoT devices interact with each other daily, which opens up tremendous opportunities for creating applications of various classes based on smart systems (Al-Bahri et al., 2020).

Obviously, to ensure correct and fast work with a huge flow of information from such devices, a reliable addressing and identification system is required, and therefore a separate area of identification tasks is allocated - the identification of the Internet of things. The main problem in this area is the assignment of unique identifiers and associated metadata to devices of the Internet of Things, allowing them to exchange information with various entities on the Internet (Alattar, et al, 2021). In (Kirichek et al., 2016), the authors considered and below generalized the main features of identification for the Internet of things, namely:

Different life cycle of devices (some IoT objects can exist for a rather long time, while others - vice versa);

The relationship of IoT objects with other entities that are not part of this system (for IoT devices during the life cycle, owners and administrators can change, which affects the processes of identification, authentication, and authorization) (Al-Bahri et al., 2019b).

Special requirements for the context in which the devices operate (in certain cases, access of objects to the same data can be allowed or limited depending on the situation). Requirements for the provision of protection mechanisms (when designing these mechanisms, it is worth considering the limited resources and performance of IoT devices).

The ability to expand the identification system to a huge number of devices (over a billion). The ability to work effectively for a wide variety of devices (devices in the IoT network can be extremely heterogeneous in their resources and performance. Transparency of the addressing system and independence from the network (in contrast to the classical addressing systems used, for example, on the Internet network, the identification of Internet of things devices should be independent of which network they are in or which user they belong to; in addition, it should be borne in mind that devices of the Internet of Things can change their location, but at the same time be uniquely identified in the network) (Al-Bahri et al., 2018a).

A flexible and effective mechanism for resolving identifiers (IoT devices must be accurately identified regardless of their location; in addition, there must be simplicity in connecting and configuring a new IoT object to an existing

network). Safety and security of user data (do not forget that IoT devices often work with a huge amount of personal data, which requires additional protection measures) (Al-Bahri M et al., 2018b).

Today, there are several approaches to building an identification system for devices in the Internet of things. One of the possible solutions to the arisen problem is the use of an identification architecture based on the architecture of digital objects DOA (from the English. Digital Object Architecture).

2. General concept of Digital Objects Architecture

As shown in the article (Kirichek et al., 2016), the existing information management systems in the network are based on the classical client-server architecture. The server in such a system is a place for storing information and processing requests from clients to work with this information. DOA, in contrast to this approach, seeks to resolve the issue not of localization, but of the context of a digital object (Lin et al, 2020;(Kahn & Wilensky, 2006).

A digital object in this architecture is characterized not only by information about its location. In addition, it is possible to obtain various information about the object itself: requirements for access, authentication, information about the author, etc. (Koucheryavy et al., 2011). All this information is entered by the creator of the digital object himself. For this purpose, a special infrastructure is integrated into the DOA, providing the necessary encryption and access verification.

The main building blocks of DOA are the digital object, the Handle System, and the digital object repository and registry. Let us dwell on the principles of the resolution system in more detail.

Each digital object in the described architecture is assigned a unique identifier - DOI (Digital Object Identificatory). This identifier is somewhat reminiscent of the URL based on which the modern Internet is built. However, unlike the latter, the assigned identifiers remain constant and do not depend on the state of the digital object. It is the resolution system that connects the identifier with information about the status of a digital object (location, access, information about authenticity) (Phupattanasilp & Tong, 2019). In the classical architecture DOA, the resolution system is two-level. The first level of resolution is the Global Handle Registry (GHR); the second level is a set of Local Handle Registry (LHR) or Local Handle Service (LHS). To resolve the identifier in this subsystem, first there is an appeal to the global register GHR, which reports information about the local register LHR, which contains the necessary information about the digital object. This process is shown schematically in Figure 1.

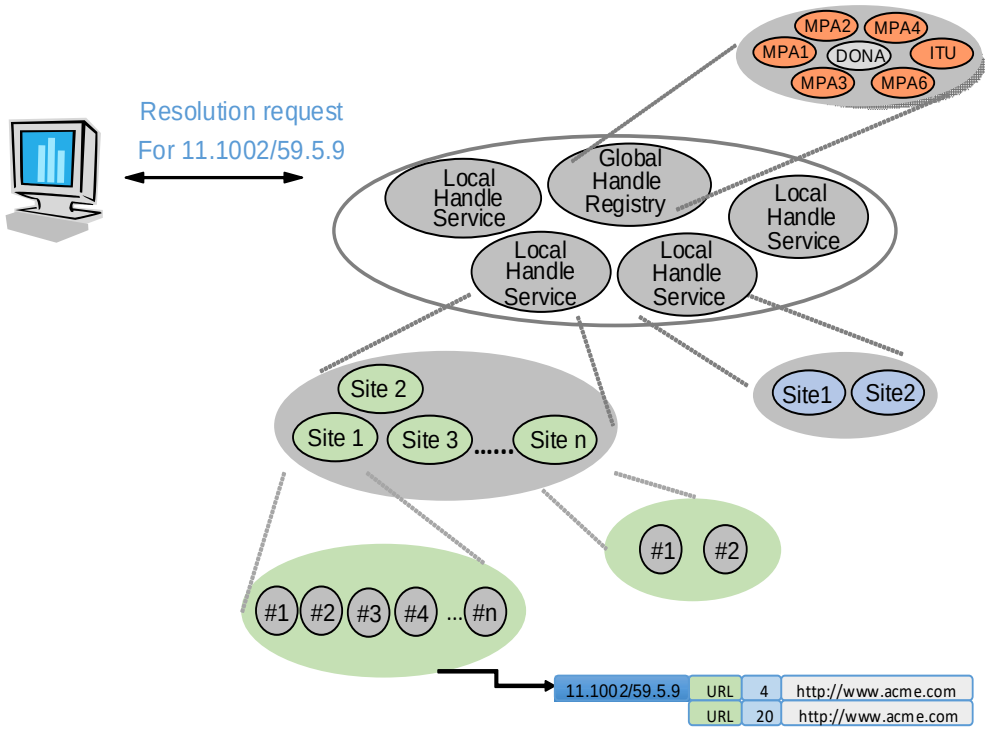


Figure 1. Structure of the Handle System

The very structure of the DOA identifier also corresponds to the two-level system (Thai, 2012). For example, consider the identifier: 10.1000 / 123abc. The first part, located before the "/", is called the prefix; the second part is a suffix. The prefix allows you to set the local registry information for the LHS digital object. This correspondence between prefix and administrator information is stored in the GHR global registry. The suffix already uniquely identifies a specific object, and this information connecting the suffix with a specific object is stored in the Local Handle Service LHS (Shortle et al., 2018).

3. Resolution system simulation model

In order to characterize the efficiency of the identifier resolution system in the DOA architecture when applied to the identification problems of the Internet of Things, let us consider the resolution system as a CMO (mass service system).

It was decided to take the M/M/s model as the QS system. This model characterizes a system with an exponential distribution of the time for servicing requests and an exponential distribution of the time between the arrival of requests (Handle, 2021). There are more research studies related implementing clod computing for Systems Modelling and

enterprise planning (Yousif & Alattar, 2017; Saini et al, 2011). In addition, the model meets the following important conditions:

- The presence of several processing channels (in this model, we will consider the GHR servers as an independent entity, only processing incoming requests).
- There is no limitation on the length of the GHR buffer (every request entering the system will be served).
- There is no priority for incoming requests, each request is processed in the sequence in which it entered the system.

It is worth noting that when analyzing the processing of request traffic over a long period of time (for example, a day), the selected model will no longer be valid. However, this model can be used for short periods of time. An interval of 200 s was chosen as the operating time of the system.

The model of the resolution system as CMO was implemented by analyzing the existing implementation of the resolution system (Al-Bahri et al., 2019; Al-Bahri M et al., 2018a; Lin et al, 2020). The existing architecture uses not one GHR server, but several servers belonging to the MPA (Multi-Primary Administrators) controlled by the DONA Foundation (Al-Bahri et al., 2020; Kahn & Wilensky, 2006). Each MPA server is a GHR capable of resolving incoming requests. By analyzing the operation of the software provided by Han-dling.net, the infrastructure of the top-level global register servers was established and the average latency for resolving a request by these servers was determined. In this software, all MPA servers are equivalent between themselves and the request for permission is sent sequentially to all servers and the response that came first is analyzed. At the same time, there is no accounting and analysis of the delay time to the server. In essence, the resolution system guarantees that if a request for permission enters the system, then it will certainly be fulfilled, however, the time that may be required for this is not clearly regulated (Lin et al, 2020; Koucheryavy et al., 2011). Table 1 shows the characteristics of the MPA servers used as GHRs in the current resolution system architecture.

Figure 2 depicts a basic queuing process flowchart that looked at the identifier resolution process. simulation modeling of the queuing system developed in anylogic.

The client’s element corresponds to the origin of requests to resolve IDs from devices. Then there is a branching into 8 channels, each of which corresponds to the infrastructure of a specific MPA. The probability of choosing each of the channels in the existing system is the same. Each MPA server is a set of claims buffer and ID processing server.

In this case, the number of channels in the processing server corresponds to the number of servers for each specific MPA, presented in Table 1.

Table 1. Characteristics of MPA servers

MPA	IP address	Average latency per resolution, ms
Average latency nCNRI (America)	132.151.20.9; 38.100.138.153; 38.100.138.131; 132.151.20.9; 2001:550:100:6::138:153; 2001:550:100:6::4; 132.151.1.179	243.548
ITU (Switzerland)	156.106.193.160	71.33
Beijing Flash Newsletter Cas Telecommunication (China)	119.90.34.34	473.583
Alicloud (China)	47.90.103.77	410.693
ATI - Agence Tunisienne Internet (Tunisia)	41.231.118.2	82.510
Gesellschaft Für	134.76.30.197	44.356
Wissenschaftliche	86.111.195.107	318.450
Datenverarbeitung Mbh Göttingen (Germany)	196.12.152.22	258.450

It should be noted that, only the upper level of GHR and the next level of work of the system with LHS was not analyzed. Interaction with local servers and analysis of their configuration should be considered separately within the framework of a specific problem being solved.

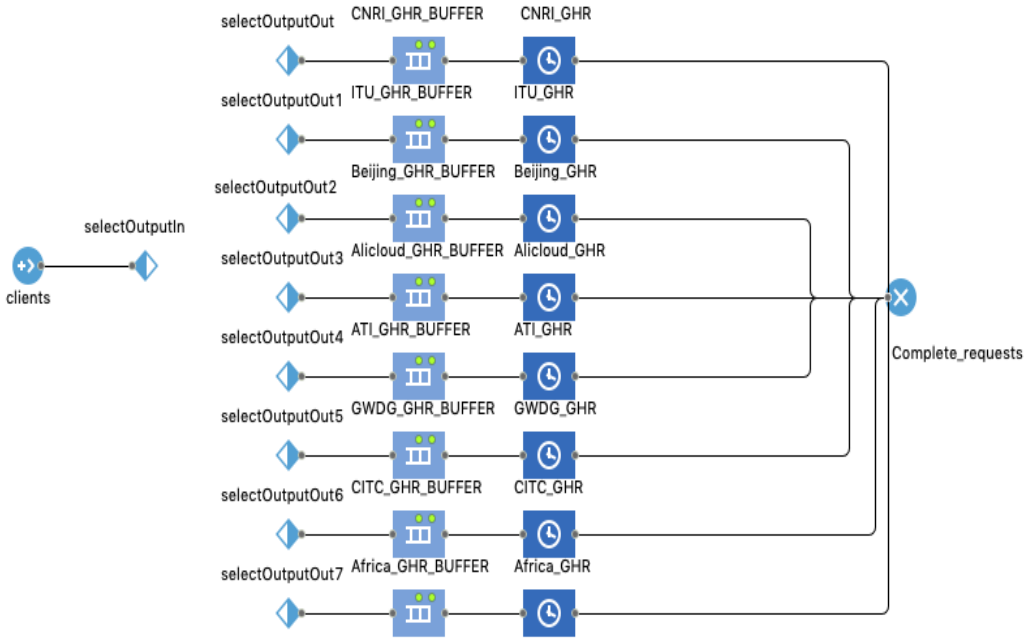
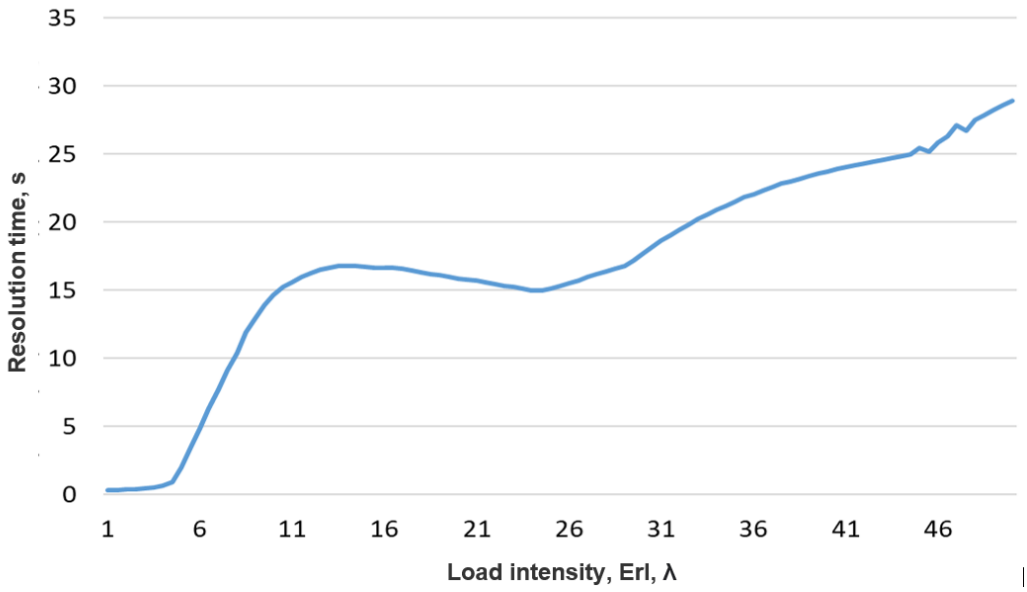


Figure 2. Simulation model of the system of resolution of the identifier of digital objects as a СМОреальности (Shortle et al., 2018).

4. Simulation Results

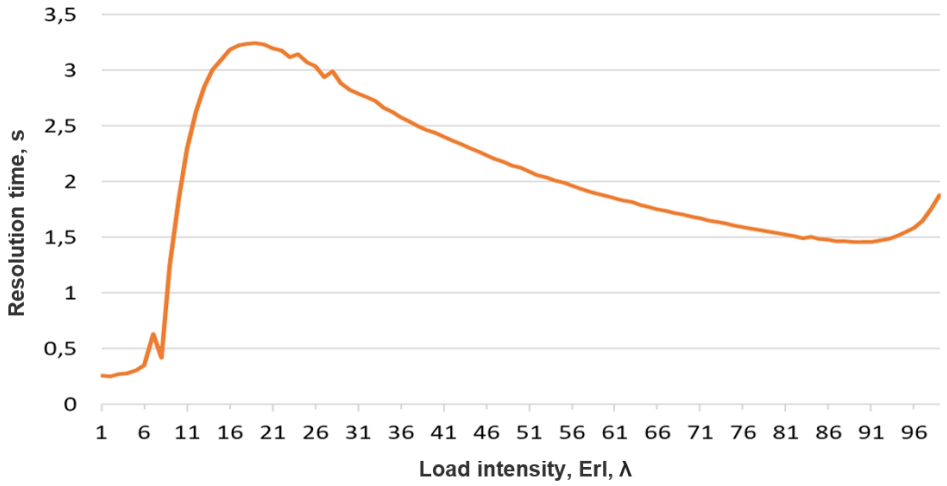
Since the DOA system is built based on a network architecture that already exists at the moment for the global Internet, the main parameters affecting the operation will be the amount of network delay for an incoming request, the speed of processing the request by the server responsible for resolution, and the number of processing channels for each MPA.

The characteristic of the resolution system, which is critical for identifying the Internet of Things, is the average service time of one request. This time will depend on both the system configuration and the intensity of the load. Figure 3-a (blue line) shows the dependence of the average time of identifier resolution on the intensity of incoming requests for the current system configuration. As can be seen from the graph, with an increase in the load intensity, the average resolution time for one identifier also increases, and under heavy loads this time reaches 30 seconds, which is quite a lot for real applications, especially when compared with the indicators of the DNS system.



a)

Figure 3-b (orang line) shows the curve of the dependence of the request resolution time on the intensity of requests arriving when configuring servers, taken as a result of the optimization experiment. Using the capabilities of the Anylogic environment, we will conduct an optimization experiment aimed at establishing the most suitable infrastructure for GHR servers with the current configuration of time delays in order to reduce the average time of identifier resolution.



b)

Figure 3. Dependence of the resolution time on the intensity of requests (a) and with optimal configuration (b)

The main parameter for optimization will be the number of GHR servers used by each MPA. As an objective function, we will strive to minimize the request resolution time. Let's set the resolution time to no more than 1 second. Let's set the value of the intensity to 50 Lambda (better with an icon). Where lambda (by the icon) is the parameter of the exponential distribution of the time of receipt of applications. The optimization results are shown in Figure 4.

	Current	The Best
Interacting	500	60
functional	3,947	0,878
Parameters		
Alfa	50	50
d1	7	7
d2	9	10
d3	4	1
d4	9	10
d5	8	10
d6	8	10
d7	10	10
d8	8	10

Figure 4. Parameters of the optimization experiment

In the created model, alfa is the load intensity parameter; d1 ... d8 is the number of servers for each MPA. The graph in Figure 4 shows that with this configuration of GHR servers, the resolution of the identifier in the system is much faster. An increase in speed by 15 times is achieved at the maximum load intensity.

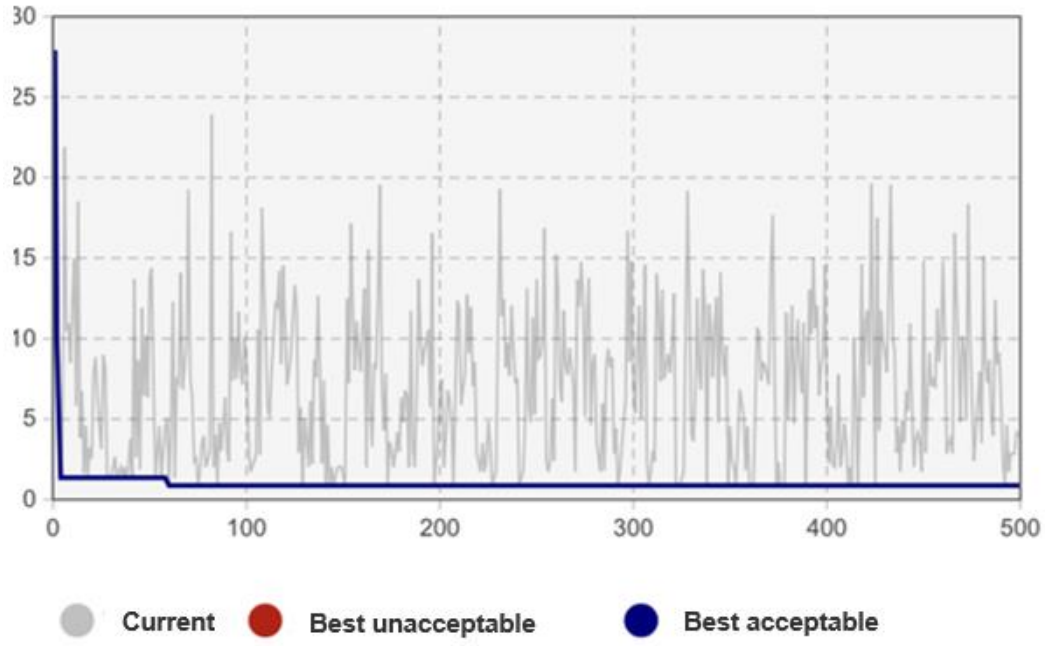


Figure 5. Results of the optimization experiment

Figure 5 shows the iterative optimization process for the developed QS model. The optimization process consists in the sequential launch of the model with varying the optimization parameters (the number of GHR servers) to achieve the set goal (the resolution time of the identifier is less than 1 sec.). The graphs in Figure 5 show a graph of sequential optimization of the optimization objective function and calculating an optimization function for the parameters of the current iteration (gray graph) and parameters of the best case (blue graph). At the end of the optimization process, we get a set of parameters (the number of GHR servers) that are closest to giving the result of the resolution time for identifiers no more than 1 sec. For the current configuration of the model, the number of servers is **7, 10, 1, 10.10, 10, 10.10** for each MPA from Table 1, respectively

5. Conclusion

Based on the results of system modeling, it can be concluded that the current infrastructure of the resolution system requires further scaling and distribution in order to be able to withstand heavy loads and minimize the resolution time of incoming requests. This is especially true when using the DOA architecture and the resolution system in tasks

related to the identification of devices in the Internet of Things, the number of which is estimated at billions; In this case, the intensity of requests in the resolution system can be extremely high.

In addition to the infrastructural expansion of the existing system, improvements need to be carried out in the program part of the resolution system. As mentioned earlier, as a result of the analysis of the open-source code of the library provided by Handling.net for building their own client solutions for interacting with the resolution system, it was found that when sending a request for identifier resolution to the GHR servers, no preliminary analysis of the network latency time to each of the servers. Each server from the list shown in Table 1 is polled in a random sequence and the first response received is analyzed. This implementation undoubtedly affects the overall time of identifier resolution. Therefore, further modification of the original is required in order to create functionality for sorting and prioritizing GHR servers, depending on the network delay from the client device.

Acknowledgment

The research leading to these results has no Funding.

REFERENCE

[1]. Al-Bahri, M., Kirichek, R., & Borodin, A. (2019a). The Digital Object Architecture as a Basis for Identification in the Era of the Digital Economy. Elektrosvyaz', (1), 12.

[2]. Al-Bahri, M., Al-Wardi, S., Dharamshi, R. R., Al-shukail, N., & Muthanna, A. (2020, November). A Smart System Based on Digital Object Architecture to Verify the Diploma Certificates. In 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI) (pp. 1-5). IEEE.

[3]. Alattar, F. N. H., & Azeez, A. (2021). Design and Implementation of an Energy Meter System for Optimized Cost using Internet of Things (IOT) Technology. Applied Computing Journal, 1(Issue 1), 55-65.

[4]. Kirichek R., Kulik V., Koucheryavy A. (2016) False clouds for Internet of Things and methods of protection. Proceedings of the 18th International Conference on Advanced Communication Technology (ICACT), 31 January–3 February 2016 Pyeongchang, South Korea. Piscataway, NJ: IEEE. p.201–205. Available from: https://doi.org/10.1109/ICACT.2016.7423328

[5]. Al-Bahri M., Yankovsky A., Kirichek R., Borodin A. (2019b). Smart System Based on DOA and IoT for Products Monitoring and Anti-Counterfeiting. Proceedings of the 4th MEC International Conference on Big Data and Smart City (ICBDSC), 15–16 January 2019, Muscat, Oman. Piscataway, NJ: IEEE,. Available from: https://doi.org/10.1109/ICBDSC.2019.8645610

[6]. Al-Bahri M., Yankovsky A., Borodin A., Kirichek R. (2018). Testbed for Identify IoT-Devices Based on Digital Object Architecture. Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Proceedings of the 18th International Conference, NEW2AN, and 11th Conference, ruSMART, St. Petersburg, Russia, 27–29 August 2018. Lecture Notes in Computer Science, vol. 11118. Cham: Springer. p.129–137. Available from: https://doi.org/10.1007/978-3-030-01168-0_12

[7]. Albahri M., Kirichek R., Ateya A.A., Muthanna A., (2018b). Borodin A. Combating Counterfeit for Io T System Based on DOA. Proceedings of the 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, Moscow, Russia, 5–9 November. Piscataway, NJ: IEEE; 2018. Available from: https://doi.org/10.1109/ICUMT.2018. 8631257

[8]. Lin, Z., Lv, T., Ni, W., Zhang, J. A., & Liu, R. P. (2020). Nested Hybrid Cylindrical Array Design and DoA Estimation for Massive IoT Networks. IEEE Journal on Selected Areas in Communications.

[9]. Kahn, R., & Wilensky, R. (2006). A framework for distributed digital object services. International Journal on Digital Libraries, 6(2), 115-123. Available from: https://doi.org/10.1007/s00799-005-0128-x

[10]. Koucheryavy, A. E., Prokopiev, A. V., & Koucheryavy, Y. A. Samoorganizuiushchiesia seti [Self-Organizing Network]. St. Petersburg: Lyubavich Printing House; 2011. 312 p.

[11]. Phupattanasilp, P., & Tong, S. R. (2019). Augmented reality in the integrative Internet of Things (AR-IoT): Application for precision farming. Sustainability, 11(9), 2658.

[12]. Thai N.D. (2012). Remote Computing Through MATLAB Web-Server as Queueing System. Proceedings of Irkutsk State Technical University, 4(63):25–32.

[13]. Shortle J.F., Thompson J., Gross D., Harris C.M. (2018). Fundamentals of Queueing Theory. Hoboken: John Wiley & Sons. , 576 p.

[14]. Handle. (2021) Handle.Net Registry. Available from: http://www.handle.net/index.html [Accessed 22nd March 2021].

[15]. Yousif, J. H., & Alattar, N. N. (2017). Cloud management system-based air quality. International Journal of Computation and Applied Sciences (IJOCAAS), 2(2).

[16]. Saini, S. L., Saini, D. K., Yousif, J. H., & Khandage, S. V. (2011, July). Cloud computing and enterprise resource planning systems. In Proceedings of the world Congress on Engineering (Vol. 1, pp. 681-684).

Author(s) and ACAA permit unrestricted use, distribution, and reproduction in any medium, provided the original work with proper citation. This work is licensed under Creative Commons Attribution International License (CC BY 4.0).