Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.026115
Article

Tech Science Press

Digital Object Architecture for IoT Networks

Mahmood Al-Bahri[1], Abdelhamied Ateya[2,3], Ammar Muthanna[3], Abeer D. Algarni[4] and Naglaa F. Soliman[4,*]

[1]Department of Computing and IT, Sohar University, Sohar, 311, Oman
[2]Department of Electronics and Communications Engineering, Zagazig University, Zagazig, 44519, Sharqia, Egypt
[3]Telecommunication Networks and Data Transmission, St. Petersburg State University of Telecommunication, St. Petersburg, 193232, Russia
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
*Corresponding Author: Naglaa F. Soliman. Email: nfsoliman@pnu.edu.sa
Received: 15 December 2021; Accepted: 10 February 2022

Abstract: The Internet of Things (IoT) is a recent technology, which implies the union of objects, "things", into a single worldwide network. This promising paradigm faces many design challenges associated with the dramatic increase in the number of end-devices. Device identification is one of these challenges that becomes complicated with the increase of network devices. Despite this, there is still no universally accepted method of identifying things that would satisfy all requirements of the existing IoT devices and applications. In this regard, one of the most important problems is choosing an identification system for all IoT devices connected to the public communication networks. Many unique software and hardware solutions are used as a unique global identifier; however, such solutions have many limitations. This article proposes a novel solution, based on the Digital Object Architecture (DOA), that meets the requirements of identifying devices and applications of the IoT. This work analyzes the benefits of using the DOA as an identification platform in modern telecommunication networks. We propose a model of an identification system based on the architecture of digital objects, which differs from the well-known ones. The proposed model ensures an acceptable quality of service (QoS) in the common architecture of the existing public communication networks. A novel interaction architecture is developed by introducing a Middle Handle Register (MHR) between the global register, i.e., Global Handle Register (GHR), and local register, i.e., Local Handle Register (LHR). The aspects of the network interaction and the compatibility of IoT end-devices with the integrated DOA identifiers in heterogeneous communication networks are presented. The developed model is simulated for a wide-area network with allocated registers, and the results are introduced and discussed.

Keywords: Internet of things; identification; digital object architecture; handle system; security

1 Introduction

Nowadays, Information Technology (IT) is developing rapidly [1]. Internet of Things (IoT) represents the main paradigm that comes with many applications in all daily life fields [2]. It enables the interactions between end-devices via machine-to-machine (M2M) communications. This promising technology faces many design challenges associated with integration, identifications, and scalability. Integrating IoT devices with other network parts and recent technologies is a challenge. Moreover, another challenge is integrating IoT networks with other existing networks, e.g., fifth-generation cellular systems (5G), and future networks, e.g., vehicular networks and sixth-generation cellular systems (6G).

The massive increase in the number of wireless sensors and devices exponentially introduces other design challenges to IoT networks. These challenges are mainly concerned with network scalability and devices identifications. All recent developments in IoT sectors force the introduction of mechanisms for the unambiguous identification of devices and applications of the IoT. These mechanisms should allow tracking the reliability of the information on the network and counterfeit combat Information and Communication Technology (ICT) products [3]. Proposals for creating such a register of objects are put forward by the international telecommunication union's (ITU) copyright holders and collective rights management societies [4].

There is a demand to choose the most optimum identification system for IoT networks. For identification, there are different software and hardware solutions that include Internet Protocol version 6 (IPv6), a bunch of Internet Protocol version 4 (IPv4) + Media Access Control (MAC), and International Mobile Equipment Identity (IMEI) [5]. However, the common drawbacks of these systems are the ability to programmatically change the identifier of the network interface and binding to hardware identifiers, which excludes the possibility of identifying digital content. These shortcomings are deprived of alternative software solutions for identification, such as Digital Objects Architecture (DOA), Uniform Resource Identifier (URI), Extensible Resource Identifier (XRI), and Internationalized Resource Identifier (IRI) [6–9]. These systems make it possible to identify any virtual or real object in the public telecommunication network (PTN), regardless of the presence or absence of a network interface [10]. These systems, e.g., hardware identification systems, use various third-party technologies to authenticate physical and digital objects [11].

The choice of the optimal system is determined by the following requirements of identification technologies that take into account its use in the public communication networks [4,10], and [12].

- Identification systems must respond to multiple requests;
- In order to work with identifiers, it is necessary to implement different access levels, i.e., user authorization system;
- The database containing the data must be separated from the identification object itself; and
- Identifiers should not contain dynamic elements or metadata.

The work on standardization of methods for identifying and combating counterfeiting based on the DOA is currently underway in the ITU-T Study Group 20 [13]. In December 2018, the recommendation “Architecture for the interaction of Internet devices based on the architecture of digital objects” was submitted to the consent procedure. In 2019, the recommendation “Decision Framework for Combating Counterfeit Internet of Things Devices Based on the Architecture of Digital Objects” was adopted. In this regard, a joint technical solution based on many IoT– DOA identifiers can be considered an effective technological chain [14]. In the module that interacts with the network infrastructure, a DOA identifier can be written, which will include all the unique parameters of an object (metadata). The proposals for such a solution can be diverse: ICT, pharmaceutical and automotive industries, aircraft manufacturing, etc. In particular, they can be used to combat counterfeit goods.

The main contributions of this article can be introduced in the following points.

1) Introducing the well-known DOA system with the main components and the handle system,
2) Developing a novel model of an identification system, based on the architecture of digital objects,
3) Developing a novel solution for identifying IoT end-devices based on the DOA,
4) Introducing the main benefits of using the proposed DOA based structure as an identification platform for modern communication networks; mainly for IoT based networks,
5) Introducing a novel interaction architecture for IoT systems that represents a modification of the well-known handle system; by introducing a Middle Handle Register, MHR, and
6) Evaluating the performance of the proposed modified DOA system.

2 Background and Related Works

Nowadays, the concept of IoT is an advanced platform that turns blind devices into smart ones through M2M interactions [15]. According to current statistics and predictions, over the next five years, more than 25 billion devices will be connected [16]. Despite all the advantages of the IoT, there have recently been cases of disclosure of data collected by IoT devices. These issues create anxiety about the identity of devices and applications as part of the Internet of Things concept. The identification process is an important part of the IoT networks, affecting overall network performance. Since attackers can use mobile Radio-Frequency Identification (RFID)/Near-Field Communication (NFC) readers to hack private data from bank cards using technology vulnerabilities like PayPass. This is possible due to the lack of identification of the owner of the RFID reader [17]. Another example is the ability of an attacker to intercept data from networks of IoT devices to obtain International Mobile Equipment Identity (IMEI) and identifiers of various terminal devices equipped with modems for subsequent broadcasting of intentionally distorted messages [18].

The manufacturers of IoT devices tend not to implement complex security mechanisms for IoT end devices, mainly due to resource constraints and device cost. This makes the resources-based security, such as Trusted Platform Modules (TPMs), inefficient for IoT devices [19,20]. These forms and other forms of complex security require additional hardware components. They are part of device resources, affecting the overall device cost, size, and available resources for computing tasks. Intrinsic Physical Unclonable Functions (PUFs) is another tool used for securing IoT devices [21]. PUFs are implemented over Dynamic Random-Access Memory (DRAM) since many IoT devices deploy DRAM modules. However, PUF is not commonly used since it is affected by ambient temperature variations [22].

Current solutions, known worldwide, aim to associate an IoT device or application with an identifier similar to an Internet Protocol (IP) address or mobile phone number. These identifiers allow understanding only: who is using this or that device. Research in this area was initiated as a result of a discussion of these issues with the Body of European Regulators for Electronic Communications (BEREC) regulatory authority [23,24]. To the best of our knowledge, this work introduces the first identification method for IoT devices and applications based on a standardized, reliable platform, i.e., DOA. The proposed solution differs completely from the existing identifiers, e.g., IP, IME, used for other wireless devices, since it cannot be hacked. The proposed identifier is built upon the DOA platform instead of embedding the identifier in the devices. The proposed system stores the identifiers in the reliable, high secure DOA registers.

Different identifiers are used based on the scope and requirements of users. Things and users must be uniquely identified to understand the uniqueness of a particular interaction object. Many other entities are also involved in the interaction while being part of the ecosystem of IoT. The interaction of various entities with the associated identifiers within the framework of the IoT concept is shown by the example of the Alliance for Internet of Things Innovation, AIOTI, 's WG03 High-Level Architecture presented in Fig. 1 [25].

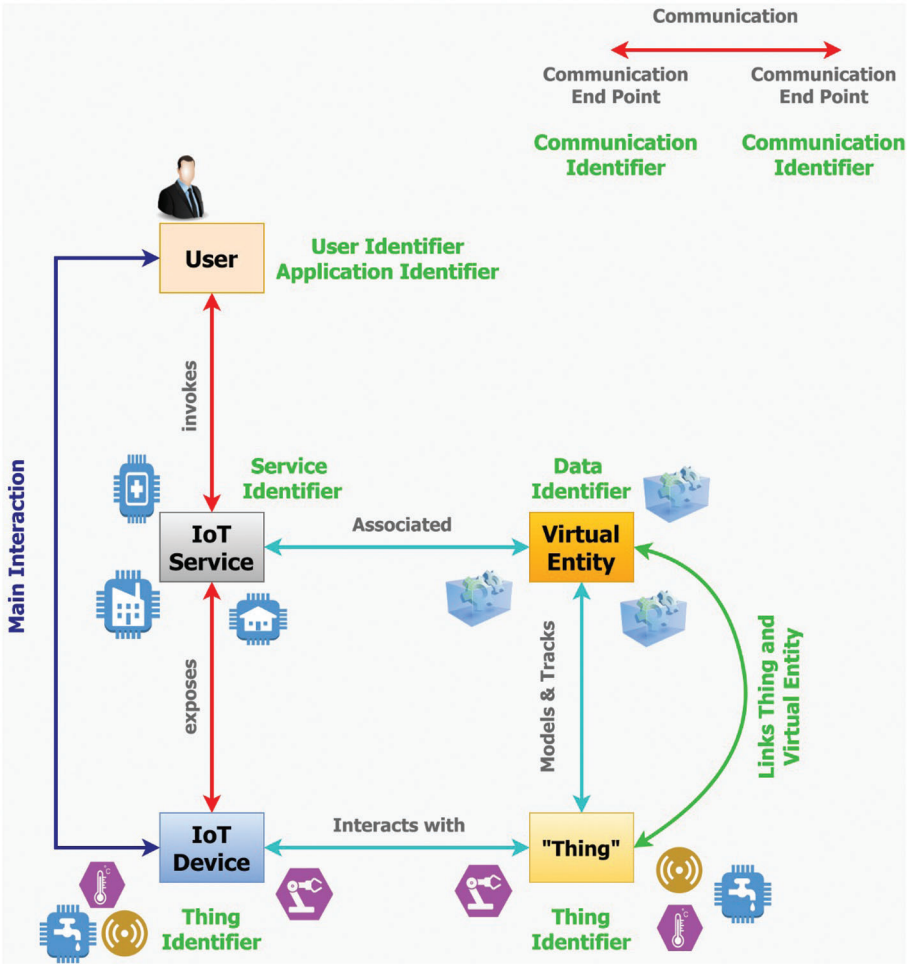


Figure 1: An example of the interaction of various entities with associated identifiers in the framework of the concept of IoT

3 Proposed System Structure for IoT Networks

We aim to break the handle system by introducing intermediate level registers between the GHR and the distributed LHRs [26,27]. These middle registers can be referred to as the mid registers (MHRs). Each MHR can serve a certain geographical region on the world map based on the density, the number of devices, and the density of manufacturers, i.e., the density of LHRs. LHR communicates with the near MHR instead of the far GHR, which reduces the communication distance and overall communication latency. Fig. 2 illustrates the system level structure with new MHRs.

The optimum number of MHRs and their optimal distribution is an optimization problem that should be solved in terms of overall system cost and communication latency. MHRs may be located at the circumference of a circle of radius R centered at Geneva, where the GHR is located, where R is a design parameter and can be obtained by solving a linear optimization problem.

The system has a main register, i.e., global handle register (GHR), located in the city of Geneva. GHR connects all mid handle registers (MHR) deployed in the system. For modeling purposes, we refer to GHR as $G\ (l,\ h,\ \varphi,\ \lambda)$, where l and h are the coordinates, and φ and λ are the longitude and latitude of the GHR's location. The set of MHRs is $M_i^j(l_i^j,\ h_i^j,\ \varphi_i^j,\ \lambda_i^j),\ j = 1,\ 2,\ 3,\ \ldots,\ N$. Where, l_j and h_j are the

coordinates, and φ_j and λ_j are the longitudes and latitude, of the location of the j^{th} mid register, and N is the total number of middle registers deployed in the system.

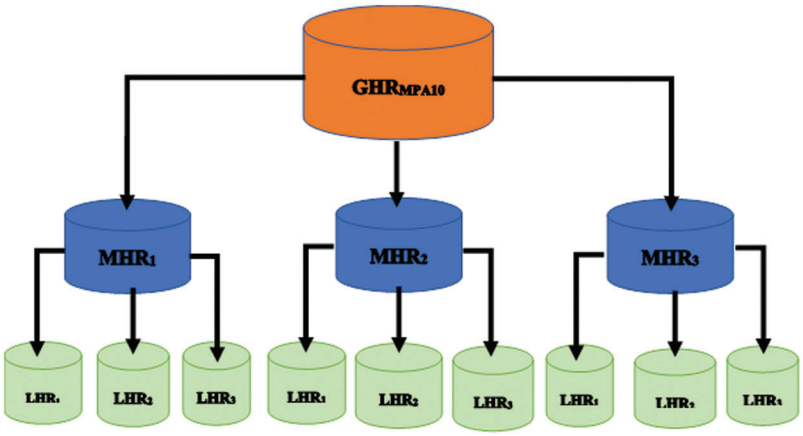


Figure 2: System-level of the modified handle system

Each mid register MHR connects and controls a group of local handle registers (LHRs). The set of LHRs connected to the j^{th} MHR is $L_i^j(l_i^j, h_i^j, \varphi_i^j, \lambda_i^j)$, $i = 1, 2, 3, \ldots, M_j$. Where $l^j{}_i$ and $h^j{}_i$ are the coordinates, and $\varphi^j{}_i$ and $\lambda^j{}_i$ are the longitudes and latitude of the location of the i^{th} LHR connected to the j^{th} MHR. M_j is the total number of LHRs connected to the j^{th} MHR register, which is characterized by l_j, h_j, $\varphi_j$and λ_j.

Since the communication latency between the two communicated servers, L, is directly proportional to the communicated distance between the transmitter and the receiver, D, as indicated in (1).

$$L \propto D \tag{1}$$

For the proposed system, the communications are mainly done between the LHR and the associated MHR. Thus, the system latency for the proposed system can be calculated as follows.

$$L_i^j \propto D_i^j \tag{2}$$

$$D_i^j = \sqrt{(l_i^j - l_j)^2 + (h_i^j - h_j)^2} \tag{3}$$

where, $L^j{}_i$ is the communication latency for the data communicated between i^{th} LHR and the j^{th} MHR, and $D^j{}_i$ is the distance between the position of the transmitter of the i^{th} LHR and the receiver of the j^{th} MHR.

For the handle system with the structure of no MHRs, the LHR registers communicate with the GHR. Thus, the communication latency is calculated between the LHR and GHR, which maintain their locations in both systems, i.e., the handle system with MHRs and the old handle system with no MHRs. The latency for the old system with no MHRs can be calculated based on the following equation:

$$L_i^{GHR} \propto D_i^{GHR} \tag{4}$$

$$D_i^{GHR} = \sqrt{(l_i^j - l)^2 + (h_i^j - h)^2} \tag{5}$$

where, L_i^{GHR} is the communication latency for the data communicated between i^{th} LHR and GHR register, and D_i^{GHR} is the distance between the position of i^{th} LHR and the position of GHR. To compare the handle

system with no MHRs, i.e., the old handle system, and the new structure for the handle system, i.e., with the deployment of MHRs, Eqs. (4) and (2) are divided as follows.

$$\frac{L_i^{GHR}}{L_i^j} \propto \frac{D_i^{GHR}}{D_i^j} \tag{6}$$

$$\frac{L_i^{GHR}}{L_i^j} \propto \frac{\sqrt{(l_i^j - l)^2 + (h_i^j - h)^2}}{\sqrt{(l_i^j - l_j)^2 + (h_i^j - h_j)^2}} \tag{7}$$

Since,

$$D_i^j \text{ " } D_i^{GHR} \tag{8}$$

Thus,

$$L_i^{GHR} \text{ " } L_i^j \tag{9}$$

Thus, the proposed handle system achieves better performance in terms of latency by reducing the communication distance between the communicated servers. This can be achieved by deploying an intermediate level of handle registers (MHRs). The distances D_i^j and D_i^{GHR} can be calculated alternatively, based on the information of the longitude φ and latitude λ of the register's location. To calculate the shortest distance between two places based on their longitudes and latitudes, we use the haversine formula to estimate the circle distance between any two points, defined by their longitudes and latitudes.

$$A_i^j = Sin^2\left(\frac{\Delta\varnothing_{j,i}^j}{2}\right) + \cos\varnothing_j \cdot \cos\varnothing_i^j \cdot Sin^2\left(\frac{\Delta\lambda_{j,i}^j}{2}\right) \tag{10}$$

$$C_i^j = 2 \cdot arctan2\left(\sqrt{A_i^j},\ \sqrt{1 - A_i^j}\right) \tag{11}$$

$$D_i^j = R \cdot C_i^j \tag{12}$$

$$A_i^{GHR} = Sin^2\left(\frac{\Delta\varnothing_{GHR,\,i}}{2}\right) + \cos\varnothing_i \cdot \cos\varnothing_{GHR} \cdot Sin^2\left(\frac{\Delta\lambda_{GHR,i}}{2}\right) \tag{13}$$

$$C_i^{GHR} = 2 \cdot arctan2\left(\sqrt{A_i^{GHR}},\ \sqrt{1 - A_i^{GHR}}\right) \tag{14}$$

$$D_i^{GHR} = R \cdot C_i^{GHR} \tag{15}$$

where, R is the earth's radius.

4 IoT Device Structure and Resolution Process

Having an identification service that includes a resolution process is a key requirement for IoT systems and, at the same time, a basic DOA principle. However, the architecture of digital objects has a special requirement for identifiers within the architecture. Namely, the possibility of resolving an identifier in metadata about an object whose resolution is taking place, or as in our case, about an Internet of Things object. Access control provides access only to certain values in the metadata [28].

Implementing DOA for IoT devices implies assigning each device a unique identifier (Handle). The identifier is mainly used to identify the device and store related information. The identifier prefix should define the country and the main region, while the suffix indicates information of a particular IoT device. Using the identifier prefix, you can obtain information about the required Local Handle Service (LHS) through the Global Handle Registry (GHR), thereby gaining access to all information related to the IoT device that is marked with this identifier (prefix + suffix) [25].

The Global Record Register (GRR), which is the same as GHR, is a registry that combines distributed local service registries (LHS) [29]. LHS can be defined for a particular manufacturer and located on its territory or, conversely, be a universal service for many manufacturers.

A preliminary goal for introducing DOA in IoT is the fight against counterfeit products in the Internet of Things. The user is allowed to verify the characteristics of the IoT device using the handle system [4]. The user can extract the identifier prefix using special technology, e.g., RFID and NFC, request the GHR server to determine the location of the LHS service, which has direct information about a particular IoT device. The GHR responds to such a request with a message containing the address of the requested LHS service. The device carries out a new request at the received address, to which it receives a message with data on a specific identifier with all the necessary information, which is monitored and modified only by the device manufacturer. Fig. 3 shows the structure and procedures for checking IoT devices for counterfeiting using the DOA system [4].

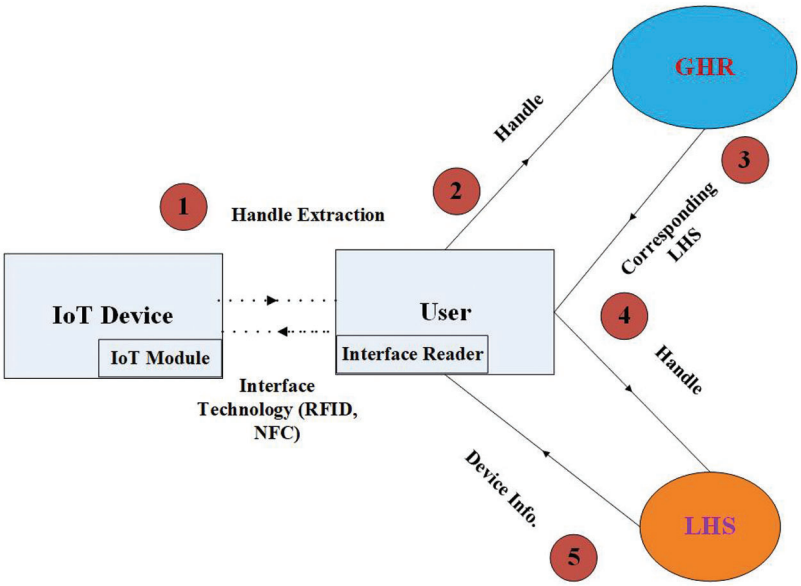


Figure 3: Resolution system based on IoT devices

The result of the resolution should be obtained in the form of a "type–value" pair to simplify the compatibility system. Each type is a globally unique identifier, which can be a globally resolved identifier in the description of its application, formats, encodings, etc. This is needed to facilitate their global reuse and processing of values.

The DOA authentication service described in this article may support the implementation of certain technologies, such as Public Key Infrastructure (PKI) [30]. This ensures data encryption and uptime of all servers used for resolution as part of the resolution service. DOA also supports third-party certificates.

In a DOA data structure, a digital object is a file, service, database, device, or combination. There is a possibility of creating a relationship between different digital objects or defining a digital object with complex operations. These two approaches provide a flexible and powerful mechanism for handling composite information [6].

5 Accessing IoT Devices Using DOA System

To ensure the availability of IoT devices, they must have a standard interface for reading and writing data, setting parameters, and diagnosing device-specific operations. These parameters necessarily vary from device to device. Fig. 8 shows an experiment using DOA architecture for identifying IoT devices. This is a stand built based on the model network of the Internet of Things laboratory at St. Petersburg State Telecommunications University [31]. In the experiment, the scenario of device identification using an intermediate verification device is considered. The modernized identification system consists of the following parts, as presented in Fig. 4.

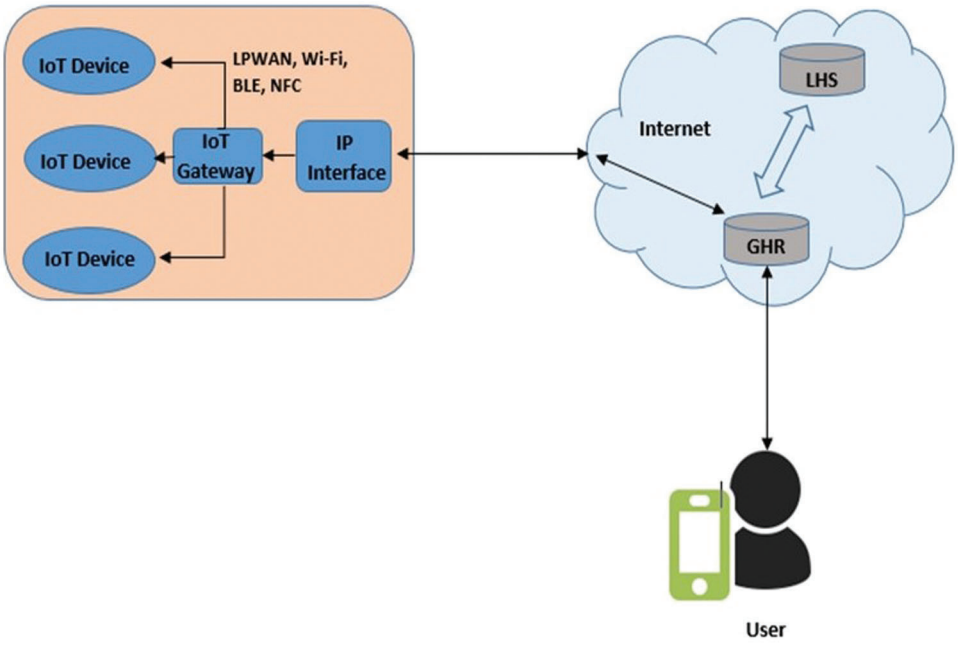


Figure 4: Experimental stand on the use of IoT devices to identify objects

1) Handle server containing information about the identified device;
2) Internet infrastructure;
3) End-device, i.e., identifiable object; and
4) Device for verification of objects in the DOA system.

Among the characteristics of the main components of the experimental system, it is worth noting the combination of GHR and LHS in one object. To conduct tests at the test bench, the study participants were given access to the DOA test zone with the prefix “11. test”, which allowed them to place their identifiers in the existing DOA system. In the future, this makes it possible to evaluate many characteristics of the developed system at the application level.

The verification device is a hardware-software complex with a set of network interfaces. It allows connecting many different devices both through direct physical interaction, using NFC technology, and through network interaction, e.g., Bluetooth and Wi-Fi.

The end-device can be either an IoT device or an ordinary object, the verification of which is necessary for some context. Thus, the device is tested through strictly defined DOA servers. The resulting system in a stationary version demonstrates the speed of the identification process and the route for the traffic to follow. This approach limits the possible scenarios of counterfeiting devices with a digital identifier while unloading the end device.

6 Performance Evaluation

In this part, the proposed modified handle system for DOA is simulated and tested over a reliable environment to check the performance and verify the latency performance enhancement compared to the existing handle system.

6.1 Simulation Setup

For simulation purposes, we consider the Matlab environment. A system with ten mid registers, N=10, is considered. The ten mid-registers are distributed over ten locations in different countries to cover and serve all LHR worldwide. Tab. 1 illustrates the specific locations of each mid register, with the longitude φ_j and latitude λ_j of each location. Moreover, the approximate communication distance between each mid-register and the GHR (D_j^{GHR}) is introduced. The total number of considered LHR registers connected to each mid-register (M_j) is presented in Tab. 2. The considered LHRs, connected to each MHR are selected with heterogenous location specifications. All other considered simulation parameters are introduced in Tab. 3.

Table 1: Location specifications of MHRs

j	Country	City	Coordinates		Approximate distances (D_j^{GHR})
			Longitude (φ_j)	Latitude (λ_j)	
1	Russian	Saint Petersburg	59.9343° N	30.3351° E	2,786.7 km
2	Egypt	Cairo	30.0444° N	31.2357° E	4,070.0 km
3	United Kingdom	London	51.5074° N	0.1278° W	992.5 km
4	Spain	Madrid	40.4168° N	3.7038° W	1,384.1 km
5	United states	Washington	47.7511° N	120.7401° W	8,365 km
6	China	Guangzhou	23.1291° N	113.2644° E	9,388 km
7	Italy	Rome	41.9028° N	12.4964° E	887.2 km
8	Brazil	Brazil	14.2350° S	51.9253° W	8,866 km
9	Canada	Ontario	51.2538° N	85.3232° W	6,279 km
10	Australia	Sydney	33.8688° S	151.2093° E	16,764 km

In order to illustrate the latency performance improvement of the modified handle system over the existing handle system, two simulation cases are considered. The first case considers the proposed modified handle system, while the other case considers the current handle system with only GHR and LHRs. The communication latency in each case is measured and compared to evaluate the performance enhancement.

Table 2: Number of LHRs connected to each MHR

M_j	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
Value	10	8	6	4	8	10	5	4	5	4

Table 3: Simulation parameters

Parameter	Abb.	Value
Propagation speed	ν	200 m/μs
Approximate GHR's location	Φ_{GHR}, λ_{GHR}	46.2044° N, 6.1432° E
N		10

6.2 Simulation Results

The communication latency between each LHR and the corresponding MHR was measured and recorded for case 1. The simulation process was repeated without MHRs, and the communication latency was measured between each LHR and GHR. Results for this scenario was recorded, and this represents case 2. Fig. 5a–5j illustrates the average latency, in each case, for each group of LHRs (M_j) connected to MHR_j.

As indicated in the results, the average latency of the modified handle system, i.e., Case 1, is less than the average latency of the existing handle system with no MHRs, i.e., Case 2. This latency performance improvement is achieved for all considered LHRs, distributed randomly all over the world.

The percentage of the latency improvement of each LHR using the modified handle system compared to the existing handle system is introduced in Tab. 4. Furthermore, the average latency improvement of each group of LHRs connected to certain MHR is introduced in Tab. 4. The total average latency improvement of all LHRs used in our proposed system is 61.56% compared to the LHRs using the existing handle system. Thus, the modified handle system can reduce the communication latency up to 60% compared to the current handle system with no MHRs.

One of the main advantages of the proposed modified handle system is the introduction of MHRs; however, if the load is unbalanced among these servers, the system will fail. Based on our previous introduced locations, the load distribution of the modified handle system was measured to define the status of the MHR registers and indicate how far the design is from failure. Fig. 6 presents the percentage of load distribution among MHR registers based on the considered topology. Fig. 6a introduces the percentage CPU load, while Fig. 6b indicates the percentage storage load of each considered MHR server. The figure shows that the load is distributed among mid-registers; however, this is not the optimum distribution. For optimum distribution, an optimization problem will be solved to get the optimum locations of the mid-registers. This is planned as our future work for this article.

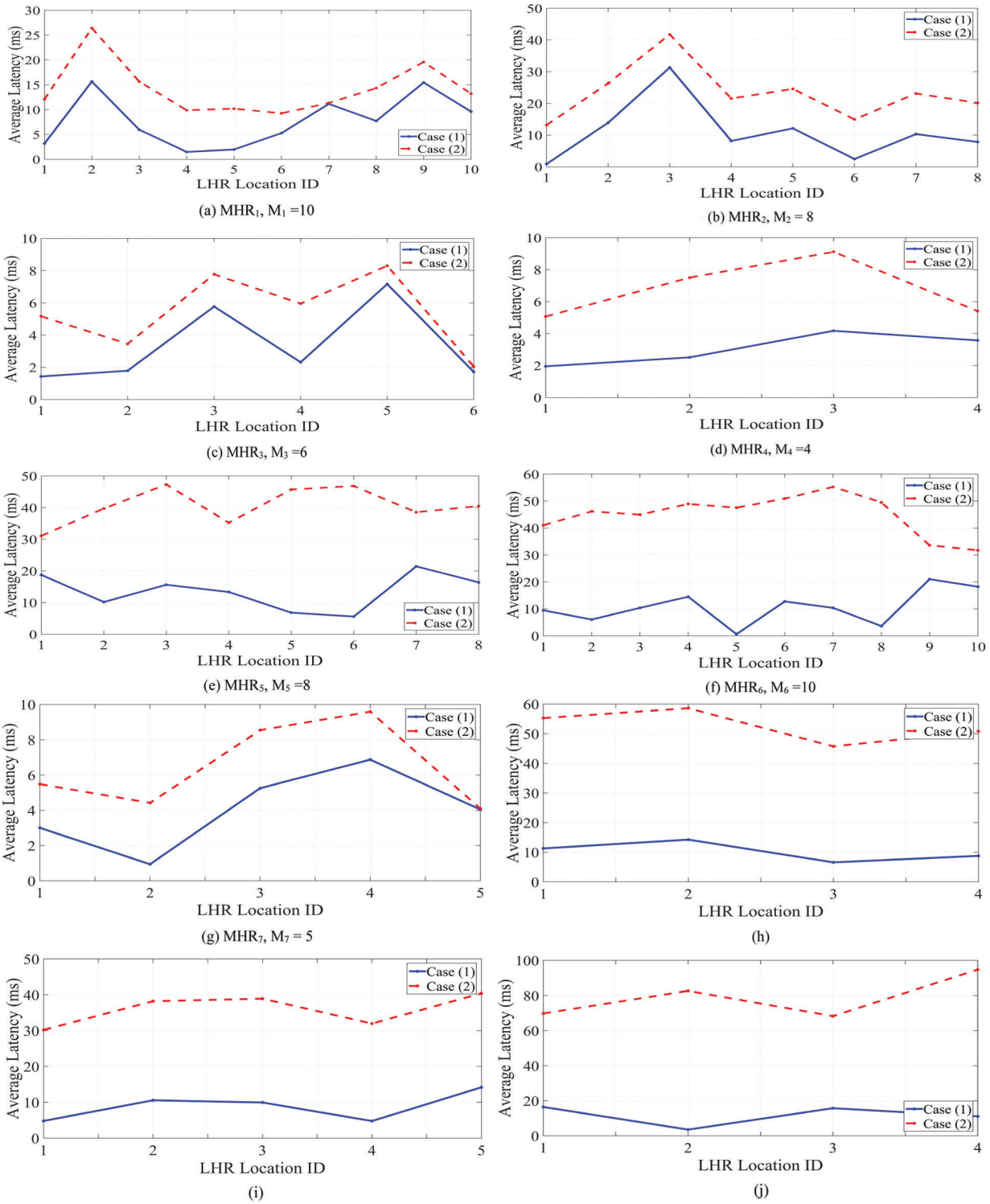
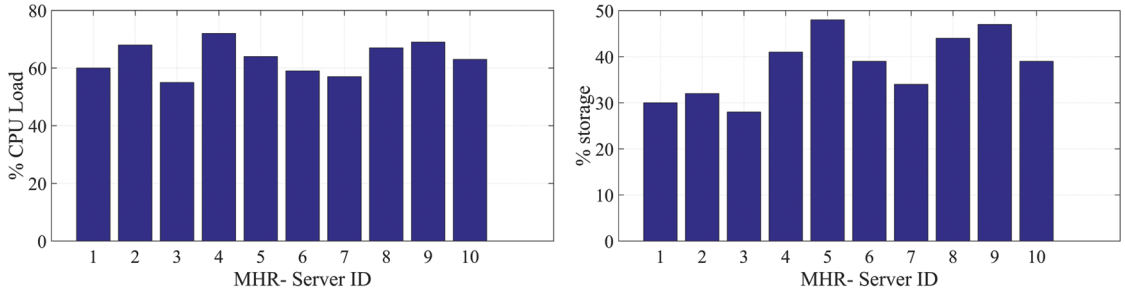


Figure 5: The average latency in each case for each group of LHRs (M_j) connected to MHR_j

Table 4: Average latency performance improvement for LHRs over the modified handle system

MHR_j	Percentage latency performance improvement of LHR_i										Average latency improvement
	LHR_1	LHR_2	LHR_3	LHR_4	LHR_5	LHR_6	LHR_7	LHR_8	LHR_9	LHR_{10}	
MHR_1	73.82	40.70	61.86	84.82	80.55	43.09	1.59	46.16	26.19	27.19	48.60%
MHR_2	93.17	47.18	24.97	62.11	50.68	83.48	55.38	61.04	-	-	59.75%
MHR_3	27.24	48.23	25.74	61.11	13.67	16.15	-	-	-	-	32.02%
MHR_4	61.52	66.53	54.21	33.94	-	-	-	-	-	-	54.05%
MHR_5	39.75	74.39	66.94	62.12	85.03	88.06	44.33	59.54	-	-	67.54%
MHR_6	76.98	86.87	76.96	70.36	98.75	74.97	81.23	92.70	37.43	42.62	73.89%
MHR_7	45.25	78.69	38.50	28.35	1.29	-	-	-	-	-	38.42%
MHR_8	79.57	75.66	85.57	82.75	-	-	-	-	-	-	80.89%
MHR_9	84.09	72.33	74.40	85.06	64.88	-	-	-	-	-	76.15%
MHR_{10}	76.41	95.68	76.93	88.25	-	-	-	-	-	-	84.32%
Average latency performance improvement of all MHRs											61.56%



(a) (b)

Figure 6: (a) Percentage CPU load of each MHR server; (b) The average latency in each case for each group of LHRs (M_j) connected to MHR_j

7 Conclusions

Digital Object Architecture can be used as the primary architecture for identifying IoT devices since it solves many compatibility issues in this area. Entities in each IoT application, including smart devices, application services, and application users registered in IoT applications, can be considered digital objects. Each digital object can have its unique global identifier, which can also be associated with a set of attributes that describe the underlying entity. Smart devices used in the IoT networks can obtain their global identifier with features that identify the owner using the developed modified handle system. It is also possible to define different access methods and service interfaces to communicate with the IoT device.

This global identifier allows accessing device specifications and checking the device's authenticity. Ownership and access control rights defined by the digital object can provide secure access to the device in many IoT applications without losing the necessary security systems. The article provided a novel DOA-based structure for identifying IoT devices and increasing network security. The proposed model breaks the common structure of the DOA system by introducing a Middle Handle Register (MHR)

between the global register, i.e., Global Handle Register (GHR), and the local register, i.e., the Local Handle Register (LHR). The system achieved higher latency and security efficiency.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. F. Sittig, A. Wright, E. Coiera, F. Magrabi, R. Ratwani *et al.,* "Current challenges in health information technology–related patient safety," *Health Informatics Journal*, vol. 26, no. 1, pp. 181–189, 2020.

[2] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali *et al.,* "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[3] M. Al-Bahri, A. Yankovsky, A. Borodin and R. Kirichek, "Testbed for identify IoT-devices based on digital object architecture," in *Proc. Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Cham, Springer, pp. 129–137, 2018.

[4] M. Albahri, R. Kirichek, A. A. Ateya, A. Muthanna and A. Borodin, "Combating counterfeit for IoT system based on DOA," in *Proc. 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, IEEE, Moscow, Russia, pp. 1–5, 2018.

[5] M. Al-Bahri and W. ALKISHRI, "Doa-A New approach to identify IoT devices," *Applied Computing Journal*, pp. 66–76, 2021.

[6] R. Kahn and R. Wilensky, "A framework for distributed digital object services," *International Journal on Digital Libraries*, vol. 6, no. 2, pp. 115–123, 2006.

[7] N. Paskin, "Digital object identifier (DOI) system," *Encyclopedia of Library and Information Sciences*, 2010.

[8] M. Al-Bahri, S. Al-Wardi, R. R. Dharamshi, N. Al-shukail and A. Muthanna, "A smart system based on digital object architecture to verify the diploma certificates," in *Proc. 2020 Int. Conf. on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, Sharjah, United Arab Emirates, IEEE, pp. 1–5, 2020.

[9] R. Kirichek and A. Koucheryavy, "Internet of things laboratory test bed," in *Proc. Wireless Communications, Networking and Applications*, New Delhi, Springer, pp. 485–494, 2016.

[10] M. Al-Bahri, A. Yankovsky, R. Kirichek and A. Borodin, "Smart system based on DOA & IoT for products monitoring & anti-counterfeiting," in *Proc. 2019 4th MEC Int. Conf. on Big Data and Smart City (ICBDSC)*, IEEE, Muscat, Oman, pp. 1–5, 2019.

[11] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal and L. F. Cranor, "Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?," in *Proc. 2021 IEEE Symp. on Security and Privacy (SP)*, San Francisco, CA, USA, pp. 1937–1954, 2021.

[12] P. P. Ray, "A survey on internet of things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291–319, 2018.

[13] ITU-T Study Group 20, last access on 20-05-2021. [Online]. Available: https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx.

[14] H. Li, Y. Kong and X. Wang, "Design and implementation of a distributed data acquisition function architecture based on DOA/Handle technology," in *Proc. MATEC Web of Conferences*, EDP Sciences, vol. 336, pp. 05018, 2021.

[15] J. Dizdarević, F. Carpio, A. Jukan and X. Masip-Bruin, "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–29, 2019.

[16] Gartner Consulting, last access on 10-11-2021. [Online]. Available: https://www.gartner.com/en/consulting.

[17] Y. J. Tu and S. Piramuthu, "On addressing RFID/NFC-based relay attacks: An overview," *Decision Support Systems*, vol. 129, pp. 113194, 2020.

[18] S. N. Matheu, A. R. Enciso, A. M. Zarca, D. Garcia-Carrillo, J. L. Hernández-Ramos *et al.,* "Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems," *Sensors*, vol. 20, no. 7, pp. 1882, 2020.

[19] N. A. Anagnostopoulos, T. Arul, Y. Fan, C. Hatzfeld, J. Lotichius *et al..,* "Securing IoT devices using robust DRAM PUFs," in *Proc. 2018 Global Information Infrastructure and Networking Symp. (GIIS)*, IEEE, Thessaloniki, Greece, pp. 1–5, 2018.

[20] R. N. Akram, K. Markantonakis and K. Mayes, "Trusted platform module for smart cards," in *Proc. 2014 6th Int. Conf, on New Technologies, Mobility and Security (NTMS)*, Dubai, United Arab Emirates, IEEE, pp. 1–5, 2014.

[21] A. S. Siddiqui, Y. Gui and F. Saqib, "Secure boot for reconfigurable architectures," *Cryptography*, vol. 4, no. 4, pp. 26, 2020.

[22] N. A. Anagnostopoulos, Y. Fan, T. Arul, R. Sarangdhar and S. Katzenbeisser, "Lightweight security solutions for IoT implementations in space," in *Proc. 2019 IEEE Topical Workshop on Internet of Space (TWIOS)*, IEEE, Orlando, FL, USA, pp. 1–4, 2019.

[23] Body of European Regulators for Electronic Communications, last access on 05-10-2021. [Online]. Available: https://berec.europa.eu/.

[24] M. A. Albreem, A. A. El-Saleh, M. Isa, W. Salah, M. Jusoh *et al..,* "Green internet of things (IoT): An overview," in *Proc.2017 IEEE 4th Int. Conf. on Smart Instrumentation, Measurement and Application (ICSIMA)*, IEEE, Putrajaya, Malaysia, pp. 1–6, 2017.

[25] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. Jeong *et al.,* "Analysis of identifiers in IoT platforms," *Digital Communications and Networks*, vol. 6, no. 3, pp. 333–340, 2020.

[26] A. Skarmeta, J. L. Hernández-Ramos and J. B. Bernabe, "A required security and privacy framework for smart objects," in *Proc. 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*, IEEE, Barcelona, Spain, pp. 1–7, 2015.

[27] M. Mulhall, "*Multi-functional Handle System*," U.S. Patent No. 10,533,700, Washington, DC: U.S. Patent and Trademark Office, 2020.

[28] Y. Wang and Q. Wen, "A privacy enhanced dns scheme for the internet of things," in *Proc. IET Int. Conf. on Communication Technology and Application*, pp. 699–702, 2011.

[29] Global Handle Registry, last access on 05-10-2021. [Online]. Available: https://www.dona.net/prefix/resolve.

[30] A. A. Ateya, A. Muthanna, M. Makolkina and A. Koucheryavy, "Study of 5G services standardization: specifications and requirements," in *Proc. 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, Moscow, Russia, IEEE, pp. 1–6, 2018.

[31] Internet of Things laboratory at St. Petersburg State Telecommunications University, last access on 05-11-2021. [Online]. Available: http://iotlab.ru.