QUBAHAN ACADEMIC JOURNAL
2024, VOL. 4, NO. 1, March 2024
https://doi.org/10.48161/qaj.v4n1a413

Enhancing IoT Network Security Through Digital Object Architecture-Based Approaches

Mahmood Al-Bahri [1*], Wasin Alkishri [2], and Falah Y H Ahmed [1], Marwan Alshar'e [1], Sanad Al-Maskari [1]

[1] Faculty of Computing and Information Technology, Sohar University, Sohar 311, Oman.
[2] Faculty of Computer Studies, Arab Open University, Muscat 130, Oman.

Corresponding author: mbahri@su.edu.om

ABSTRACT: The Internet of Things (IoT) encompasses a network of different devices, both stationary and mobile, that may interact with the physical world. Ensuring the security of the Internet of Things (IoT) is of utmost importance in a world where devices are interconnected at various levels, including wearables, home automation, smart cities, industrial sectors, and more. Ensuring the security of this interconnected network of "things" and devices is imperative, leaving no space for mistakes or inadequacies. The purpose of this article is to present an approach that utilizes Digital Object Architecture (DOA) to identify Internet of Things (IoT) devices and applications within communication networks. This study investigates various methodologies for incorporating the DOA identifier into Internet of Things (IoT) devices that are equipped with a range of wireless data transmission modules. Furthermore, this study presents a security model that aims to strengthen the resolution system based on data transmission security. The objective is to reduce the number of service messages exchanged between internetwork parts and decrease network latency. The essay finishes by examining some strategies for modernizing DOA in order to improve the quality of service.

Keywords: Internet of Things, Identification, Security, DOA, Handel System.

I. INTRODUCTION

The Internet of Things (IoT) is a contemporary concept that involves the representation of various devices, instruments, and even objects united within a single global network, utilizing a network infrastructure that enables these entities to interact with each other and with people through public communication networks [1-22]. Currently, the proliferation of IoT devices is escalating rapidly. These devices find applications in diverse fields of human activity, including education, medicine, agriculture, and other industries, effectively addressing the crucial challenge of automating their interaction with both each other and humans [2]. However, with the pursuit of automation, new challenges emerge, such as addressing the substantial number of devices and ensuring the secure exchange of data among them.

The notion of the Internet of Things (IoT) stands as a progressive foundation within the realm of digital intelligence, particularly within the framework of the "Smart Country" concept [3]. The global count of IoT-connected devices is experiencing exponential growth. Figure 1 illustrates the current and projected number of IoT devices in billions from 2015 to 2030, along with their market impact [4]. While this surge presents extensive possibilities, it also raises concerns regarding safeguarding individual privacy in the context of IoT. Identity's significance within IoT is pivotal.

The interconnected nature of IoT systems and the several disciplines required for their implementation have created fresh security obstacles. The implementation of security techniques such as identity, encryption, authentication, access control, network, and application security for Internet of Things (IoT)

devices and their vulnerabilities is deemed ineffective. Thus, current security measures need to be improved to adequately protect the IoT environment.

When referring to a device identifier, we are indicating a specific, publicly available attribute or set of attributes and names. Typically, these identifiers operate within a defined area or network and may not always be universally applicable for identifying entities worldwide. In the context of modern IoT devices, it is common for them to possess multiple identities within existing networks [5].

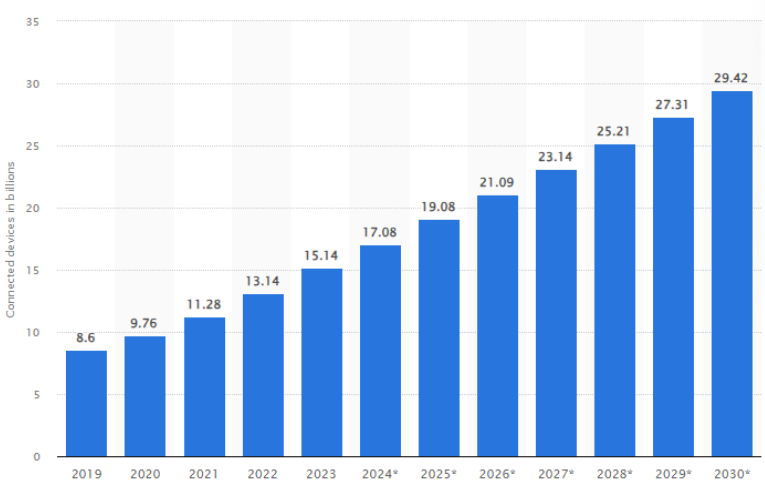

FIGURE 1. Number of IoT-connected devices between 2019 and 2030 in billions [4].

It's important to emphasize that the unique identifier doesn't replace device addressing; rather, it complements it. Device addresses are crucial at the network and data link layers, facilitating data transfer and packet routing. In contrast, the identifier primarily functions at the session layer. Nevertheless, network and channel addresses can also function as device identifiers depending on the specific task and security requirements [6].

Currently, a plethora of diverse software and hardware solutions are available for acquiring a unique global identifier. Broadly, these solutions can be categorized into two groups:

- User, Manufacturer, or Regulator Assigned Identifiers: This group includes identifiers that are assigned by the user, manufacturer, or regulatory body.
- Inherently Unique Identifiers: This group comprises unique identifiers derived from distinctive characteristics or properties inherent to the device.

Today, various methods exist for constructing a system aimed at recognizing Internet of Things (IoT) devices [7, 8, 9]. One potential approach to address this difficulty entails adopting an identifying framework based on the Digital Object Architecture foundation. In our study, we have introduced a technique in [15] that utilizes the Digital Objects Architecture (DOA) to identify Internet of Things (IoT) devices and applications in diverse networks. The model presented in reference [11] ensures a satisfactory level of quality of service (QoS) within the existing framework of public communication networks. A unique interaction architecture has been proposed, which incorporates a Middle Handle Register (MHR) situated between the Global Handle Register (GHR) and the Local Handle Register (LHR). The proposed architectural design enhances network interaction and guarantees interoperability IoT end-devices and the system. The authors of [12] presented a novel anti-counterfeiting smart system that utilizes Digital Object Architecture (DOA) and the Internet of Things (IoT) for the purpose of product identification. The primary objective of this system is to protect products from counterfeiting through the utilization of sophisticated digital identifying techniques.

In In this paper, we have put forward a security model designed to enhance resolution systems, with the objective of strengthening data transmission security. By doing so, we aim to reduce the quantity of service messages exchanged between internetwork elements and mitigate network latency.

The paper structure: have the Literature Review in Section II, Background Theory In Section III, Proposed Method in Section IV, the conclusion in section V.

II. LITERATURE REVIEW

The Several researchers have provided recommendations and techniques for identifying IoT applications and devices. Most of the literature on this topic will be thoroughly reviewed in this section.

In [16], the authors address the fundamental challenge of device identification on the Internet of Things. The accurate identification of devices is crucial for various essential services such as access control and intrusion prevention within a network. Traditional methods, like using the device's MAC address, face challenges due to vulnerabilities, such as MAC address spoofing. Additionally, considering dynamic characteristics like traffic patterns in IoT devices offers an alternative avenue for device identification. The authors propose a solution leveraging machine learning, specifically an unsupervised machine-learning approach, to tackle IoT device identification. Unsupervised machine learning provides a promising alternative to supervised techniques by delivering reliable results without requiring a large amount of labelled data. This research aims to propose and analyse the efficacy of an unsupervised machine-learning methodology in the context of identifying Internet of Things (IoT) devices.

The authors in reference [17] introduce a machine learning approach known as IoTDevID (Internet of Things Device Identification) to enhance the security of a network comprising a multitude of IoT devices. The objective of this strategy is to identify devices by examining the attributes of their network packets. The paper presents a comprehensive analysis and selection process of features to create a model for device behavior that is both generalizable and realistic. The model demonstrates a high level of predicted accuracy when applied to two publicly available datasets. The predictive power of the underlying feature set of the model surpasses that of commonly used feature sets for device identification. Furthermore, the model demonstrates its capacity to extrapolate to data that has not been encountered before throughout the process of selecting features. IoTDevID stands out from other methods of identifying IoT devices by its ability to detect devices that utilize non-IP and low-energy protocols. This enhances its suitability and efficiency in many IoT scenarios.

In [18], the study acknowledges the security challenges posed by IoT devices and emphasizes the need for automated management to mitigate these issues. Specifically, the focus is on robustly identifying IoT devices to facilitate the application of appropriate network security policies. The researchers delve into the accurate identification of IoT devices based on their network behavior, building on approaches previously proposed by other researchers. To assess identification accuracy, the study compares four different machine learning models—both tree-based and neural network-based—utilizing packet trace data collected over a six-month period from a sizable IoT testbed. The findings reveal that while all models demonstrate high accuracy when evaluated on the same dataset they were trained on, their accuracy diminishes over time when assessed on data collected outside the training set. Typically, the accuracy of the models exhibits a reduction over a span of several weeks, resulting in a decrease of up to 40 percentage points. This loss is seen to have an average range of 12 to 21 percentage points. The research emphasizes the importance of regular updates in order to uphold the precision of these models at a superior level. The aforementioned acknowledgment highlights the fluidity of behavior in IoT devices, underscoring the significance of continuous endeavors in enhancing and adjusting machine learning models to achieve efficient and robust identification of IoT devices.

Internet of Things devices have a significant influence on shaping human experiences in the age of widespread computing. Although these devices provide a wide range of services, they are not exempt from limits, particularly in relation to resource constraints that could impede their capacity to complete assigned duties. In order to tackle this issue, the implementation of a delegation mechanism becomes imperative, as it facilitates the effective management of task requests by devices that possess constrained resources. Concurrently, the inherent sensitivity of the data held by these devices underscores the need for a trust mechanism that can effectively identify trustworthy devices for the purpose of delegating functions that include sensitive information.

The research [19] presents a paradigm that utilizes ontologies to tackle the difficulties associated with incomplete task requests from resource-constrained IoT devices, with the aim of identifying trusted IoT devices for delegation. The ontology being suggested aims to provide a strong and reliable link between models and real-world situations, thereby offering a thorough comprehension of domain knowledge in widespread and omnipresent systems, such as Internet of Things (IoT) devices. Furthermore, the study introduces a semantic matching method that has been specifically developed to priorities devices that are highly favorable and trustworthy, taking into account resource and trust factors.

The implementation of the ontology is carried out using the Protégé editor, and its evaluation is conducted using a web query language. The suggested system exhibits improved performance in comparison to existing techniques, as evidenced by the experimental results obtained through simulation and parametric evaluations. The present study makes a significant contribution towards improving the effectiveness and reliability of IoT device delegation. It provides a beneficial solution for addressing limitations in resources and assuring the secure management of sensitive data.

In their study, the researchers in [20] tackle the persistent issue of device identification in the Internet of Things (IoT) by suggesting a method that entails extracting characteristics from devices and merging them to generate a time-based pattern, which functions as a distinct identifier. This technique serves the dual purpose of device identification and authentication. The paper's simulation findings showcase the efficacy and importance of the patterns employed for device identification.

The above-mentioned prominent technique for device identification does not exist. Identification of the various equipment, users, and devices in an IoT network is therefore crucial, and it will likely remain a key area of study for IoT researchers in the future.

III. BACKGROUND THEORY

1. DIGITAL OBJECT ARCHITECTURE

The Early in the 1990s, the Corporation for National Research Initiatives (CNRI) built the Digital Object Architecture and related Handle System resolution system on top of digital libraries for the Defense Advanced Research Projects Agency (DARPA) [10]. The necessity to recognize items and gather data about them over a long period of time was one of the initial driving forces behind the creation of DOA. With the creation of DOA, an effort was made to switch from utilizing IP addresses and URL sets to represent data on the Internet to finding and distributing information in the form of digital objects.

The development of DOA aimed to change the way people perceived the internet: instead of seeing it as centered on a list of hosts and the means of accessing them, people saw it as centered around the discovery and distribution of digital objects, or information.

DOA is an architecture for distributed storage, location, and information retrieval on the Internet. Figure 2 illustrates DOA- Information Management on Networks.

The main components of DOA include [11]:

• A digital object is an organized record that includes metadata, data, and information about the data's current state. There's a chance the digital object has links to locations with pertinent information. No matter

what the underlying technological systems are, every digital object can be accessed using a specific digital object protocol. Every digital item has a description that explains what's within. Every digital asset has access control guidelines specific to it.

- Digital objects can be stored and accessed using the Digital Object Repository (DO Repository). The system can have an infinite number of repositories.
- Handles: a collection of persistent, unique identifiers for digital objects that are not dependent on the underlying logical or physical system.
- Handle System: a system for specifying location data resolutions. Registries specify groups of items that are stored in repositories.
- Digital object collections are defined by the DO Registry, which also registers objects that might be kept in one or more public repositories. By using its identification, the registry can also access details about an object that has already been registered, such as its location, attributes, writers, rights holders, etc.

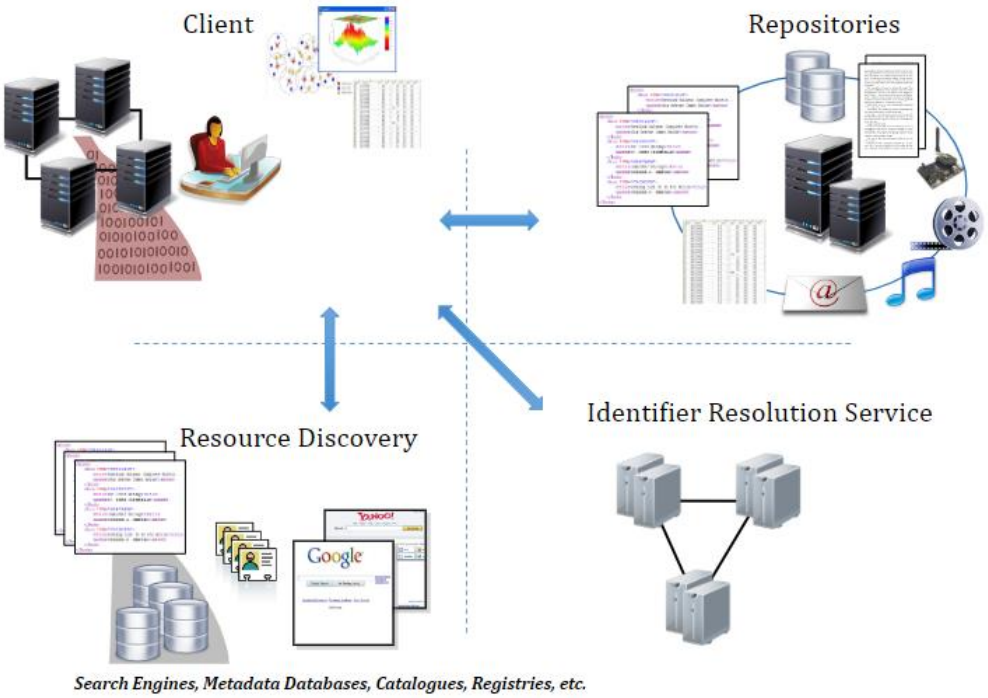

FIGURE 2. Basic components of DOA

Although DOA was originally designed to allow for a variety of identification systems, over time, it has moved almost entirely to using a handler system.

2. *HANDLE SYSTEM*

The Handle System resolution was developed to address the limitations in the functionality of existing object identification systems on the Internet [12].

Resolution is a procedural mechanism in which an identification functions as a solicitation to a network service in order to get up-to-date information (state data) pertaining to the specified entity, typically a geographical location. The Handle System is capable of accommodating numerous resolutions, so enabling the response to a request to encompass the whereabouts of diverse object instances, associated services, and any additional information explicitly stated in the object's metadata. The provided data extends

beyond merely indicating the existence of the object. It may encompass a comprehensive depiction or condition of the object, indicators, measurements, associations with other entities, and further details.

A Handle is a globally unique and resolvable identifier in the format "prefix/suffix," where the prefix is unique within the Handle System. Here's an illustration of a handle: 11.1000/100. The prefix 11.1000 is given to the naming authority, and the local name within that namespace is 100 in the first example, which is the handle for the HANDLE.NET software license.

The general design of the Handle System resolution system is depicted in Figure 3.

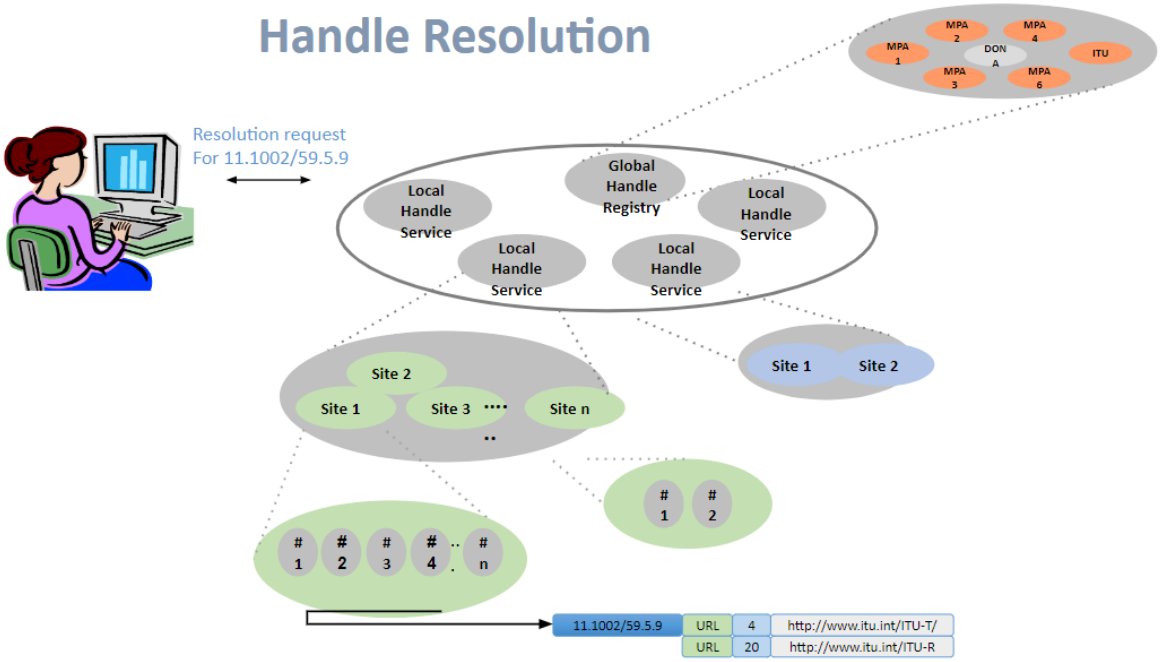

FIGURE 3. General architecture for the Handle System resolution system

The client sends GHR a handling request. In response, GHR gives service information identifying the LHR system in charge of preserving the identifier prefix. After that, the client contacts the designated LHR with a request. The digital object is then retrieved after the LHR recognizes the server. The response provides the client with the desired information. The client then processes the data that was received [13].

The root of the system descriptor hierarchy is under the control of GHR. It does this by assigning distinct prefixes and providing the LHR with a worldwide prefix binding service.

The DOA governance model is now being reorganized, moving away from the single main administrator (previously CNRI) and towards the MPA (Multi-Primary Administrator) model, which consists of multiple top-level administrators. The non-profit organization The DONA Foundation, which was founded in 2014 in Geneva, Switzerland, authorizes and oversees the actions of these MPAs, which operate as multi-purpose primary administrators of a network of digital IDs [14].

The ITU-T Study Group SG20 is working to standardize techniques for recognizing and thwarting counterfeiting that are based on the digital object's architecture. "Architecture for the interaction of Internet of Things devices based on the architecture of digital objects" was the recommendation that was submitted by December 2018 for the consent procedure. The recommendation "Structure of solutions to combat counterfeit Internet of Things devices based on the architecture of digital objects" is intended to be adopted in 2019. [15]

A collaborative technical solution that makes use of the Internet of Things–DOA identifier link emerges as a strong technological chain in light of these advancements. In order to do this, a DOA identifier that encompasses the distinctive characteristics of a particular item (metadata) must be included into a module

that communicates with the network infrastructure. An array of industries, including ICT, pharmaceuticals, automotive, and aircraft production, can benefit from the use of this solution. Especially, it could be used to fight counterfeiting in these industries.

3. RESEARCH FOCUS

The DOA framework serves as a systematic approach to the management of digital resources, offering a standardized methodology for the identification and retrieval of digital objects. It can be employed in IoT systems to oversee and verify different IoT devices and their corresponding data.

The Handle System, conversely, is a technological solution utilized for the allocation of distinct identifiers to digital assets. Handles, which are identifiers, offer a uniform and universally distinct method of referencing digital items. inside the realm of the Internet of Things, the utilization of the Handle System can be implemented to allocate distinct IDs to IoT devices, hence guaranteeing their secure connection inside the network.

Hence, the primary objective of this study is to investigate the potential integration of DOA and the Handle System in order to improve security, data management, and interoperability within IoT environments. This encompasses the creation of frameworks that enable the secure identification and management of Internet of Things devices, guarantee the integrity of data, and provide smooth communication among various IoT platforms and applications.

IV. MATHEMATICAL MODEL

This section explains the potential of DOA in addressing the obstacles associated with enhancing trust and security in the communication process between digital object architectures and IoT devices. Our objective is to safeguard the confidentiality of intelligent devices inside the application domain. As previously stated, a crucial component of DOA is the resolution mechanism, also known as the Handle mechanism. Examine the security model of the resolution system in this section.

1. KEY NOTATIONS:

1) $\Psi_{S,D}$ – a shared security key transmitted between the source node S and the destination node D.

2) Γ_S – the public encryption key of the source node S.

3) Φ_S – the private encryption key of the source node S.

4) $M_S^{\Gamma}=\{b_1, b_1, b_1, \ldots, b_n\}$ – A message encrypted by the source node S using its public key Γ_S.

5) $M_S^{\varphi}=\{b_1, b_1, b_1, \ldots, b_m\}$ – A message encrypted by the source node S using its private key Φ_S.

6) $[M_S^{\varphi}]^{-1}=\{b_1, b_1, b_1, \ldots, b_m\}^{-1}$ – Message decrypted by source node S using its private key Φ_S.

7) $<M_1, M_2, \ldots, M_n>$ – set of given messages $M_1, M_2, M_3, \ldots, M_n$.

8) $S \rightarrow D$: M – source server S sends message M to destination server D.

9) Rand (i) – random number generation with speed i;

10) R_{GHR} – random number generation rate generated by the GHR server and used to encrypt and decrypt messages.

11) R_{LHR} – the speed of generating random numbers generated by the Local Handle Register (LHR) server and used to encrypt and decrypt messages.

12) ID_{LHR} – LHR identification number.

13) L_{GHR}- Buffer used by GHR.

14) L_{LHR}- Buffer used by LHR.

15)Q_n – request number.

16) γ – LHR encryption key.

17) Π_{GHR} – GHR public key.

18) Mess-Size(*M*) – a method for calculating message digests and digital signatures (a message digest is a numeric representation of a fixed size message content, calculated by a hash function).

2. PROPOSED SECURITY ENHANCEMENT SCHEME FOR THE RESOLUTION SYSTEM

The LHR and GHR servers have their own predefined keys Ψ_{LHR}, $_{GHR}$, used in messaging and authentication processes. Each server (LHR and GHR) generates a random number with a predefined frequency of RLHR and RGHR respectively. The generated numbers are used for encryption and decryption.

$$LGHR=Rand\ (RGHR) \tag{1}$$
$$LLHR=Rand\ (RLHR) \tag{2}$$

The LHR server performs a sequence of actions that combines the LHR server identification number with a randomly generated number at a predetermined frequency and a given request number.

$$M_1^{\gamma_1} = \{\mathrm{ID}_{\mathrm{LHR}}, L_{\mathrm{LHR}}, Q_n\} \tag{3}$$

Message M1 is encrypted using the public key γ1. The LHR server then determined the required set of message data to be exchanged with the centralized GHR registry.

$$LHR \rightarrow GHR : < M_1^{\gamma_1}, M_2^{\gamma_1}, M_3^{\gamma_1}, \ldots., M_n^{\gamma_1} > \tag{4}$$

The GHR receives the data set and decrypts the M_1 message using the pre-shared key. The decrypted message looks like this:

$$[M_1^{\gamma_1}]^{-1} = \langle \mathrm{ID}_{\mathrm{LHR}}, L_{\mathrm{LHR}}, Q_n \rangle \tag{5}$$

The GHR server then retrieves the LHR ID to check server access permissions as Follow:

$$\mathrm{ID}_{\text{host, app-serv}} = \mathrm{ID}_{\text{host}} \oplus L_{\mathrm{GHR}} \tag{6}$$
$$\mathrm{ID}_{\text{IP, app-serv}} = Q_n \,||\, (\mathrm{ID}_{\text{host, app-serv}} \oplus L_{\mathrm{LHR}}) \tag{7}$$

Next, the GHR server calculates the hash sum and the digital signature. The hash sum, which is calculated using the hash function, is a numeric representation of the content of the message. Its length is predetermined.

$$\Pi_{GHR} = \left[\left(Mess - Size\left(ID_{IP,\ app\text{-}serv} \right)^{\Gamma_{GHR}} \right) \right]^{-1} \tag{8}$$

$$Mess - Size\left(ID_{IP,\ app\text{-}serv} \right) = \Pi_{GHR} \tag{9}$$

The GHR server returns Π_{GHR} and $ID_{IP,\ app\text{-}serv}$, app-serv to the LHR server, which is a confirmation of the signatures.

$$ID_{IP,\ act} = Q_n \,||\, \left(ID_{host,\ app\text{-}serv} \oplus L_{LHR} \oplus L_{LHR} \right) = Q_n \,||\, ID_{host,\ app\text{-}serv} \tag{10}$$

In the proposed security model for the Handle system, the various notations play crucial roles in facilitating secure communication between the LHR and GHR servers:

$\Psi_{S,D}$, Γ_S, Φ_S: These keys are utilized for encryption, decryption, and authentication between the source node (LHR or GHR server) and destination node (GHR or LHR server), ensuring confidentiality and integrity of exchanged messages.

MSΓ, $M_S\varphi$, $[M_S\varphi]$-1: These notations represent messages encrypted with public or private keys, and their corresponding decryption. In the Handle system, messages are encrypted and decrypted to ensure secure transmission and reception between the servers.

R_{GHR}, R_{LHR}, γ, Π_{GHR}: These elements are related to random number generation, encryption keys, and public keys used in the encryption and decryption processes between the LHR and GHR servers. They ensure secure encryption and decryption of messages exchanged between the servers.

ID_{LHR}, L_{GHR}, L_{LHR}, Q_n: These symbols relate to server identification, buffers, and request numbers used in the communication process. They aid in the organization and management of messages exchanged between the LHR and GHR servers.

Mess-Size(M): This notation represents methods for calculating message digests and digital signatures, ensuring message integrity and authenticity. In the Handle system, digital signatures are used in messages exchanged between the servers to authenticate the sender and ensure the message's integrity.

V. SIMULATION MODEL

To assess the efficacy of the identifier resolution system within the DOA architecture for the purpose of identifying the Internet of Things, it is advantageous to conceptualize the resolution system as a queuing system (QS). The decision was made to adopt the M/M/s model as the quality control (QS) system. This model describes a system that follows an exponential relationship between the time it takes to serve requests and the time it takes for requests to arrive. Furthermore, the model meets the following crucial criteria:

- The model under consideration involves the existence of several processing channels, wherein GHR servers are regarded as autonomous entities solely responsible for processing incoming requests.
- The duration of the GHR buffer is not limited, as each request that is received by the system will be processed.
- Incoming requests do not have a priority. The processing of each request follows the sequential order in which it was received by the system.

It is important to acknowledge that while examining the processing of request traffic over an extended duration, such as several days, the chosen model will become obsolete. Nevertheless, this concept is applicable for brief durations. A time interval of 200 seconds was selected as the duration for system operation.

The resolution system model was developed through an analysis of the current implementation of the resolution system. The existing architecture employs multiple servers owned by MPA (Multi-Primary Administrators), which are under the jurisdiction of the DONA Foundation, rather than relying on a single GHR server. Every MPA server functions as a GHR, specifically designed to handle incoming requests by analysing the software offered by Handling.net. The infrastructure of top-level global registry servers was developed. The average delay for resolving a request by these servers was determined by the system. All MPA servers in this programme are considered equivalent, and a request for permission is made in a sequential manner to all servers. Subsequently, the initial response is examined. Simultaneously, there is a lack of accounting and analysis of the server's delay time. The resolution system ensures that upon the entry of a permission request into the system, it will be duly executed. Nevertheless, it is important to establish regulations about the duration of this process. The features of the MPA servers utilised as GHRs in the existing resolution system architecture are presented in Table 1.

Multi-Primary Administrators	**IP address**	**Mean resolution delay, ms**
CNRI (USA)	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 Newslet-ter Cas Telecommunication (China)	119.90.34.34	473.583
Alicloud (China)	47.90.103.77	410.693
ATI – Agence Tunisien-ne Internet (Tunisia)	41.231.118.2	82.510
Gesellschaft Für Wissenschaftliche Datenverarbeitung Mbh Göttingen (Germany)	134.76.30.197	44.356
Communications And Information Techno-logy Commission (Saudi Arabia)	86.111.195.107	318.450
Liquid Telecommunications Operations Limited (Kenya)	196.12.152.22	258.450

Figure 4 depicts a rudimentary flowchart illustrating the override handling procedure of the queuing sy stem, specifically focusing on the ID resolution phase.
A simulation of a queuing system was constructed using AnyLogic.

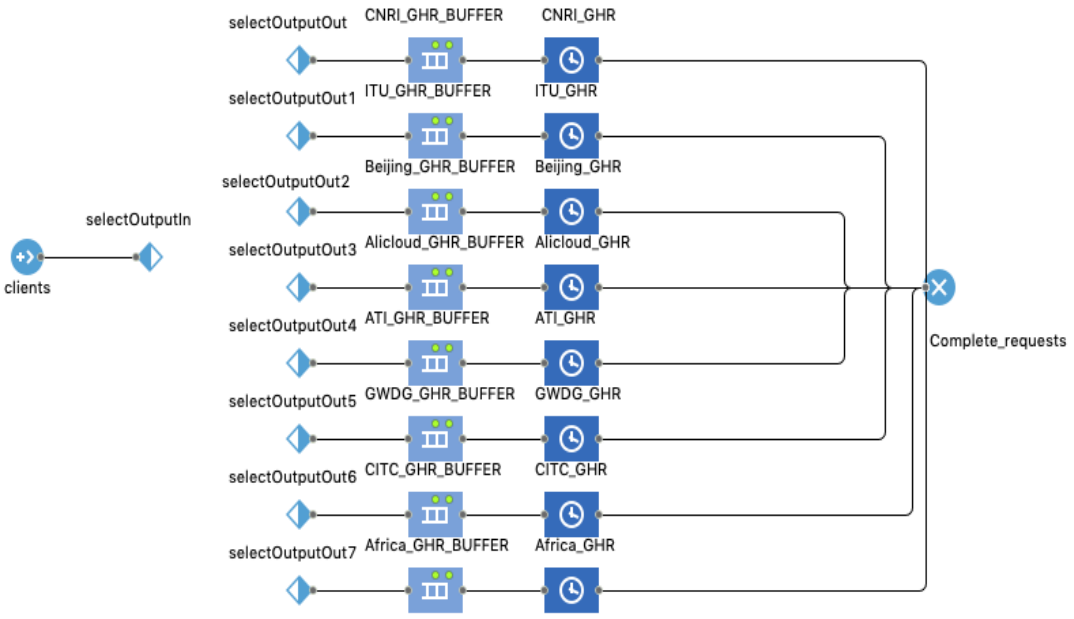

FIGURE 4. DOI resolution system is simulated using QS.

The client element is associated with the origin of identity resolution requests originating from devices. Following this, there is a division into 8 channels, with each channel representing the infrastructure of a certain Multi-Primary Administrators (MPA). The likelihood of selecting each channel within the current system is equal. A collection of a ticket buffer and an identification processing server constitutes each MPA server. Simultaneously, the quantity of channels in the processing server aligns with the quantity of servers for each individual MPA, as seen in Table 1.

It is important to acknowledge that the analysis of the subsequent level of system functioning with LHS was limited to the upper level of GHR. The consideration of interaction with local servers and study of their configuration should be approached as distinct entities within the context of a particular task at hand.

VI. RESULTS AND DISSECTION:

1. MATHEMATICAL MODEL

The notations are interconnected and play a crucial role in creating a secure communication structure between the LHR and GHR servers in the Handle system. The security model guarantees the protection of messages transmitted between servers against unauthorized access, manipulation, or interception through the utilization of encryption, decryption, authentication, and digital signatures. In addition, the system decreases data transfer overhead and minimizes delays by minimizing the number of authentication messages while maintaining security. This makes it suited for usage in resource-constrained IoT devices..

In order to address security concerns in the region between the LHR and GHR servers, the proposed Handle system establishes two distinct categories of messages that are involved in the communication process. The initial form of communication is transmitted from the LHR server to the GHR server and subjected to encryption using a predetermined key. Digital signatures are included in the second type of message, which is forwarded from the GHR server to the LHR server. The suggested Handle system employs a security model that minimizes the number of messages required for the authentication procedure. This technique demonstrates efficacy in the context of Internet of Things (IoT) devices due to its

ability to decrease the overall volume of data transmitted, while concurrently mitigating delays in the security procedure.

The mathematical model described in this study aims to enhance the security and confidentiality of transmitted data during the exchange of service messages within the framework of digital objects. By optimizing data exchange operations, the model enables the utilization of a minimal number of messages to guarantee the authentication process. The efficacy of the suggested strategy in IoT devices lies in its ability to minimize data transfer volume and concurrently mitigate network latency throughout the security process.

2. SIMULATION RESULTS

The operational performance of the DOA system is influenced by several key parameters. These parameters include the network delay experienced by incoming requests, the processing speed of requests by the resolution server, and the number of processing channels allocated to each MPA. It is important to note that the DOA system is constructed upon an existing network architecture for the global Internet.

The average service time for a single request is a crucial characteristic of the resolution system that plays a significant role in defining the Internet of Things. The duration of this process will be contingent upon both the configuration of the system and the magnitude of the load.

Based on the current system setup, Figure 5 illustrates the relationship between the average identifier resolution time and the intensity of incoming requests. The graph illustrates a positive correlation between load intensity and the average resolution time for a single identifier. At elevated workloads, the duration of this process extends to 30 seconds, a considerable duration for practical applications, particularly when juxtaposed with the operational efficiency of the DNS system.

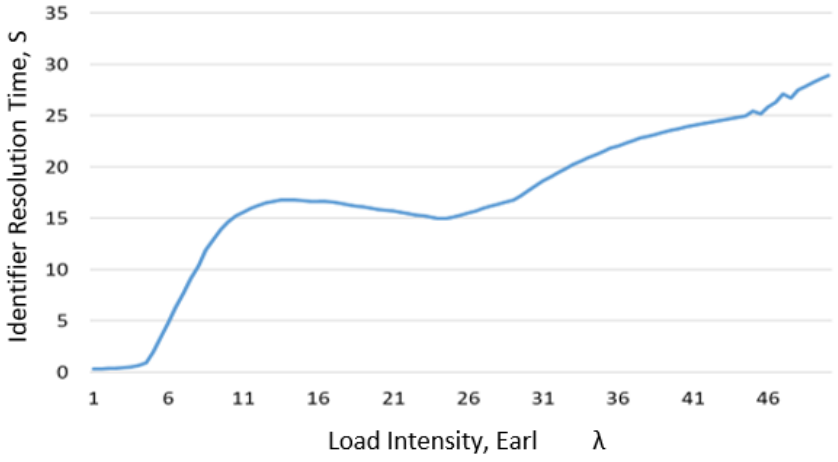

FIGURE 5. The relationship between resolution time and request intensity

In this study, we will utilize the Anylogic environment to do an optimization experiment aimed at determining the optimal server architecture for the GHR system. The objective is to minimize the average identifier resolution time by considering the present configuration of time delays. Each MPA will utilize a specific number of GHR servers as the primary parameter for optimization. Our purpose is to minimize the time it takes to resolve requests. Please configure the resolution time to a maximum of 1 second. It is

recommended to assign an intensity value of 50 Lambda, denoted by a symbol, where lambda represents the parameter of the exponential distribution of the time at which requests are received. The results of the optimization process are depicted in Figure 6.

In the developed model, the load intensity parameter is denoted as alfa, while the number of servers for each MPA is represented by d1...d8. The graph depicted in Figure 5 illustrates that the utilization of this particular arrangement of GHR servers significantly enhances the speed of the identification resolution within the system. At the highest intensity of the load, a 15-fold increase in speed is attained.

	Current	Best
Iterations completed:	500	60
Objective: ↓	3.947	0.878
Parameters		Copy best
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 6. The resolution time is contingent upon the intensity of requests prior to achieving optimal configuration.

The iterative optimization method for the proposed QS model is depicted in Figure 7. The optimization method involves the successive execution of the model, wherein different optimization factors, such as the number of GHR servers, are varied to attain the predetermined objective of achieving an identifier resolution time of less than 1 second. The optimization function for the parameters of the current iteration (shown by the grey graph) and the parameters of the optimal version (represented by the blue graph) is calculated. Upon completion of the optimization process, we obtain a collection of parameters (namely, the number of GHR servers) that closely yield an identifier resolution time of no more than 1 second. The present model setup consists of 7, 10, 1, 10.10, 10, 10, and 10 servers for each MPA, as indicated in Table 1.

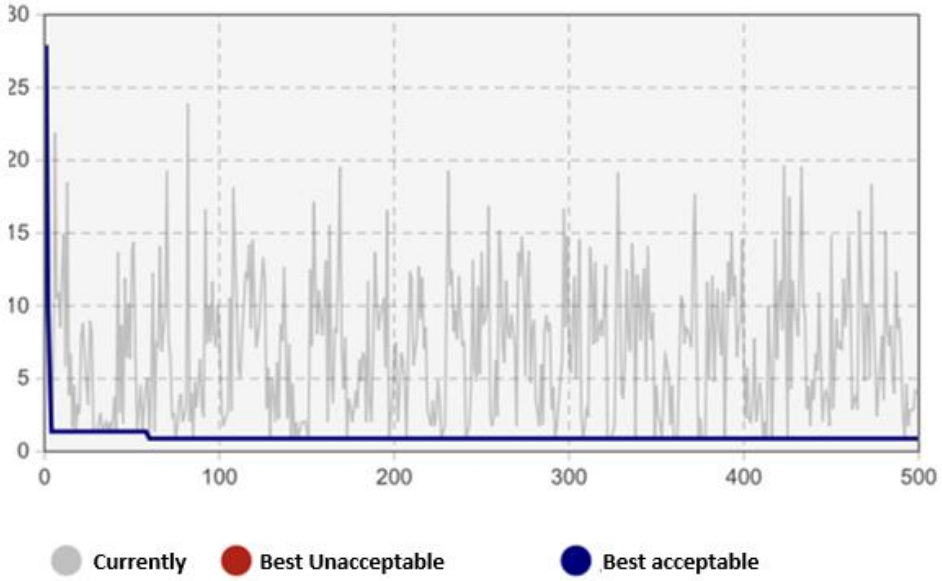

FIGURE 7. The relationship between resolution time and request intensity.

Figure 8 illustrates the correlation between the time it takes to resolve a request and the number of requ ests received, using the server configuration obtained from the optimisation experiment.

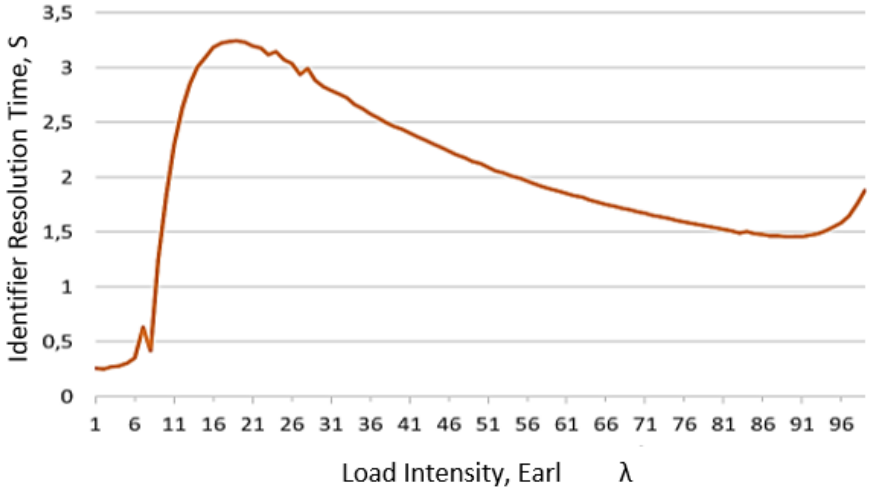

FIGURE 8. The relationship between resolution time and request intensity following optimal configuration.

This graph provides insight into how changes in the volume of incoming requests impact the time it takes for the server to process and resolve these requests. By analyzing this dependency, one can better understand the performance characteristics of the server under varying workload conditions.

VII. CONCLUSION

Digital Object Architecture has the potential to become the Internet of Things' primary device architecture, resolving a number of compatibility problems. To enhance the security and confidentiality of transmitted data during service message exchange within the digital object's framework, a mathematical model is proposed. This model optimizes data exchange processes, enabling authentication with minimal message usage. The scheme is particularly effective for IoT devices as it reduces data transfer volumes and network delays while ensuring overall security.

For the benefit of other applications that wish to communicate with this device as well as the original IOT application, the global identification permits access to the device and its detection. In many Internet of Things applications, the ownership and access control rights established by the digital object can guarantee secure access to the device without sacrificing the essential security measures. Without regard to the original program, the interface communicating with the device is readily available. According to the results of the system simulation, the existing infrastructure of the resolution system has to be expanded and distributed in order to handle high workloads and reduce the time it takes to resolve incoming requests. This assertion holds validity when employing the DOA architecture and resolution system in tasks pertaining to the identification of Internet of Things (IoT) devices, which are estimated to be in the billions. In this scenario, the level of requests within the resolution system can reach a significantly elevated intensity.

In conjunction with the expansion of the current infrastructure, it is imperative to enhance the software component of the resolution system. Upon analyzing the open-source library provided by Handling.net for constructing client solutions to interact with the resolution system, it was observed that there was no initial assessment of network delay time for each server when sending an identifier resolution request to GHR servers. A random order is employed to query each server listed in Table 1, and the initial response returned is subjected to analysis. Undoubtedly, this implementation has a significant impact on the overall duration of identification resolution. Hence, more novel adaptations are necessary to establish the capability of sorting and prioritizing GHR servers based on the network latency experienced by the client device.

REFERENCES

1. Lakhan, A., Mohammed, M. A., Zebari, D. A., Abdulkareem, K. H., Deveci, M., Marhoon, H. A., ... & Martinek, R. (2024). Augmented IoT Cooperative Vehicular Framework Based on Distributed Deep Blockchain Networks. *IEEE Internet of Things Journal*.
2. Abualkishik, A., Alzyadat, W., Al Share, M., Al-Khaifi, S., & Nazari, M. (2023). Intelligent Gesture Recognition System for Deaf People by using CNN and IoT. International Journal of Advances in Soft Computing & Its Applications, 15(1).
3. Yousif, J. H., & Abdalgader, K. (2022). Experimental and mathematical models for real-time monitoring and auto watering using IoT architecture. Computers, 11(1), 7.
4. Mohammed, M. A., Lakhan, A., Zebari, D. A., Abd Ghani, M. K., Marhoon, H. A., Abdulkareem, K. H., ... & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, *129*, 107612.
5. Dayong, W., Bakar, K. B. A., & Isyaku, B. (2023). A Survey on IoT Task Offloading Decisions in Multi-access Edge Computing: A Decision Content Perspective. *Qubahan Academic Journal*, *3*(4), 422-436.
6. Mohammed, M. A., Lakhan, A., Zebari, D. A., Abdulkareem, K. H., Nedoma, J., Martinek, R., ... & Tiwari, P. (2023). Adaptive secure malware efficient machine learning algorithm for healthcare data. *CAAI Transactions on Intelligence Technology*.
7. Zahid, H. M., Saleem, Y., Hayat, F., Khan, F. Z., Alroobaea, R., Almansour, F., ... & Ali, I. (2022). A framework for identification and classification of iot devices for security analysis in heterogeneous network. Wireless Communications and Mobile Computing, 2022.
8. Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., et al. (2023). Homomorphic federated learning schemes enabled pedestrian and vehicle detection system. *Internet of Things*, *23*, 100903.
9. Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017, April). ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In Proceedings of the symposium on applied computing (pp. 506-509).

10. Mohammed, M. A., Lakhan, A., Abdulkareem, K. Het al. (2023). Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. *Internet of Things*, *22*, 100815.
11. Al-Bahri, M., Ateya, A., Muthanna, A., Algarni, A. D., & Soliman, N. F. (2023). Digital Object Architecture for IoT Networks. Intelligent Automation & Soft Computing, 35(1).
12. Al-Bahri, M., Yankovsky, A., Kirichek, R., & Borodin, A. (2019). Smart system based on DOA & IoT for products monitoring & anti-counterfeiting. In 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC) (pp. 1-5). IEEE.
13. Jubair, M. A., Mostafa, S. A., Zebari, D. A., et al. (2022). A QoS aware cluster head selection and hybrid cryptography routing protocol for enhancing efficiency and security of VANETs. *IEEE Access*, *10*, 124792-124804.
14. Durand, A. (2019). Digital object architecture and the handle system. Los Angeles: ICANN—Office of the CTO.
15. Al-Bahri, M., & Al Kishri, W. (2022). DOA Based Identification for Devices and Applications of IoT in Heterogeneous Networks. In The International Conference on Innovations in Computing Research (pp. 417-428). Cham: Springer International Publishing.
16. Koball, C., Rimal, B. P., Wang, Y., Salmen, T., & Ford, C. (2023). IoT Device Identification Using Unsupervised Machine Learning. Information, 14(6), 320.
17. Kostas, K., Just, M., & Lones, M. A. (2022). IoTDevID: A behavior-based device identification method for the IoT. IEEE Internet of Things Journal, 9(23), 23741-23749.
18. Kolcun, R., Popescu, D. A., Safronov, V., Yadav, P., Mandalari, A. M., Mortier, R., & Haddadi, H. (2021). Revisiting iot device identification. arXiv preprint arXiv:2107.07818.
19. Khalil, U., Ahmad, A., Abdel-Aty, A. H., Elhoseny, M., El-Soud, M. W. A., & Zeshan, F. (2021). Identification of trusted IoT devices for secure delegation. Computers & Electrical Engineering, 90, 106988.
20. Kirubadevi, T., Ramamoorthy, S., & Rajavarman, V. N. (2019, November). Device identification and authentication for internet of things using predefined characteristics. In Journal of Physics: Conference Series (Vol. 1362, No. 1, p. 012067). IOP Publishing.
21. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685.
22. Ahmed, F. Y., Yousif, J. H., Alshar'e, M., El Sheikh, M., Al-Ajmi, E., & Al-Bahri, M. (2024). Smart In-Cabin Air Monitoring System using IoT Technologies. Qubahan Academic Journal, 4(1), 78-90.