Artificial Intelligence & Robotics Development Journal
Volume 1, Issue 1, pp 43-57, January 2021, https://doi.org/10.52098/airdj.202123
ISSN: 2788-9696 Received: 4/2/2021 Revised: 15/2/2021 Accepted: 22/2/2021

Expert system for identifying and analyzing the IoT devices using Augmented Reality Approach

Wasin Al-Kishri[1] and Mahmood Al-Bahri[2, *]
[1,2] Faculty of Computing and Information Technology, Sohar University, Oman.
[*] Corresponding author: Mahmood Al-Bahri, mbahri@su.edu.om

Abstract

Biometrics In conjunction with the new development of the Internet of Things (IoT), augmented reality (AR) systems are evolving to visualize 3D virtual models of the real world into an intelligent and interactive virtual reality environment that facilitates physical identification of objects and defines their specifications efficiently. The integration between AR and IoT in a complementary way helps identify network-related items' specifications and interact with the Internet of Things more efficiently. An identity is a dedicated, publicly known attribute or set of names for an individual device. Typically, identifiers operate within a specific area or network, making it difficult to identify things globally. This paper explores the use of Augmented Reality (AR) Technology for identifying devices and displaying relevant information about the device to the user. Based on the developed model network, the developed system of identification of IoT devices was tested. Also, the traffic generated by the AR device when generating requests to the organization server was investigated. According to the test results, the system is undemanding to the main network indicators. The system-generated traffic is self-similar. The test results show that the server software can solve the problems of identifying IoT devices through interaction with augmented reality devices.

Keywords: Augmented reality; Internet of Things; Human Computer Interactions; IoT evaluation; Communication networks;

1. Introduction

The Internet of Things is currently a generally accepted concept for developing communication networks in the short and long term. It is also considered an advanced platform for creating digital intelligence in the idea of a "smart state" (Albahri et al., 2018). According to most consulting analytics firms, over the next five years, more than 30 billion devices will be present in each area of human activity. Thus, we can talk about the pervasive nature of the Internet of Things' penetration into our daily life (Albahri et al., 2019c).

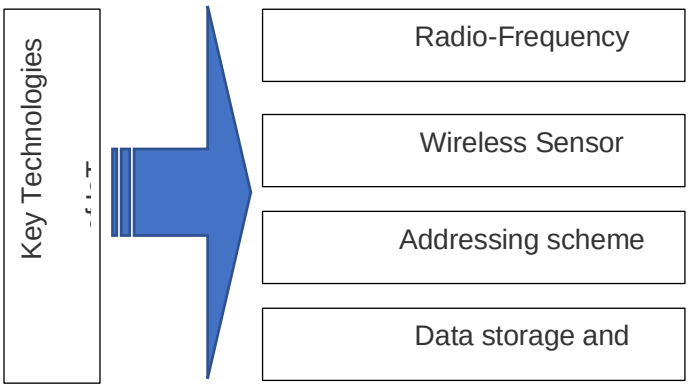
The phrase "Internet of Things" was first heard by Kevin Ashton in 1999 at the presentation of innovative solutions from Procter & Gamble. Ashton suggested applying RFID tags to its products and thus ensuring its interaction with the radio receiver. Kevin Eton indicated that such data collection could be used to solve many problems in the real world. Internet, interacting with smartphones, with each other and with similar, similar devices (Albahri et al., 2019a). In 2001, the MIT Auto-ID Research Center (where Kevin Ashton worked) adapted RFID tags for various products that could track over the Internet. In 2005, the term Internet of Things was officially used by the International Telecommunication Union (ITU) in a technical report on promising concepts for developing communication networks (Albahri et al., 2019b).

In the last decade, the Internet of Things has become one of the breakthrough technologies generally recognized by all world countries. IoT allows people and things to interact anywhere, anytime, and in any combination using the IoT infrastructure. The IoT ecosystem involves collecting data from sensors (or sending commands to actuators), transmitting them through a communication network to cloud platforms for subsequent analysis to provide intelligent services for people. Figure 1 shows the key components required to build an IoT system. According to the model, sensors and information retrieval devices collect various data types about a particular object. These data can then be further processed and analyzed to extract useful information to provide intelligent services (Al-Bahri et al.,2020).

The Internet of Things can be seen as a collection of four main elements:

- Internet: to ensure communication anytime and anywhere between any participants in the internetworking exchange. Cloud computing, intelligent web services, etc.
- Hardware: includes communication equipment and pickup terminals such as sensors, tags, actuators, and transmitters.
- Middleware: used for storing data, calculating, and analyzing transmitted data;
- Interface: used to visualize and interpret the collected results for different platforms and applications.

Various IoT applications are aimed at solving specific problems. Typical applications include data management, analytics, visualization, management of heterogeneous networks, research goals, etc. Nevertheless, IoT research is still in its infancy due to the existence of many unresolved problems. For example, issues related to battery life, the



simplicity of the "lightness" of data transfer technologies, performing actions depending on the context of what is happening, identification and security issues, the cost of terminal devices, scalability, and heterogeneity (Standardisation, 2017).

Figure 1. Key Technologies of IoT (Albreem et al., 2017)

Despite all the advantages of the Internet of Things, there have recently been cases of disclosure of data collected by IoT devices, which raises concerns about the identity of devices and applications within the IoT concept framework. Indeed, identifying things plays a vital role in the classification and recognizing system (Hasoon et al., 2011). For example, attackers can use portable RFID / NFC readers to steal personal information from bank cards in public transport using technology vulnerabilities such as PayPass. This is possible due to the lack of confirmation of the identity of the RFID reader's owner. Another example is the possibility of an attacker intercepting data from networks of IoT devices to obtain IMEI-identifiers of various terminal devices equipped with modems to subsequent broadcasting of intentionally distorted messages.

Current solutions worldwide are mainly aimed at binding an IoT device or application with an identifier similar to an IP address or a mobile phone number. One can understand who is using a particular device. Research in this area was initiated due to discussing these issues in the BEREC (Body of European Regulators for Electronic Communications) (Standardisation, 2017). Simultaneously, identification has a much broader scope and is more appropriate for many applications and entities (subjects) in IoT. In addition to identification purposes in communications, ongoing research includes issues of identification of physical and virtual things, such as services for

users using IoT, collected data, location. Today, various identification schemes have already been standardized and implemented in multiple devices available in the open trade (Albreem et al., 2017).

Different types of identifiers are used depending on the application and user requirements (Saini et al., 2009). The Internet of Things is the interaction between things and users of things using auxiliary elements of the ecosystem: sensors, actuators, wireless communications, cloud platforms, etc. (Yousif & Alattar, 2017). Items and users should 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 IoT ecosystem; identification is also an important aspect. The interaction of various entities with associated identifiers within the IoT concept framework is shown in Figure 2, utilizing AIOTI WG03 High-Level Architecture (Standardisation, 2017).

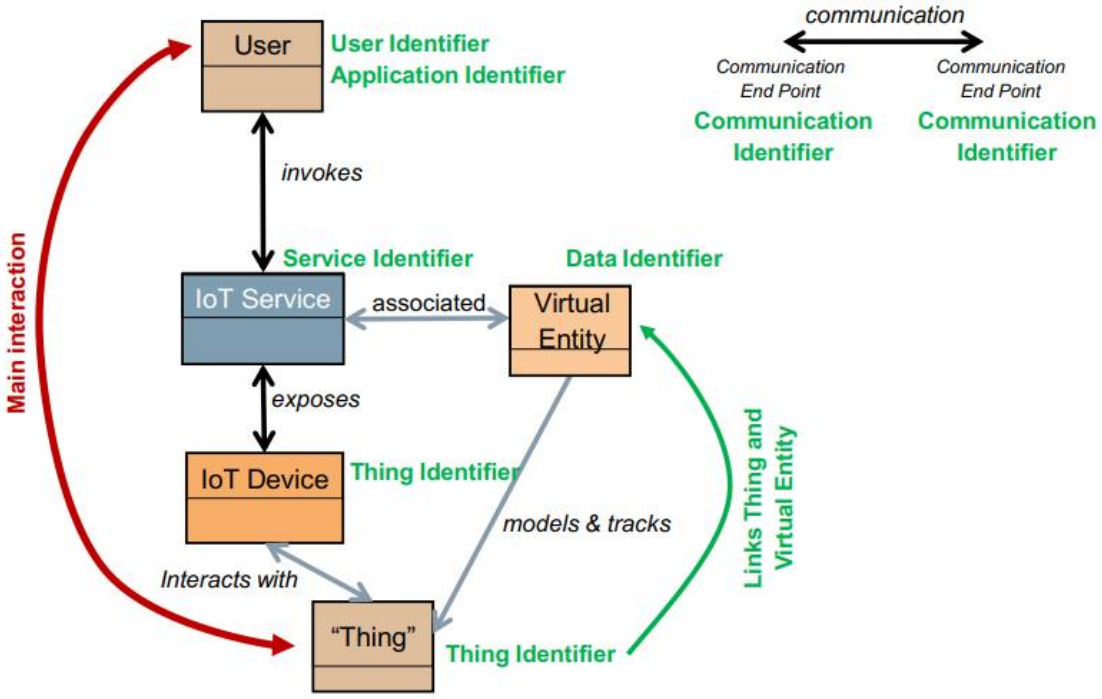


Figure 2. The main components of the Internet of Things (Standardisation, 2017)

The new generation of the Fourth Industrial Revolution has recently emerged, enabling connectivity and access to real-time insights across processes, products, and people. That give user unlimited opportunities for using various services and applications over the internet. Recently, scientists have become more interested in the Internet of Things (IoT) and Augmented Reality (AR)

to make spaces more intelligent and interactive. The amazing development of the Internet of Things technology enables the possibility of connecting and exchanging data between various devices through the Internet and communication protocols (Hu et al., 2021). The Internet of Things supplies related data in the physical environment (sensory, auditory, visual) into augmented reality to provide a convenient and intuitive way for users to visualize and interact with objects in the real world.

One of the exciting areas of this concept is the provision of services based on augmented Reality Technology. Augmented reality supplements the existing world with the necessary data. For example, looking at a shop window glasses, augmented reality can be seen and the mannequins the entire range of products, sizes, and prices, without going inside. There is already an extensive selection of augmented reality glasses, differing in functionality and communication network requirements. Some of them are almost indistinguishable from regular glasses (Hu et al., 2021). The availability and simplicity of equipment stimulate the creation of a variety of services. So, the use of augmented reality technology is difficult to overestimate; it is used both in medicine and education. Also, it uses for solving everyday problems, in industry and agriculture, in VANET networks, and flying sensor networks.

2. Literature Survey

The Phupattanasilp and Tong (Phupattanasilp and Tong, 2019) introduced the AR-IoT method based on augmented reality (AR) to support IoT data visualization. The proposed method uses IoT Multi-camera data over real-world objects to improves the identification of 3D images with a non-destructive and low-cost imaging platform of the IoT. The results show a high integration of IoT data with AR resolution, effectively updating accuracy and precision (Phupattanasilp & Tong, 2019). Miettinen (Miettinen et al., 2017) designed a system for automatically identifying IoT devices to manage the security and privacy risks in users' networks. The researchers introduce the IoT devices identification technique based on profiling of the device type-specific communication behavior of each device in the network. The proposed system protects the user's network by enforcing network isolation of potentially vulnerable devices. Thus, error occurrence is controlled and mitigates the security risks associated with these devices. They achieve 0.95 accuracies for 17 devices, most of them reaching 1. However, 10 devices got identified with lower accuracy of around 0.5 (Al-Bahri et al.,2020).

Hamad (Hamad et al., 2019) illustrated that the IoT system identifies challenges by processing a series of network packets. the proposed system tracks the network flow data and extracts specific features to establish a fingerprint for

each device in the network. The researchers adopt a novel supervised machine learning technique for IoT identification tasks. The proposed approach can automatically recognize white-listed device types and unknown devices with abnormal behavior connecting to the network by constraining and enforcing privileges rules for IoT device communications. They achieve 90.3% accuracy, as unknown devices are detected with limited overhead (Hamad et al., 2019). Jo and Kim (Jo and Kim, 2019) adopted an architecture for integrating augmented reality (AR) technology with the Internet of Things for a better shopping experience. AR technologies and frameworks are scalable to deal with any IoT product due to its incorporation into the IoT platform. An intuitive augmented reality-based visualization and interaction allow the provided AR service to reduce latency significantly. The researchers focus on three major architectural components that are required for simplified, scalable AR services, and expertise for IoT-ready products have been identified: object-focused data processing and visualization, entry, control, and interaction with objects, and interoperability. Lund et al. discussed the concept of "Identity in the Internet of Things" and introduced the abbreviation IDoT. Besides, a parallel and analysis is carried out on the subject: why it is so unique compared to the concept of "identity of users" (IDoU) in traditional networks and communication systems. Using ideas of "Identity" of the user (IDoU) from conventional approaches and networks, a stack for "identity" in the Internet of Things is proposed as in Figure 3. The presented information stack has four categories: inheritance, association, knowledge, and context (Lund et al., 2014).

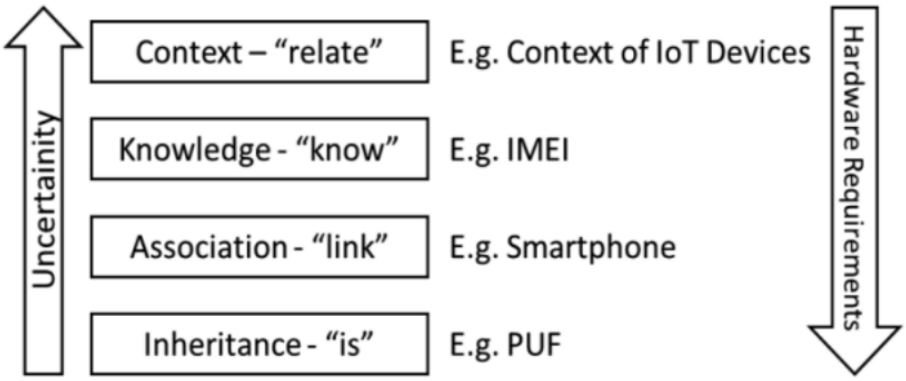


Figure 3. Identity in the internet of things (Lund et al., 2014).

The authors noted that using the proposed stack to define IDIoT is indeed a new paradigm compared to IDoU. Due to the limited availability of information in the middle categories (i.e., "Associations" & "Knowledge"), and the inflexibility of the Inheritance category and the imprecision of the Context category. The risk-based authentication

using multiple factors will certainly be preferred as an option for the Internet of Things. Recommendation ITU-T Y.2057 (Y.2057 11/2011) presents studies based on new Identifier and Locator Split (ILS) schemes. Figure 4 illustrates the abstract concept of traditional identifier (IDF) and locator separation. According to the recommendation, identity is not explicitly associated with the corresponding identifier (s) in all existing ILS schemas. The essence of a thing (or object) may perform many functions in future network architecture, allowing for identifier separation. Therefore, the authors proposed a new IIS schema and the ILS paradigm, which is promoted within a single framework with various potential value-added services (Halavachou & Fei, 2020). Al-Bahri (Al-Bahri et al.,2020) studied the ability of Digital Object Architecture (DOA) Technology to identify IoT devices. The authors mentioned that DOA technology allows for unambiguous persistent identification of objects in which these objects' copyright holders are interested. This makes it reasonable to develop DOA technology as a global identification system with equal rights for all members. The paper shows that there have been no works in which the DOA would be analyzed in detail as a method for identifying devices and applications of the Internet of Things.

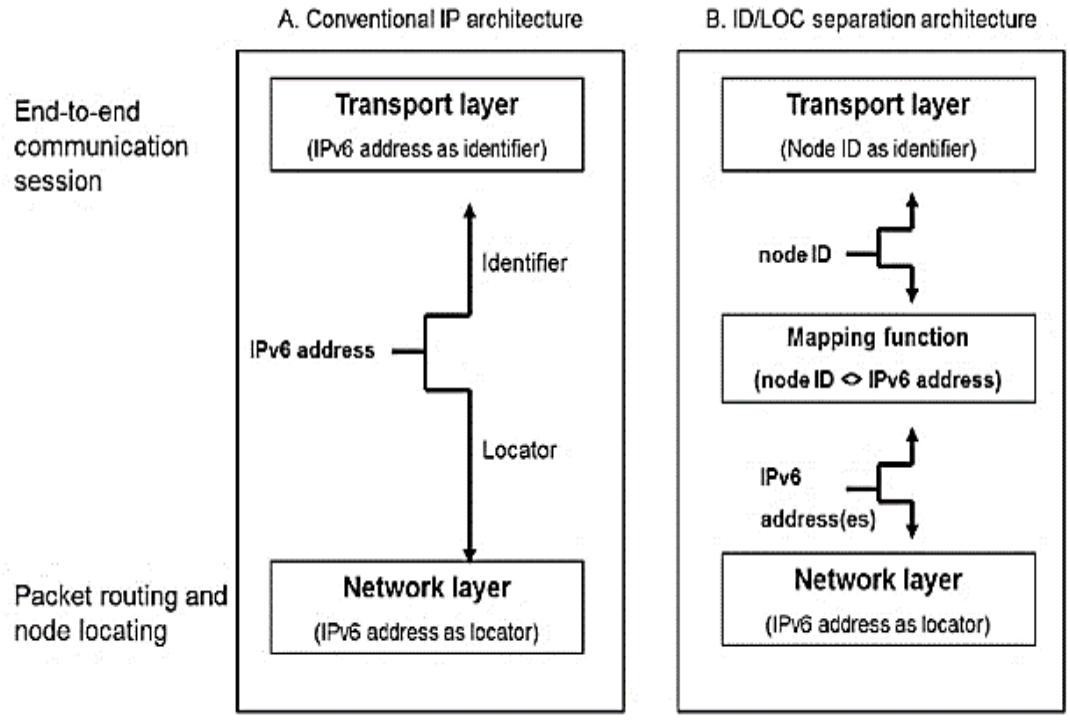


Figure 4: Comparison between conventional IPv6 architecture and ID/LOC separation IPv6 architecture (Halavachou & Fei, 2020)

The proposed approach shows how people can shop in the future using digital and analogs like the real world. The proposed system indicates that shopping augmented reality is more likely to lead to increased usability and customer

loyalty. Through pilot tests, significant support was obtained by the synergies and benefits of the trial. However, there remains a concern that the system should standardize the protocol for sharing data and displaying content.

3. Research Methodology

This work adopted an experimental investigation to explore the Augmented Reality technology implementation in identifying the connected IoT devices in a system and display the relevant information about each of them. Also, a quantitative research method was deployed to analyze the collected data. As noted earlier, the response time to a change in the environment is one of the leading indicators of the quality of augmented reality services. A possible scenario for providing augmented reality services using SETCO cloud services is considered, and hands of the quality of perception under different conditions are analyzed. One of the most pressing problems in the development of the concept of the Internet of Things (IoT) is the identification of IoT devices. The growth in the number of devices connected to the public communications network and their low computing power led to a situation where a person cannot uniquely identify an object. It is proposed to use augmented reality technology to solve the visual identification of devices of the Internet of Things. Augmented Reality allows supplementing the real world with digital information. There are already several solutions based on augmented reality technologies for identifying and inventorying various objects. The identification process assumes that information about the objects searched for by the identifier is stored in a system for storing and processing large amounts of data. As such a system, it is proposed to use "SETCO: Enterprise" to automate the enterprise. This system is successfully used for the inventory of objects owned by the enterprise.

4. Experimental Method

This section proposes a system for identifying IoT devices. This system is based on augmented reality technologies and server software "SETCO: Enterprise" and a model network developed and tested. Figure 5 illustrates the architecture of the identification system (SI) of IoT devices based on augmented reality technologies of the SETCO: Enterprise server software. This identification system consists of:

- SETCO: Enterprise servers (Identification Server - IS).
- Augmented reality devices (Identification Device - ID).
- Devices of the Internet of Things (Identifiable Object - IO).

This model has an identification device, an augmented reality device (namely augmented reality glasses), to identify the Internet of Things devices. The identification device then sends a request to the identification server, a web version of the SETCO: Enterprise software. The identity server processes the request and accesses the database, which returns the sought data and then sends the identity device's data.

4.1. Model network for identification of IOT devices

Based on the above architecture, a model network was developed, as shown in Figure 2. Consisting of:

- Identification devices in Augmented Reality glasses are where a program is run to recognize IoT devices' identifiers (using Bluetooth technology, BLE). Then requests are created to the SETCO server (using HTTP REST), traffic is intercepted and analyzed.
- Identification object is an IOT device with its identifier, on which the software is responsible for interacting with the IoT functions (using Bluetooth technology, BLE).
- Identity servers - a server that is a web version of the SETCO: Enterprise application and a Microsoft SQL 2012 database that stores object identifiers and information.
- Interaction with the identity server takes place using the HTTP REST interface.
- Network jamming devices - a NetDisturb software device allows to simulate a public communication network's operation.

Identification devices were implemented based on augmented reality glasses - Epson Moverio BT-300, operating based on the Android operating system. The Java Programming Language and Android SDK Toolkit (Android Bluetooth, Android HTTP Library) were used to develop programs responsible for interacting with OI and SI. To create the software responsible for intercepting and analyzing traffic, the C ++ was used to the programming language, Android NDK tools, and libations libraries. The identification object was implemented based on an Intel Edison microcomputer. The software responsible for interaction with the Identification Device was implemented using the C ++ programming language and the "libblepp" library.

The identification server is implemented based on SETCO software company "SETCO: Enterprise", SETCO programming language, Microsoft SQL 2012 database. The HTTP REST interface, developed based on the REST concept, includes the following commands:

- GET request. It searches for an item in the database by an object identifier and returns information about the identified object.
- DELETE request. It removes an element from the database by an object identifier.
- POST request. It adds a new object by identifier and information about it.

4.2. Model network testing

The proposed system of identification of IoT devices was tested based on the developed model network. Also, was investigated the traffic generated by the AR device when generating requests to the SETCO server. The work was carried out for periodic GET and POST + DELETE requests for the following network parameters: latency, bandwidth, Hurst parameter. Some parameters were performed on the identification device: Interaction, traffic analysis, and calculation of network parameters. The delay between the arrivals of network packets was calculated using the UNIX Time Stamp system. Throughput was calculated as the sum of the sizes of all packets received in one second.

The Hurst parameter (H) parameter characterizes the system's self-similarity and is used in time series analysis (Coelho, 2011) The value of H can take on the following:

- 0 <H <0.5 - the time series is not self-similar, anti-persistent; it is more likely to change the direction of deviation, high deviation values follow low ones and vice versa.
- H = 0.5 - the time series is random; the next value does not depend on the previous values.
- 0.5 <H <1 - the time series is self-similar, persistent.

In this paper, the Hurst parameter is calculated based on the R / S analysis method based on an array consisting of network delays between packet arrival. The calculation was made according to the following steps:

1. Based on the array of network delays Mi, the time series Ni is calculated for each element of the series i, using the logarithmic ratio as in equation 1:

$$N_i = = \ In\left(\frac{M_i}{M_{(i-1)}}\right) \quad (1)$$

where : i ∈ (1,2,3... N); N = The length of the series Mi

2. Next, the row Ni is divided into A of adjacent intervals Ia of length n, where a is the number of the interval a∈ (1,2,3...A). The average value Ea for each of the intervals Ia is determined as in equation 2:

$$E_a = \frac{1}{n} \sum_{k=1}^{n} N_{k.a} \quad (2)$$

where k ∈ (1,2,3... N);

3. Time series of accumulated deviations Xka from the average value Ea for each of the intervals Ia,

$$X_{k,a} = \sum_{i=1}^{k}\left(N_{i,a} - E_a\right) \sum_{k=1}^{n} N_{k.a} \quad (3)$$

when k∈ (1,2,3..N.) is calculated as in equation 3:

4. The range of the accumulated deviations Ra is calculated as the difference between the maximum and minimum values of the deviation Xk, a within each interval Ia as determined in equation 4:

$$R_a = max\left(X_{k,a}\right) - min\left(X_{k,a}\right) \quad (4)$$

where: 1≤k≤n

5. The standard deviation Sa is calculated for each interval Ia as determined in equation 5:

$$S_a = \frac{1}{n}\sum_{k=1}^{n}\left(N_{k,a} - E_a\right)^2 \quad (5)$$

where: 1≤ k ≤ n

6. The normalized swing of the range of deviations for each interval can be obtained by dividing the swing of the range of accumulated deviations Ra by the standard deviation Sa. Thus, the normalized range of deviations (R / S) n for a period with n elements in the interval is defined as in equation 6:

$$(R/S)_n = \frac{\sum_{a=1}^{A}(R_a/S_a)}{A} \quad (6)$$

where: A- is the number of gaps, a ∈ (1,2,3... A).

7. Items from 1 to 6 are repeated with an increased value of n - the number of elements in the interval up to the value N/2.
8. Next, the regression is performed using the least squares method on **$\log_n$**, where n is the number of elements in the interval as an independent variable and log (R / Sn), where R / Sn is the normalized range of deviations (dependent variable). The result is determined in equation 7:

$$log(R/S_n) = H\, log(n) + c \quad (7)$$

where: i ∈ (1,2,3... A);

5. Experimental Results

The Testing was carried out for the case in which the Augmented Reality device requests information by identifier using the HTTP GET method. The total testing time (traffic interception) is 180 seconds. The countdown starts after receiving the first HTTP packet, which is a request to the identification server. The average packet size is 107 bytes. During testing, various degradations were introduced into the network using a server to install the free NetDisturb software. To create network interference, impairments were made to the following parameters: network delay (ms), throughput (Kbps), jitter (ms). Testing was repeated 50 times, and all results were averaged. The test results are shown in Tables 1, 2, and 3 accordingly (Kulik et al.,2017) and shown in Figures 6, 7, and 8, respectively.

Table 1: System test results with Insertion delays

Insertion delays (ms)	Number of packages delivered	Bandwidth (Kbps)	Latency (ms)	Hurst coefficient
0	2361	31.72	217	0.66
10	2303	30.91	231	0.64
50	2118	26.87	264	0.64
100	1717	21.39	307	0.62
250	1366	16.09	479	0.67
500	715	9.30	701	0.61

Table 2 System test results with input Bandwidth

Input Bandwidth (kbps)	Number of packages delivered	Bandwidth (Kbps)	Latency (ms)	Hurst coefficient
5	364	4.65	1034	0.51
10	738	9.76	628	0.53
15	1022	14.89	432	0.56
20	1389	19.79	284	0.58
30	2345	29.98	223	0.66
35	2360	31.43	215	0.66
No limits	2361	31.72	217	0.66

Table 3. System test results with increasing jitter

Input jitter (ms)	Number of packages delivered	Bandwidth (Kbps)	Latency (ms)	Hurst coefficient
0	2361	31.72	217	0.66

5	2357	30.98	221	0.57
20	2173	27.71	237	0.51
50	1708	22.10	251	0.48
75	1328	17.26	279	0.43
100	813	9.94	431	0.41
150	571	7.90	607	0.38

According to the test results, we can determine that this scenario's system is undemanding to the leading network indicators. The traffic generated by the system is self-similar. The developed model network is resistant to low and average service quality indicators but shows severe deviations from the norm with increasing network restrictions. A particularly severe degradation in system performance can occur when bandwidth is limited; when the jitter indicator's value rises, the traffic changes its properties to anti-persistent.

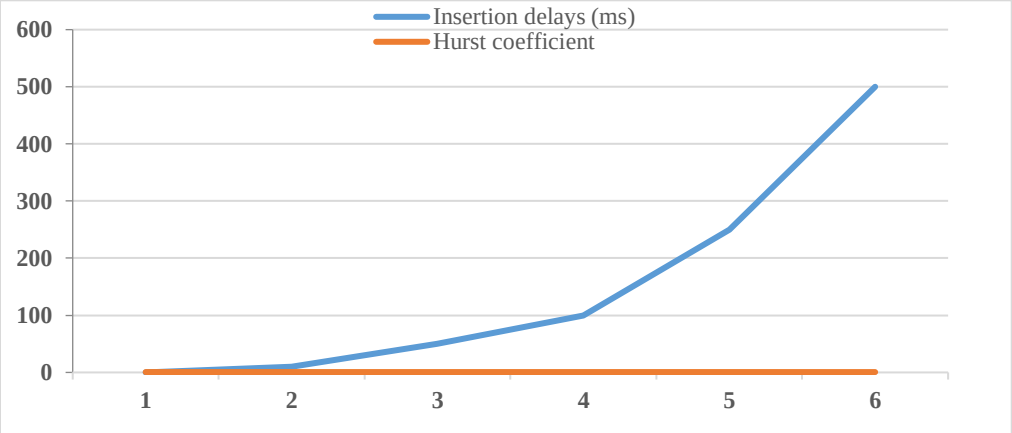


Figure 6: System test results with input delays

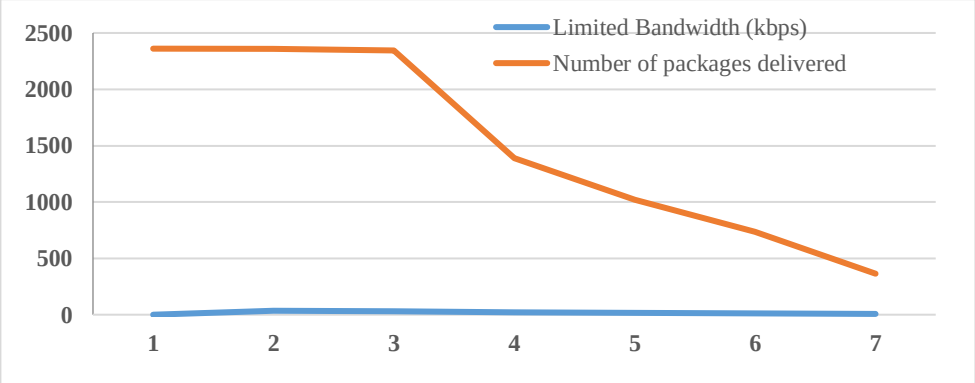


Figure 7: System test results with input Bandwidth

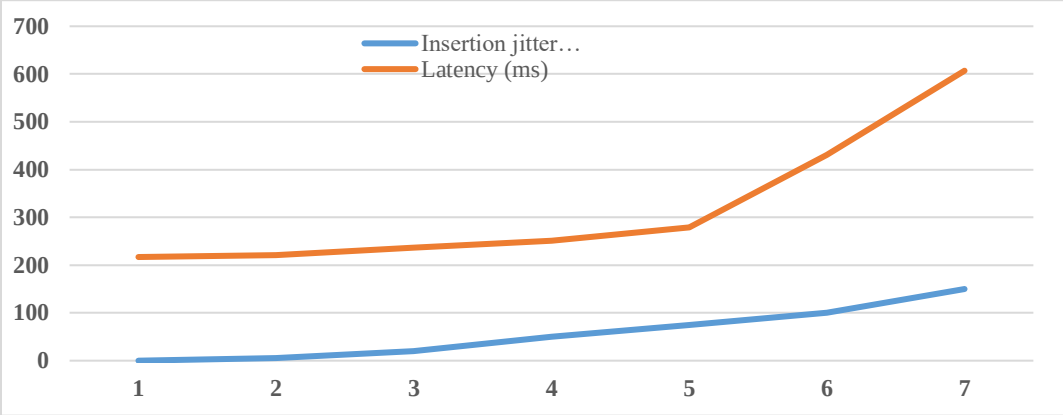


Figure.8: System test results with input jitter

6. Conclusion

This study presents the system's architecture for identifying the IoT devices using augmented reality technologies and server software "SETCO: Enterprise". The use of augmented reality technology to inventory at enterprises and general identification of IoT devices seems interesting. The combined use of SETCO: Enterprise software and augmented reality allows creating several services that can speed up the execution of specific processes in enterprises and improve the quality of perception in the provision of augmented reality and the Internet of Things services. The model network was created and tested based on the proposed architecture. The test results show that the SETCO: Enterprise server software can solve the problems of identifying Internet of Things devices through interaction with augmented reality devices. During testing, it was found that the developed system is resistant to changes in network characteristics. This feature is essential since existing networks transmitting large volumes of different traffic types do not always guarantee the fulfillment of service quality indicators' established values.

Acknowledgment

The research leading to these results has no Funding.

REFERENCE

[1]. Albahri, M., Kirichek, R., Ateya, A. A., Muthanna, A., & Borodin, A. (2018, November). Combating counterfeit for IoT system based on DOA. In 2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) (pp. 1-5). IEEE.

[2]. Al-Bahri, M., Yankovsky, A., Kirichek, R., & Borodin, A. (2019a). 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.

[3]. Al-Bahri, M., Ruslan, K., & Aleksey, B. (2019b). Integrating internet of things with the digital object architecture. In Internet of Things, smart spaces, and next generation networks and systems (pp. 540-547). Springer, Cham.
[4]. Al-Bahri, M., Ruslan, K., & Aleksey, B. (2019c). Integrating internet of things with the digital object architecture. In Internet of Things, smart spaces, and next generation networks and systems (pp. 540-547). Springer, Cham.
[5]. 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.
[6]. Albreem, M. A., El-Saleh, A. A., Isa, M., Salah, W., Jusoh, M., Azizan, M. M., & Ali, A. (2017, November). Green internet of things (IoT): An overview. In 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA) (pp. 1-6). IEEE.
[7]. Coelho, R. F. (2011). *U.S. Patent No. 7,904,295*. Washington, DC: U.S. Patent and Trademark Office.
[8]. Halavachou, Y. U. R. Y., & Fei, X. (2020). Comparison Research on Future Network Between IPv4, IPv6 and IPV9. *Associate Editor-in-Chief*, 28.
[9]. Hamad, S. A., Zhang, W. E., Sheng, Q. Z., & Nepal, S. (2019, August). IoT device Identification via network-flow based fingerprinting and learning. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 103-111). IEEE.
[10]. Hasoon, F. N., Yousif, J. H., Hasson, N. N., & Ramli, A. R. (2011). Image Enhancement Using Nonlinear Filtering Based Neural Network. Journal of Computing, 3(5), 171-176.
[11]. Hu, M., Luo, X., Chen, J., Lee, Y. C., Zhou, Y., & Wu, D. (2021). Virtual reality: A survey of enabling technologies and its applications in IoT. Journal of Network and Computer Applications, 102970.
[12]. Jo, D., & Kim, G. J. (2019). IoT+ AR: pervasive and augmented environments for "Digi-log" shopping experience. Human-centric Computing and Information Sciences, 9(1), 1-17.
[13]. Kulik, V., Kirichek, R., Borodin, A., & Koucheryavy, A. (2017, September). Measurement system architecture for measuring network parameters of e2e services. In *International Conference on Distributed Computer and Communication Networks* (pp. 291-306). Springer, Cham.
[14]. Lund, D., MacGillivray, C., Turner, V., & Morales, M. (2014). Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand. *International Data Corporation (IDC), Tech. Rep*, *1*(1), 9.
[15]. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017, June). Iot sentinel: Automated device-type identification for security enforcement in iot. In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS) (pp. 2177-2184). IEEE.
[16]. Phupattanasilp, P., & Tong, S. R. (2019). Augmented reality in the integrative Internet of Things (AR-IoT): Application for precision farming. Sustainability, 11(9), 2658.
[17]. Saini, D. K., Yousif, J. H., & Omar, W. M. (2009). Enhanced inquiry method for malicious object identification. ACM SIGSOFT Software Engineering Notes, 34(3), 1-5.
[18]. Standardisation, A. W. L. (2017). High Level Architecture (HLA). Technical specification.
[19]. Yousif, J. H., & Alattar, N. N. (2017). Cloud management system based air quality. International Journal of Computation and Applied Sciences (IJOCAAS), 2(2).