www.ijaceeonline.com ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

Literature Review on IoT Challenges and Testing

Roaa Wadullah Tareq
PG Scholar, College of Engineering,
Computer Engineering Department, University of Mosul, Iraq
Email: roaa.enp77@student.uomosul.edu.iq

Turkan Ahmed Khaleel
Senior Lecturer, College of Engineering,
Computer Engineering Department, University of Mosul, Iraq
Email: turkan@uomosul.edu.iq

Abstract: *Day after day technology is developing in the world. Also, the development of these technologies brings innovations and Comforts to all areas of life. However, ensuring the durability of these innovations brought about by technology reveals various problems. Among the most important of these innovations is the Internet of Things. The Internet of things increases the quality of human life and is the most important topic of work in recent times. The Internet of Things has entered into several aspects, including in smart homes, medical applications, in the agricultural and industrial fields, and others. It is important to be able to communicate more securely and work in a coordinated manner to ensure the continuity of applications. Therefore, it faces challenges that must be overcome as well as it needs testing and examination methods to improve the quality of Internet of things applications and to be accepted by users. In this paper, we try to cover the Internet of Things architecture and challenges, to understand more Internet of things systems, in addition to the methods and types of tests, and the most important future trends in this field.*

Keyword: *Internet of Things; IoT Architecture; Challenges; Testing; MQTT protocol;*

1. INTRODUCTION

One of the most important innovations is the Internet of Things in the world, which has entered most aspects of life. It was first introduced in 1999 by Kevin Ashton [1]. The Internet of Things (IoT) allows objects and machines to communicate and connect to exchange data via the Internet. [2] The idea behind this new technology is to connect objects through the Internet that we utilize in daily life. Special kinds of sensors are connected to each object to collect and capture information from the physical world. The information after collect is analyzed via local processing to remove needless data and then store this information in local storage. From the local storage, the information is transfer to the cloud storage where whole the sensors (objects) collected it. Finally, utilizing the information collected, objects, and machines can also be managed remotely and utilize the information to hold records for future utilize [3].

Humans can interact with the Internet of things to access data, give instructions, or configure it, but it does its work without human intervention as it connects the real world to the virtual world. IoT objects or devices can be connected to a network and each other using wireless and wired technologies, for instance, Wi-Fi, Bluetooth, LTE, etc. Soon, the Internet of Things will generate a massive amount of data this can be called (Big Data), which has characteristics various from those of the conventional communication paradigm (Data, Video, Voice) [4]. Figure 1 indicates the using the Internet of Things (IoT), anything (object) can connect to the Internet at any time and from anywhere to provide any service through any network (any net) to anyone (any person). This notion will create new types of applications such as smart homes, smart cars as well as in the medical field and the agricultural and industrial field to provide and supply many services like notifications, energy-saving, security, and other services.

By 2020, about 50 billion smart devices will be connected via the Internet [5]. The presence of these devices is possible thanks to all the small elements of the smartphone that are available in great numbers these days besides the fact that the permanent connection to the Internet is the default case of work or home networks. Realizing the IoT model involves numerous challenges that need to be solved, including reliability, availability, performance, interoperability, scalability, mobility, security, trust, and management [6].

Cite this paper:

Roaa Wadullah Tareq, Turkan Ahmed Khaleel, "Literature Review on IoT Challenges and Testing", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 11, pp. 1-10, November 2020.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

Many communication protocols for the Internet of Things are being developed by companies to enable IoT devices to communicate more efficiently for the network to process the protocol used to connect devices. Network traffic, amount of data transferred, data transmission, as well as problems with limited hardware features of IoT devices with hardware and power-efficient issues in issuing important devices [5].

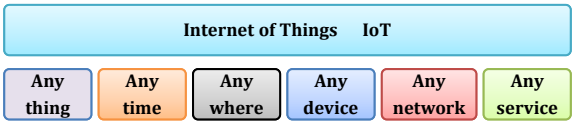

Figure 1 Internet of Things (IoT) Concept

The most common protocol in the Internet of Things Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), and HyperText Transfer Protocol (HTTP)[7]. Efforts are now concentrated on testing the Internet of things environment by adopting various types such as usability and communication tests using protocols as a simulation of the environment in which the device will be used, and ensuring the exchange of information in a safe manner [8] as well as Performance and Interoperability tests, but in return, some challenges must be faced and solutions to them. The Internet of Things faces open issues that need to be addressed to properly implement it, including security and privacy, as well as scalability, interoperability, and data management in addition to the lack of homogeneity of components with each other [9]. Implementing the Internet of Things requires several important things Which: Cloud Computing the big data can be accessed through the cloud where it is stored there and processed there It can be said that the cloud represents the " Brain" of most of the Internet of things [10], Access the ability to access from anywhere, anytime , Security is an important factor that forms part of the requirements of the Internet of Things, in addtion User Experience , Smart Machines, Asset Management, Big Data Analytics and Management and Energy Efficiency.

2. THE FUNDAMENTAL LAYERS OF IOT ARCHITECTURE

There is no standard structure for the Internet of Things. It may consist of three, four, or five layers [11]. The most common consists of three layers: the perception layer, the network layer, and finally the application layer [3, 12]. The tertiary structure illustrates the basic idea of the Internet of Things. To understand the structure more, the network layer is divided into two layers, the transport layer and the processing layer, and also the business layer is added to the application layer. To better understand the basics of the IoT testing environment, We need first to understand this IoT application architecture:

2.1 Perception Layer

Includes sensors, actuators, and edge devices that interact with the environment and the physical environment [13]. The goal of this layer is to identify objects in the Internet of Things uniquely, which can be achieved by gathering information from the sensors as they send data from the surrounding environment to the next layers (upper) for processing. One of the problems facing components in this layer is power consumption as well as network connectivity, as well as the data collected, which may be vulnerable to penetration in addition to large data volume.

2.2 Network Layer

Connects devices across the network that are responsible for the connection of other smart things, network devices, and servers [13]. It is split into two sub-layers, the first layer is the Transport Layer, the transfer and transmission of sensor data between layers and over networks such as WAN, MAN, and LAN via Wi-Fi, Bluetooth, LoRaWAN, etc. It also utilizes IPv6 addressing to give addresses to the objects in the IoT system. The second, the Processing Layer, is also called the Middleware Layer. It is responsible to collect the information that comes from the transport layer that is responsible for analyzing, storing, and processing the large data collected from the sensors [14]. They may use databases, cloud computing, and big data processing resources [15]. TABLE (I) illustrates the most important communication techniques in the field of IoT [16-18]. The network may suffer from problems such as weak wireless signal, ensuring efficient and safe communication.

2.3 Application Layer

Responsible for providing specialized services and functions to users [19]. IoT applications can be in smart homes, smart cities, and smart vehicles as well as medical care and other applications. The services may differ for each of these applications because the service relies on the information collected by the sensors. The application layer is divided into a business layer that works application management and deals with privacy and security.

The second layer is also known as the application layer, which differentiates between various applications. There are a lot of issues at the application layer where security is the main issue. The protocols on the Internet are being developed within the application layer to make them more secure. The most important protocols in the application layer [20, 21] are shown in TABLE II.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

TABLE I COMMUNICATION TECHNOLOGY OF IOT

Communication Technology	Standard	Network	Specification
Wi-Fi	IEEE 802.11	WLAN	High data rate but high consumption energy
Bluetooth LE	IEEE 802.15.1	WPAN	Moderate to transmit data with low power consumption
ZigBee	IEEE 802.15.4	WPAN	Low data rate but doesn't require a lot of power
6LOWPAN	IEEE 802.15.4	WPAN	Low data rate and low power consumption
LoRaWAN	LoRa Alliance	Long Range Wireless WAN	Low data rate and low power consumption

TABLE II APPLICATION LAYER PROTOCOL OF IOT

Protocol	Designed By	Model	Security	Transport
CoAP	IETF	Request/ Response	DTLS	UDP
MQTT	IBM	Publish/ Subscribe	TLS/SSL	TCP
AMQP	OASIS	Request/ Response or publish/ subscribe	TLS/SSL	TCP
XMPP	IETF	Request/ Response bidirectional communication and Publish/ Subscribe multi-directional communication	TLS/ SASL	TCP

3. INTERNET OF THINGS (IOT) CHALLENGES

The Internet of Things (IoT) makes things (smart devices) in the environment around us to be active, that is, they share information with other objects or communicate across networks (wireless / wired) that utilize the Internet Protocol (IP) predominately. Data processing makes the Internet of Things to know changes and events in the environment around us and "things" can behave and interact independently.

However, all of these demand heterogeneous devices exchange for the information in a way called an interoperable manner to enable their data, interpretable, and services accessible by other devices. The Internet of Things is a modern emerging field that requires not only the expansion of technologies and infrastructure but also the deployment of new services capable of supporting, scalable (cloud-based) and interoperable (communication protocols). An important IoT problem that needs to be solved is the interoperability of services and information [23]. The most important challenges facing the Internet of Things can be summarized:

3.1 Interoperability

It knows interoperability as the ability to implement programs, transfer data, and communicate between different functional units in a way. IEEE defines interoperability as the ability of two or more systems or components to exchange information and to use the information that has been exchanged [24]. In the Internet of things, objects and components are heterogeneous, as the various elements that make up the Internet of Things (devices, communications, applications, services, etc.) must correspond, collaborate seamlessly also communicate with each one with another [25]. In-Network level, interoperability transacts with mechanisms to make the seamless interchange of messages among systems through various networks for End-To-End communication. Because of the dynamic and heterogeneous network that is in an IoT environment, the level of network interoperability must be able to deal with issues such as addressing, routing, resource optimization, security, quality of service, and mobility support [26]. IoT interoperability can be seen from different perspectives such as device interoperability, networking interoperability, syntactic interoperability, semantic interoperability, and platform interoperability.

3.2 Security and Privacy

Since the basic principle of the Internet of Things includes connecting devices, it enables everything locatable and routes it which enables our life easier. However, making everything online opens the field to hackers. Without suitable confidence about privacy and security, will never be attracted to the Internet of Things by the user. Therefore, it must have a robust infrastructure [27]. Privacy and Security and represent a major challenge in IoT systems, which requires sev-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

eral things, including the authentication of devices, confidentiality, and data integrity, as well as the implementation and operation of security operations on the scope of the Internet of Things system and meeting performance requirements according to the use case of the system. It is important to keep the system data without being hacked or tampered with.

3.3 Coverage

Coverage is one of the challenges facing the Internet of Things, as it is restricted to the power supply in addition to Scalability [28]. Devices in the Internet of Things usually move and are not united to a power source, so their intelligence must be powered from a self-sufficient power source as well. The Internet of Things has a great concept from the traditional Internet because things collaborate in an open environment so functions such as communication and service discovery must work efficiently in Both large and small-sized environments. The Internet of Things requires methods and new functions to have an efficient scalability process [29].

3.4 Volume and Data Exchange

Wireless technologies are used to connect smart devices. Whereas, it includes issues such as availability, network delays, congestion, and so on [30]. Also, it will collect huge amounts of data at the central level in network nodes or servers. This phenomenon represents Big Data and it requires many operational mechanisms in addition to new technologies for storage, as well as processing and management [29].

3.5 Self-configuration

Devices within the Internet of things must be able to self-configure in a specific environment without user intervention (manual configuration).

4. IOT ARCHITECTURE TESTING AND CHALLENGES

There are still some challenges facing the IoT that need to be verified, such as network and interconnection, and security is a major concern in the IoT platform, and the complexity of software and system may mask the error in IoT technology as well as resources such as memory limitations, processing power, bandwidth, and battery life. And so on. The heterogeneous nature of IoT hardware and components [31] requires robust testing abilities to guarantee performance and service that meets user needs and requirements as well as service-level acceptance among consumers and service providers. Testing is the process of identifying failures that occur in a particular system. The failure consists of any discrepancy between actual and expected results [32]. To ensure the performance of IoT-based devices, scalability, reliability, and security must be verified. Recently, there has been a need to focus on testing the different layers and components that make up the Internet. IoT systems rely heavily on data, and ensuring the integrity of the data, and making sure that the system is resilient to anomalous data will do so. These are just a few of the many IoT-related testing and confirmation issues [33].

Challenges for testing IoT environment can be mentioned as follows: Much effort is required between multiple teams to obtain correct test data, There are many sub-systems and sub-components that are related to each other and a problem with any of them can affect the entire system, It takes a lot of effort and is difficult to replicate the actual environment, Compatibility factor, Security challenges, Complexity issue, Safety concerns, Finally The tools used in IoT may not be available every time. Internet of Things service requires extensive testing to meet user and marketing requirements.

We look at some of the best practices that can ensure IoT testing is successful. To make implementation effective, we must focus on quality assurance through a good testing approach. Where the basis of IoT testing is also determined by the structured requirements, overall testing plan, unit testing, system testing, and integration testing. The use of advanced tools, controllers, and simulators can ensure the successful implementation of the test and the project. An understanding of architecture, operating systems, and hardware can assist in designing and implementing good new test cases.

5. LEVELS TESTING AND METHODS

There are certain kinds of virtual object testing. The Virtual object exists in the world of information and can be manipulated, accessed, and stored. Examples of these things are multimedia content and application software.

5.1 TEST LEVELS

Different test levels are defined, as follows [32]:

5.1.1 Unit Testing

To determine which errors are likely to occur in the system, the program components are examined separately and separately. Each part of the system is isolated and individual parts are shown to suit the requirements and functions.

5.1.2 Integration Testing

The components and contents of the program that were tested through unit testing are combined and then tested for problems. As software and hardware components are integrated, they are tested to verify the interaction between them and how they perform together.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

5.1.3 System Testing

The entire system's functioning is analyzed in the interaction between its software and hardware components. Complete and integrated system testing to verify the system's compliance with specific behavior and requirements.

5.1.4 Acceptance Testing

An acceptance test is performed to determine Whether the system meets the acceptance criteria or not. The user usually runs these tests during a beta test period.

5.2 TEST METHODS

Different methods can be used to test the System Under Test (SUT), gray-box testing, white-box testing, and black-box testing. These methods are followed as:

5.2.1 The Black Box Testing

The Black Box Testing is a technique used to examine and test a specific application program without knowing the details of the design, code, structure, knowledge of internal paths in addition to the internal implementation of the program or system.

5.2.2 The White Box Testing

In White Box Tests, a thorough knowledge of the structure, code, and implementation under the test of the system is required where all internal parts of the SUT are visible. It is not limited to detecting failure only, but also in detecting errors for the system. This test is performed at the beginning of the system development process with unit tests as well as the first parts of the integration phase.

5.2.3 The Gray Box Testing

The last method is a combination of the two types, the white box, and the black box, in which knowledge of the system or program is partly, in addition to understanding how it works partially. Only failures are detected.

6. INTERNET OF THINGS TESTING TYPES

During system development, it is necessary to test the physical hardware in addition to software testing, interface analysis, data, and real-time flow testing. It is requisite to begin testing with the architecture of the Internet of Things and the specific tasks to find methods to improve the performance of the existing system of the most important types of testing the Internet. Within the Internet of Things system, several types of tests are conducted as defined by Cognizant [34]:

6.1 Functional Testing

The functionality of the components of the Internet of Things application is verified to ensure the correct work of the system to obtain the required quality [35]. It is important to have prior planning to build solutions and tools necessary to simulate systems environments that may face obstacles and challenges that companies must deal with through the testing of their products. This will require a lot of experimental innovation to ensure quality. The functional testing phase of the Internet of Things begins with making virtual devices that can emulate a real environment and real connectivity, for instance, the Nest team designed the Nest Home Simulator Test Tool Working with Nest products, common system events, and sensor conditions are tested using a virtual environment.

6.2 Connectivity Testing

Two main things are verified: the presence of the network connection and the absence of the connection. This test responsible for testing the wireless signal to locate if many devices are trying to communicate or there is a poor connection [36]. The primary goal of connectivity testing is to make communication among objects and components of the Internet of Things and the communications infrastructure. Seamless and secure communication is its main theme Significance in the Internet of Things. All objects must be connected and to other systems, such as servers of IoT. The success of the IoT system relies on how well the objects or devices communicate in an IoT environment. A disconnection or loss of a connection in a part second may lead to incorrect and inaccurate data, creating an unusable system data file. There are currently many tools obtainable for testing APIs.

The tools can emulate a message sent/received by the device, helping to verify the accuracy of the information. Connection testing is performed both offline and online. The online test can analyze communication among data transmission, and network security, devices, and applications. Some applications need constant communication such as health monitors or pacemakers Regardless of the network state, the application should have the capacity to save and store as well Processing data created while offline, then transferring it when the connection of the network is being operated. This should be taken into account in connection tests (signal strength, network type, Also, weather conditions, etc. must be taken into account) and the application must be checked if it works under these conditions.

6.3 Performance Testing

The computational capabilities, data collection and processing, and communication are checked. Performance testing refers to testing and confirming the conduct of IoT devices along with the network and

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

the internal abilities of the network and systems communications. The network and communication speed is further evaluated Computing capabilities. It must be verified that data is being transferred and saved properly, even in the event of an unforeseen outage. The main goal of performance testing is to locate the relevance between the program and the object that interacts with it and unify the link among them. As well as the performance test to verify the correctness of the hardware and software components according to the Specific test situations.

It is evaluated whether the application can manipulate the expected excess. In user traffic, frequency of transactions, amount of data, further processing Scalability The extent of compatibility between the system must also be checked for the effectiveness of4. the Sensors in a real IoT environment. For evaluation and validation of the performance of an IoT application Response time for various download rates, the code requires to be improved and should be followed varied scenarios like memory reduction, switching between different Grids and battery discharge, and so on.

Performance Testing of IoT includes the next aspects:

- Every authenticated device within the domain must be able to communicate.
- The device should be able to transmit any amount of data (as needed).
- If the data transfer by a device overtakes the preset amount, the data must be transferred It starts only after receiving confirmation.
- The device should be able to transmit data, in case of problems with the power supply these cases should be fixed possible quickly.

There are three levels to target performance Testing:

- System level: database, processing, and analysis.
- Application level.
- gateway and Network level: Test technologies like Wi-Fi, Z-Wave, Bluetooth, and protocols like MQTT, CoAP, HTTP, and others.

6.4 Security and Privacy Testing

Focus on authorization, privacy, and authentication features. It is important to focus on protecting data so that hackers cannot access it remotely via a wireless connection. The security testing covered confidentiality, independence, oversight, and protection from spying. Appropriate security and penetration tests are necessary due to poor security this can lead to loss of important sensitive personal information. In the situation of IoT applications, Also cybercriminals, stealing private information can also attack home security Systems or the systems inside the car that cause incidents. With the increase in the number of embedded sensors reaching billions, there must be a treatment to data privacy issues in the IoT ecosystem. Among the most important requirements for a security test are:

1. Identification and authentication.
2. Protect data by encrypting it.
3. Providing security for data stored in the local cloud and also the remote cloud.

No unauthorized (not having permission) access to systems or information.

The Security Test is predominately overlooked due to persistent market pressure on companies for new product launches, this type of test is also neglected the manufacturers of IoT objects do not understand the Security Tests.

Two Security Testing Types [37]:

- **Static Test:** It is performed either with support code verification tool or manually. The major function is to analyze program code established for the device, recognition is potential security vulnerabilities.
- **Dynamic Test:** It used specific tools to examine the device through its normal execution and detected the issues with authentication, objection and analyze network traffic, hacker attack simulation, etc.

6.5 Compatibility Testing

Checks correct functionality with different protocols and configurations of IoT. Different operating systems, browser types, and their versions, different generation devices, and connection mode compatibility testing are very important for IoT [38]. Since the nature of the Internet of things and its components is different and heterogeneous addition to that they may differ in operating systems, versions, networks, and devices, and the interaction of each component must be ensured, as well as ensuring compatibility of the communication protocols and security and scalability in data exchange. All this requires compatibility testing is a step Basic needs to be done in the real world without virtual simulation.

6.6 Exploratory Testing

Also called User Experience testing, which is based on the user's evaluation. The exploratory test is done in an experimental system where it can be studied. The IoT Embedded Software Exploratory Test com-

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

bines the logical world of the Internet and the physical world. The success of any program, including IoT software, is specified by its users. IoT applications that meet user requirements can fail if they do not gain the trust and credibility of the target audience. Also, Exploratory tests are significant due it allows to determine the behavior of the application when used by a file the end-user. An Exploratory Test is a kind of test that is the procedure from a user's view.

6.7 Interoperability Testing

To ensure interoperability at the network level between hardware components, it is not sufficient to simply adhere to the specifications of the used protocol because these often contain ambiguities that can lead to partially or completely incompatible implementations. Also, developers may choose to improve protocol implementation that may have a negative impact on communication with a different application [39]. Interoperability test It requests from producers to test their products on the same actual site with a network intermediate they can agree on Performing tests on how two or more products are communicating access to special interoperability functions. The interoperability test does not verify whether the product conforms to the reference protocol standard specifications. This test defines a set of test scenarios to verify a program target that can interact with the other. The software components are developed based on the same specifications but are implemented by various manufacturers. As an outcome, to procedure, a suitable test for the target program standards level based interoperability testing with conformance testing must be procedure as finished mechanisms [40].

6.8 Updates Testing

The Internet of Things consists of several operating systems, protocols, devices, network layers, firmware, and so on. To rule out potential errors while updating the system or the application as all, it is needful to behavior a during test. At the same time, different adjustments are performed to the total strategy to avert the obstacle and difficulties related to the update [4].

6.9 Combinatorial Testing

Combinatorial Testing (CT) is a Black Box Testing method that ensures high-quality of the software program with decreased check effort. It is a check format methodology and has proved to be very fine when utilized on giant complicated structures involving a massive wide variety of parameter-value combinations. CT can be utilized on two varieties of testing, configuration parameter-values acknowledged as configuration-based checking out or combos of entering parameter values recognized as input-based trying out [41, 42].

6.10 Stressing Testing

This type of test correlating with the generation of packet flow in the network. this is used to determine the behavior of the networks in the following three things: Throughput, Latency, and Fault evidence [43].

7. FUTURE WORK TRENDS FOR IOT TESTING

1. Artificial Intelligence (AI)

The use of artificial intelligence will ensure that IoT systems are tested with a degree of reliability more than a manual test that requires intense work. Technology experts have already started working in this field to take advantage of the capabilities that artificial intelligence can provide in this field.

2. Wireless Connectivity Tests

The wireless network will play a major role in IoT systems that rely on standards such as Wi-Fi, ZigBee, and 4G LTE. There will be several scenarios for testing wireless connectivity ensuring continuous data transfer between the device and the server.

3. Testing Big Data

The Internet of things generates a large amount of data that needs to be organized and processed also needs to manage. All of this requires advanced testing as it is not possible to deal with this huge data using traditional testing techniques. It is expected that work on developing big data testing will take place soon.

4. Security Challenges

Work is continuing in the field of testing the security of the Internet of things systems, as it is considered an important factor to ensure confidentiality and privacy. Security for the data is extremely important.

5. Communication Protocols

The use of communication protocols for the Internet of Things to create algorithms to ensure uninterrupted communication in the network as well as to ensure security and privacy.

8. LITERATURE REVIEW

Recently, interest in the field of testing the Internet of Things has become in various aspects applications, and work is still underway on the development of this field. Most reports focus on performance testing and IoT testbed deployments. The TABLE (III) below shows the most important work carried out in this field.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

TABLE III LITERATURE REVIEW OF IOT TESTING

Paper	Describe	The Result
[44]	Using middleware to evaluate and study under different conditions of the network the performance of the CoAP and MQTT protocols. The goal of the experiment was to determine the impact of different parameters like Bandwidth “total data transferred per message” and delay.	The Experiment results show when packet loss is reduced, the protocol MQTT suffers less delay than CoAP. Also, the protocol CoAP suffers the greatest delays when increasing packet loss.
[45]	A sensor was used Temperature & Humidity Sensor with PC Server as MQTT Broker.	MQTT protocol faster to transfer data (Six times faster) than HTTP in real-time.
[46]	Healthcare has been implemented using heart rate monitoring sensors, a SpO2 monitor, and a comparative performance evaluation between CoAP based system and MQTT.	The Experiment shows that the protocol proposed CoAP based messaging system is superior to previous messaging systems.
[47]	Tested The Range of Distance And Reliability of LoRa Technology.	We can say that LoRa is a promising technology in the field of long-range and high-reliable communication.
[48]	Read data from pressure, temperature, and humidity sensors, then publish them on a specific topic to an MQTT broker server using different brokers. another MQTT client, called "subscriber" was created to receive data.	Mosquitto wasted the least time to transfer the messages to the client after then came HiveMQ.
[49]	1. Implement of MQTT client in gateway layer and MQTT server in the backend layer. 2. Testing the accuracy by using HTTP.	The time taken to transfer data is less in MQTT protocol than HTTP. It is also less energy-intensive than HTTP But it is not reliable MQTT is an asynchronous protocol.
[50]	Stress Testing was performed using MQTT Protocol for several types of Brokers the comparison of the results is presented by different metrics (CPU, latency, and message rates).	Mosquitto is the most efficient, optimized with the least latency in QoS1 and QoS2 category among all brokers have tested so far.

From the above, we note that Internet of things systems face challenges in their design, as well as that the testing process for them is mostly in the application layer using communication protocols, and the most important of these protocols are MQTT and CoAP.

9. CONCLUSION

The Internet of Things is the link between the real world and the virtual world. Interest in and demand for it has increased, as it entered all aspects of life. It has become possible to imagine anything smart that can collect data, connect to the Internet, and make decisions on behalf of humans by giving him orders, and based on them, he can meet most human needs. On the other hand, obstacles and challenges are facing this innovation. Work is still being done to develop and improve the Internet of Things.

The most important challenges that are still researched and considered important topics in this field are maintaining data security and privacy. Researches are focusing on developing lightweight encryption algorithms, developing a secure structure for the Internet of Things, and work is still ongoing. Security is a major issue. There is also a need for intermediate software to control, manage, and monitor the data collected from the sensors. Likewise, the nature of the components in the Internet of things is heterogeneous and tends to be complex. Other challenges have emerged, interoperability, and interoperability between components. This type of challenge is concerned with the capabilities, standards, and protocols of devices connected to the Internet, which aims to support the practice of seamless communication. Also, there are other challenges such as energy and memory limitations. All of the above needs to be tested by the developers to ensure the quality of the IoT application before it is on the market and to be at the required level for the user without errors or failure.

REFERENCES

[1] Bassam Al-Shargabi and Omer Sabri, (2017), “Internet of Things: An exploration study of opportunities and challenges*”, International Conference on Engineering & MIS (ICEMIS)*, pp. 1-4

[2] Marcus Oppitz and Peter Tomsu. (2018) , “Inventing the cloud century*” Cham: Springer, Internet of Things*, Austria. pp. 435-436.

[3] Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. (2018), “IoT elements, layered architectures, and security issues: A comprehensive survey” *Sensors*, Vol. 18, Issue. 9, pp. 2796.

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

[4] Svitlana Popereshnyak, Olha Suprun, Oleh Suprun, and Tadeusz Wieckowski, (2018), "IoT application testing features based on the modeling network", *Proceedings of IEEE XIV-the International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH)*, pp. 127-131

[5] Fikret Yalçinkaya, Hüseyin Aydilek, Mustafa Yasin Erten, and Nihat Inanç, (2020), "IoT based Smart Home Testbed using MQTT Communication Protocol" *Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi,* Vol. 12, Issue. 1, pp. 317-324.

[6] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, (2015), "Internet of things: A survey on enabling technologies, protocols, and applications" *IEEE communications surveys & tutorials,* Vol. 17, Issue. 4, pp. 2347-2376.

[7] Eyhab Al-Masri, Karan Raj Kalyanam, John Batts, Jonathan Kim, Sharanjit Singh, Tammy Vo, and charlotte Yan, (2020) "Investigating Messaging Protocols for the Internet of Things IoT" *IEEE Access,* Vol. 8, pp. 94880-94911.

[8] Rahul Reddy Nadikattu (2020), "Data Safety and Integrity Issue in IoT" *International Journal of Electrical and Computer Engineering (IJECE),* Vol.8, Issue.6, pp. 1268-1276.

[9] C.C. Sobin. (2020), "A Survey on Architecture, Protocols, and Challenges in IoT" *Wireless Personal Communications,* pp. 1-47.

[10] Chamandeep Kaur. (2020), "The Cloud Computing and Internet of Things (IoT)" *International Journal of Scientific Research in Science, Engineering, and Technology(IJSRSET),* Vol. 7, Issue. 1, pp. 19-22.

[11] A. Tewari and B. Gupta. (2020), "Security, privacy and trust of different layers in Internet-of-Things (IoT) framework" *Future generation computer systems,* Vol. 108, pp. 909-920.

[12] Ibrahim Mashal, Osama Alsaryrah, Tein Yaw Chung, Cheng Zen Yang, Wen Hsing Kuo, and Dharma P. Agrawal. (2015), "Choices for interaction with things on the Internet and underlying issues" *Ad Hoc Networks,* Vol. 28, pp. 68-90.

[13] Pallavi Sethi and Smrruti R. Sarangi. (2017), "Internet of things: architectures, protocols, and applications" *Journal of Electrical and Computer Engineering,* Vol. 2017, pp. 25.

[14] K. Govinda and R.A.K Saravanaguru.(2016), "Review on IoT technologies" *International Journal of Applied Engineering Research,* Vol.11, Issue.4, pp. 2848-2853.

[15] Shivangi Vashi, Jyotsnamayee Ram, Janit Modi, Saurav Verma, and Chetana Prakash. (2017), "Internet of Things (IoT): A vision, architectural elements, and security issues", *International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)(I-SMAC)*, pp. 492-496

[16] Shadi Al-Sarawi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi. (2017), "Internet of Things (IoT) communication protocols", 8*th International Conference on information technology (ICIT)*, pp. 685-690

[17] Dan Dragomir, Laura Gheorghe, Seriu Costea, and Alexandru Radovici. (2016), "A survey on secure communication protocols for IoT systems", *International Workshop on Secure Internet of Things (SIoT)*, pp. 47-62

[18] Tara Salman and Raj Jain. (2019), "A survey of protocols and standards for internet of things" *arXiv preprint arXiv:1903.11549,* Vol.1, Issue.1, pp. 20.

[19] Dagogo Godwin Orifama and Hope Okoro. (2020), "Security Challenges in IoT Platforms and Possible Solutions" *Computing,* Vol.8, Issue.1, pp. 1-7.

[20] Vasileios Karagiannis, Periklis Chatzimisios, Francisco Vazquez-Gallego, and Jesus Alonso-Zarate.(2015), "A survey on application layer protocols for the internet of things" *Transaction on IoT and Cloud computing,* Vol. 3, Issue.1, pp. 11-17.

[21] Jasenka Dizdarević, Francisco Carpio, Admela Jukan, and Xavi Masip-Bruin. (2019), "A survey of communication protocols for the internet of things and related challenges of fog and cloud computing integration" *ACM Computing Surveys (CSUR),* Vol.51, Issue.6, pp. 1-29.

[22] Amine Rghioui and Abdelmajid Oumnad. (2017), "Internet of Things: Surveys for Measuring Human Activities from Everywhere" *International Journal of Electrical and Computer Engineering (IJECE),* Vol. 7, Issue.5, pp. 2474-2482.

[23] Benny Sand, (2015), "IoT Testing-The Big Challenge Why, What and How", *Springer in International Internet of Things Summit*, pp. 70-76

[24] Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung, (2016), "The internet of things: new interoperability, management and security challenges", *arXiv preprint arXiv:1604.04824*, Vol. 8, Issue.2, pp. 85-102.

[25] Mahda Noura, Mohammed Atiquzzaman, and Martin Gaedke. (2019), "Interoperability in internet of things: Taxonomies and open challenges" *Mobile Networks and Applications,* Vol. 24, Issue.3 pp. 796-809.

[26] Oladayo Bello, Sherali Zeadally, and Mohamad Badra. (2017), "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)" *Ad Hoc Networks,* Vol. 57, pp. 52-62.

[27] Carsten Maple. (2017),"Security and privacy in the internet of things" *Journal of Cyber Policy,* Vol. 2, Issue.2, pp. 155-184.

[28] A. Haridas, V. S. Rao, R. V. Prasad, and C. Sarkar. (2018), "Opportunities and challenges in using energy-harvesting for NB-IoT" *ACM SIGBED Review*, Vol.15, Issue.5, pp.7-13.

[29] Zeinab Kamal and Elmustafa Sayed Ali Ahmed. (2017), "Internet of things applications, challenges, and related future technologies" *World Scientific News,* Vol. 2, Issue.67, pp. 126-148.

[30] Ashvini Balte, Asmita Kashid, and Balaji Patil. (2015), "Security Issues in the Internet of things (IoT): A survey" *International Journal of Advanced Research in Computer Science and Software Engineering,* Vol.5, Issue.4, pp.450-455.

[31] Anna Katrina Gomez and SimiKamini Bajaj, (2019), "Challenges of Testing Complex Internet of Things (IoT) Devices and Systems", *Proceedings of IEEE 11th International Conference on Knowledge and Systems Engineering (KSE)*, pp. 1-4

[32] Joao Pedro Dias, Flavio Couto, Ana C. Paiva, and Hugo Sereno Ferreira, (2018), "A brief overview of existing tools for testing the internet-of-things", *Proceedings of IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, pp. 104-109

[33] Jeffrey Voas, Rick Kuhn, Phillip Laplante, and Sophia Applebaum, (2018), "Internet of Things (IoT) Trust Concerns (Draft)", *National Institute of Standards and Technology*, pp.1-42

ISSN: 2456 - 3935
International Journal of Advances in Computer and Electronics Engineering
Volume 5, Issue 11, November 2020, pp. 1–10

[34] Cognizant, *The internet of things: Qa unleashed*, retrieved date:[November 2016], online available at https://www.cognizant.com/whitepapers/the-internet-of-things-qa-unleashed-codex1233.pdf

[35] John Esquiagola, Laisa Costa, Pablo Calcina, Geovane Fedrecheski, and Marcelo Zuffo. (2017), "Performance Testing of an Internet of Things Platform", *IoTBDS*, pp. 309-314

[36] Ghadeer Murad, Aalaa Badarneh, Abdallah Qusef, and Fadi Almasalha, (2018), "Software Testing Techniques in IoT", *Proceedings of IEEE 8th International Conference on Computer Science and Information Technology (CSIT)*, pp. 17-21

[37] Shantanu Pal, Michael Hitchens, and Vijay Varadharajan, (2017), "On the design of security mechanisms for the internet of things", *Proceedings of IEEE 11th International Conference on Sensing Technology (ICST)*, pp. 1-6

[38] Manas Kumar Yogi and K. Mahesh Kumar. (2017), "Testing IoT: Novel Perspectives, Challenges, Future Work" *International Journal Of Engineering Technology And Management Sciences,* Vol. 1, Issue.1, pp. 1-6.

[39] Philipp Rosenkranz, Matthias Wählisch, Emmanuel Baccelli and Ludwig Ortmann, (2015), "A distributed test system architecture for open-source IoT software", in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, pp. 43-48

[40] Hiun Kim, Abbas Ahmad, Jaeyoung Hwang, Hamza Baqa, Franck Le Gall, Miguel Angel Reina Ortega, and Jaeseung Song. (2018), "IoT-TaaS: Towards a prospective IoT testing framework", *IEEE Access,* Vol. 6, pp. 15480-15493.

[41] Preeti Satish and Krishnan Rangarajan. (2019), "A hybrid test prioritization technique for combinatorial testing" *International Journal of Intelligent Systems Technologies and Applications,* Vol.18, Issue. 1/2, pp. 84-100.

[42] Jeff Voas, Rick Kuhn, and Phil Laplante, (2018), "Testing IoT Systems", *IEEE Symposium on Service-Oriented System Engineering (SOSE)*, pp. 48-52

[43] Piotr Lech and Przemysław Włodarski, (2016)," IoT WiFi Home Network Stress Test", *Springer International Conference on Image Processing and Communications*, pp. 247-254

[44] Dinesh Thangavel, Colin Keng-Yan Tan, Xiaoping Ma, Alvin Valera and Hwee-Xian Tan, (2014), "Performance evaluation of MQTT and CoAP via a common middleware", *IEEE 9th international conference on intelligent sensors, sensor networks and information processing (ISSNIP)*, pp. 1-6

[45] R. Atmoko, R. Riantini, and M. Hasin. (2017), "IoT real-time data acquisition using MQTT protocol" *Journal of Physics: Conference Series*, Vol.853, Issue.1, pp. 1-6

[46] Brian Oryema, Hyun-Su Kim, Wei Li, and Jong Tae Park, (2017), "Design and implementation of an interoperable messaging system for IoT healthcare services", *IEEE 14th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 45-52

[47] Hrvoje Rudeš, Ivana Nižetić Kosović, Toni Perković and Mario Čagalj, (2018), "Towards reliable IoT: Testing Lora communication", *IEEE 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 1-3

[48] Biswajeeban Mishra, (2018), "Performance evaluation of MQTT broker servers", *Springer International Conference on Computational Science and Its Applications*, pp. 599-609

[49] J. Maha Kavya Sri, V. G. Narendra, and Vidya Pai. (2019), "Implementing and testing of IoT technology in agriculture" *International Journal of Recent Technology and Engineering,* Vol.7, Issue.6, pp. 848-852.

[50] Biswajeeban Mishra and Biswaranjan Mishra, (2020), "Evaluating and Analyzing MQTT Brokers with Stress-testing", *University of Szeged 12th Conference of Ph.D. Students in Computer Science,* pp.1-4

Authors Biography

Roaa Wadullah Tareq received a B.Sc. degree in Computer and Information Engineering from Mosul University, Mosul, Iraq, in 2012. She is currently working toward an M.Sc. degree in Computer Engineering at the College of Engineering at Mosul University. She is interested in researching the Internet of Things, Protocols that use in this field**,** and Testing IoT.

Dr. Turkan Ahmed Khaleel received the B.Sc., the M.Sc., and a Ph.D. degree in Computer Sciences from Mosul University, Mosul, Iraq, in 1993, 2002, and 2013, respectively. She was a Lecturer with the Computer Engineering Department, Mosul University, Mosul, Iraq, Her research interests include remote sensing image processing, neural network, computer networks, IoT, and network security

Cite this paper:

Roaa Wadullah Tareq, Turkan Ahmed Khaleel, "Literature Review on IoT Challenges and Testing", International Journal of Advances in Computer and Electronics Engineering, Vol. 5, No. 11, pp. 1-10, November 2020.