A Comprehensive Review of Recent Advances, Architectures, Applications, Open Challenges, and Future Research Directions in Internet of Things

Ammar Thabit Zahary [1,2,*]
Elham Ali Shammar [1]

[1] Faculty of Computer and Information Technology, Sana'a University, Sana'a, Yemen

[2] Department of Computer Science, Faculty of Computing and Information Technology, University of Science and Technology (USTY), Sana'a, Yemen

* Corresponding author: a.zahary@ust.edu.ye

https://doi.org/10.59222/ustjet.4.1.1

A Comprehensive Review of Recent Advances, Architectures, Applications, Open Challenges, and Future Research Directions in Internet of Things

Abstract:

Recently, the Internet of Things (IoT) has gained significant popularity and has become a fundamental part of our world. Nowadays, IoT applications are more frequent than we think; the number of IoT devices is exponentially increasing. Many significant studies and research investigations were introduced to improve technology using IoT. However, for researchers who have a lack of holistic technical knowledge and recent advances of IoT, numerous topics and issues related to advances of IoT must be addressed from a before IoT can fully realize its potential, such as IoT architecture, components including hardware, operating systems (OSs), communication technologies, protocols, and applications. This paper conducts a holistic review of recent advances, visions, evolution, architectures, Components (hardware, middleware, and OSs), and applications of IoT. In addition, the paper investigates the recent challenges, open issues, and future research of IoT technologies. This paper assists researchers in understanding the key advances with a technical depth of the Internet of Things and the recent applications in the real world. The paper identifies IoT priority challenges and open issues, providing a guide for those leading IoT initiatives and revealing opportunities for future IoT research.

Keywords: Internet of Things, IoT, IoT advances, IoT architecture, IoT technologies, IoT applications.

https://doi.org/10.59222/ustjet.4.1.1

مراجعة شاملة للمفاهيم الحديثة، والمعماريات، والتطبيقات، والتحديات المفتوحة، والاتجاهات البحثية المستقبلية في إنترنت الأشياء

الملخص:

اكتسبت تقنية انترنت الأشياء مؤخرا شعبية هامة وأصبحت جزء أساسي من عالمنا الحديث. في أيامنا هذه أصبحت تطبيقات انترنت الأشياء متوفرة أكثر مما نتصور، حيث أصبحت أعداد أجهزة انترنت الأشياء تتزايد بدالة أسية. تم اجراء العديد من الدراسات والبحوث السابقة لتحسين التكنولوجيا باستخدام انترنت الأشياء، لكن الباحث الذي لا يمتلك معرفة عميقة بالعديد من المواضيع والقضايا لا يزال بحاجة الى تسليط الضوء من خلال رؤية حديثة وشاملة لتلك المواضيع المرتبطة بإنترنت الأشياء. وهذا ما تقدمه هذه الورقة البحثية، حيث تقدم مراجعة حديثة وشاملة للمواضيع المهمة في انترنت الأشياء مثل المفاهيم المتقدمة لإنترنت الأشياء، ورؤيتها، ومراحل تطورها، والمكونات المادية، والبرمجية وخصوصا نظم التشغيل، إضافة إلى المعماريات والتطبيقات الحديثة لإنترنت الأشياء. إضافة إلى ذلك، تحلل هذه الورقة البحثية في أحدث التحديات والقضايا المفتوحة والاتجاهات المستقبلية لإنترنت الأشياء. هذه الورقة البحثية تساعد الباحثين على فهم أبرز القضايا الحديثة بعمق تقني في إنترنت الأشياء وتطبيقاته الحديثة في العالم الحقيقي. تحدد الورقة البحثية التحديات والقضايا المفتوحة ذات الأولية، والاتجاهات البحثية المستقبلية في إنترنت الأشياء.

الكلمات المفتاحية: انترنت الأشياء، IoT، المفاهيم المتقدمة في أنترنت الأشياء، معمارية انترنت الأشياء، تقنيات انترنت الأشياء، تطبيقات انترنت الأشياء.

1. Introduction

The Internet of Things (IoT) is a relatively new and well-recognized concept that is rapidly expanding. It specifies a dynamic ecosystem of networked smart computing devices with varied components that allow for smooth communication, data transfer, and processing [1]. Since its start in 1999, when Kevin Ashton invented the phrase "Internet of Things," it has progressed from a basic concept to one of the most essential commercial development drivers [2]. As illustrated in Figure 1, the Internet of Things is founded on the widespread use of wireless sensor networks (WSN), in addition to mobile computing (aka MobiCom), ubiquitous computing (UbiComp), and concepts of information technology. Sensors are increasingly being integrated into everyday objects due to the trend of shrinking size, decreasing price, and decreasing energy consumption. IoT represents a significant evolutionary step in a field that dates back to the mid-1980s. MobiComp and UbiComp are two distinct earlier stages in this evolution [3].

Citizens are, in fact, gradually equipping their smart homes with smart IoT devices such as heating systems, lighting systems, Internet boxes, smart TVs, home remote controls, and so on. The cooperation of robots and other smart tools in factories and industrial environments improves the efficiency of automation systems and allows for better production. The Internet of Things (IoT) is now widely used in a variety of other IoT devices that are being used more and more in a variety of fields, including smart cities, healthcare, the military, and agriculture. In certain situations, they are even being used as evidence in criminal cases. Data and records of IoT devices' interactions can be used for auditing. Fitbit data (for example, steps walked) was used to disprove the suspect's claims about the victim's movement before the crime [2].

https://doi.org/10.59222/ustjet.4.1.1

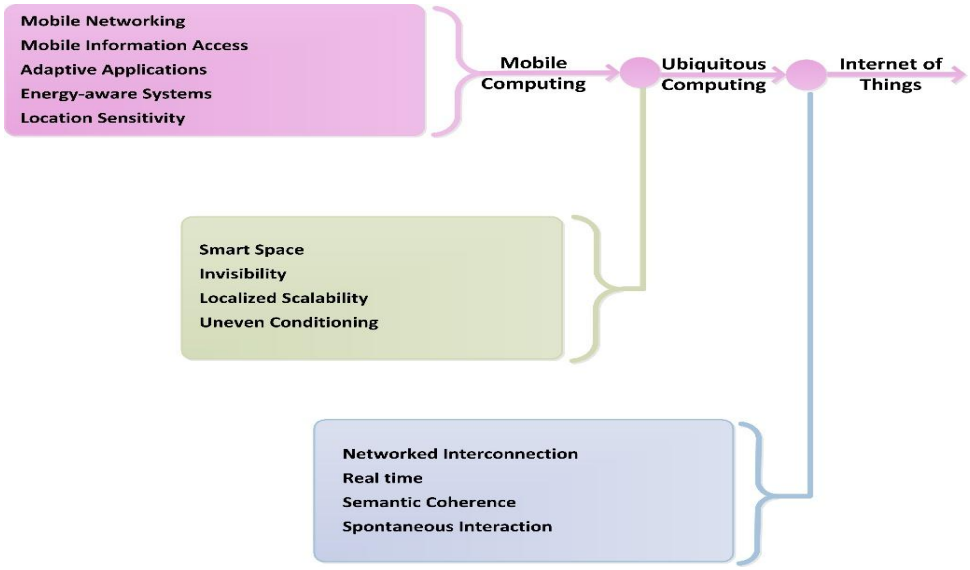


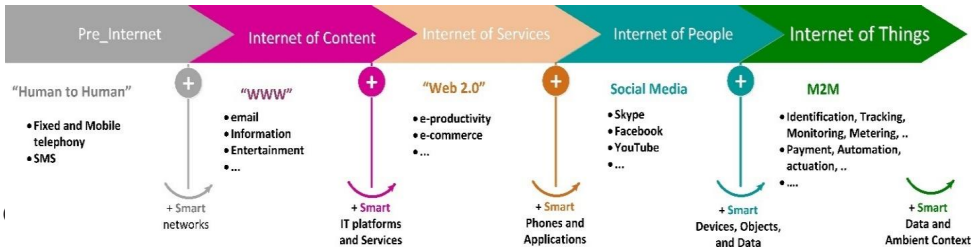
Figure 1. Relationships between Mobile Computing, Ubiquitous Computing, and IoT[3]

In 2018, it was approximated that there were approximately 7 billion IoT devices in the world [2]. It increased to 5 billion in 2019 and will be 29 billion in 2022 [4]. The National Intelligence Council and the McKinsey Global Institute estimate that by 2025, ubiquitous objects such as food packaging, furniture, and paper documents will be Internet nodes. By merging human-interaction technology, they illuminate the future to be constructed[5]. The authors of [6] predict that by 2025, there will be 50 billion IoT devices worldwide. Additionally, the 2020 IoT study from Business Insider predicts that the IoT industry would expand at a rate of over $2.4 trillion per year by 2027 [7]. This means that by 2027, there will be 41 billion IoT devices, up from 8 billion in 2019.

This paper aims to provide a general review of the IoT ecosystem. The paper discusses various IoT concepts, architectures, hardware including hardware and operating systems, as well as key application domains. This paper will assist readers and researchers in understanding the IoT and its application in the real world. The rest of the paper is organized in this manner. Section 2 recounts the history of the development of the Internet of Things. In Section 3, IoT architectures are discussed. In Section 4, the IoT components are described.

2. IoT Evolution

As seen in Figure 2, the term "Internet" developed through several stages before becoming the IoT. Communication during the initial phase, often known as the pre-Internet period, was confined to a short messaging service (SMS) and a telephone. Later, mobile telecommunication devices were introduced as a means of communication. The second phase, also called the Internet of Content, could send large messages such as e-mail with attachments. The basic possibilities for this phase included information, entertainment, and so on. The third phase, known as the Internet of Services, focuses on electronic applications such as e-commerce and e-productivity. The fourth phase, known as the Internet of individuals, allows individuals to connect and communicate with one another through social media platforms like Facebook, YouTube, Orkut, and Skype.



of Things. This feature enables various devices to interact with one another to carry out a range of guided tasks depending on their functional capabilities and design. Nonetheless, the present day could not be considered the concept's demise. As a result, an excessive number of researchers are trying to integrate the idea of artificial intelligence (AI) into these networked gadgets so that they can act independently and make the right judgments like smart devices. According to authors in [8], the upcoming phase may be referred to as "IoTAI" because it will be powered by Artificial Intelligence based on the IoT.

3. IoT Architecture

The Internet today uses the TCP/IP protocol layered stack invented long ago for communications among network hosts. IoT will connect everything and

https://doi.org/10.59222/ustjet.4.1.1

everyone to share data between them, including many types of connected devices and countless technologies. Architecture solutions will require integrating all these different devices and technologies into the systems [9], [10]. With the rapidly growing number of internet-connected devices, vast amounts of data are being generated that are beyond the capacity of the current infrastructure and architecture, thus demanding the implementation of an open architecture that is focused on service quality. It must be able to support current network applications using open protocols. IoT is not yet mainstream due to concerns regarding privacy and security that need to be addressed [11]. Security and data privacy are predominant issues in IoT [11]. Researchers have proposed a number of multi-layered architectures for supporting distributed and heterogeneous IoT needs.

3.1 The 3-Layer Architecture

During the early stages of the Internet of Things, the 3-Layer architecture was the standard. This is composed of the perception, network, and application layers. The perception layer consists of RFID tags, sensors, GPS, cameras, and other devices that are in charge of object identification and data acquisition. The network layer, which is the brain of the IoT, receives and processes information from the perception layer. Conversely, the network layer is based on the most recent Internet and mobile telecommunication infrastructure, and its main purpose is the transmission of data over long distances. The Internet, the wireless and wired communication networks, and other private networks come under the network layer. Cloud computing, platforms, expert systems, and numerous others are some of the many components that intelligently process and take into account enormous volumes of data. The application layer is an intermediary between the Internet of Things and its users, which may be humans, organizations, or other systems. IoT and professional industry technologies are connected [12] [13].

3.2 SOA-based Architecture

SOA, or service-oriented architecture, is one of the newest architectures. An architectural technique known as Service-Oriented Architecture (SOA) has gained popularity for enhancing the functionality of conventional systems while maintaining their key characteristics. Because of its versatility, the SOA method has piqued the interest of both academic and commercial groups, notably in the creation of world-leading technologies like cloud computing and IoT [14]. Service-Oriented Architecture (SOA) consists of five layers:

service composition, service management, object abstraction, objects, and applications. To develop IoT-based systems, SOA concepts have been used as a de facto software architecture. Though SOA provides numerous advantages, there are several challenges to integrating with IoT-based systems, including configurability, interoperability, and manageability [15].

3.3 The 5-Layer Architecture

Network stack-based architectures, such as the 3-layer model, have shortcomings that make them unsuitable for real-world IoT scenarios. On the Internet of Things platform, for instance, not all of the fundamental technologies utilized to transmit data are included in the network layer. Furthermore, only certain communication mediums, such as wireless sensor networks, are meant to work with these models. In contrast, in a SOA-based architecture, the device must devote substantial time and resources to interacting with other devices and integrating the required services via the service composition layer [16]. These issues were resolved using the 5-Layer design. To construct a five-layer architecture, the middleware and business layers are added to the three levels of the three-layer model. Data from the network layer is received by the middleware layer and stored in the database. It performs UbiCom, processes information, and makes decisions depending on the outcomes. IoT services and apps are part of the Business Layer, which controls the whole system. The business layer uses data from the application layer to generate business models, flowcharts, graphs, and other visual aids. Additionally, this layer will help discover and predict future company plans and activities based on the outcomes analyzed. Consequently, the five-layer design is the most often used for Internet of Things systems and their uses [9], [17].

3.4 European FP7 Research Project

The development of IoT architecture (IoT-A) is based on this. The European FP7 Research Project proposed the Architectural Reference Model (ARM). Based on current technology, application-specific needs, and commercial considerations, the IoT-A is advised [11].

https://doi.org/10.59222/ustjet.4.1.1

3.5 ITU Architecture

The proposed Internet of Things (IoT) architecture by the International Telecommunication Union (ITU) consists of five layers: application, middleware, network, access, and sensor. In computer networks and data transmission, these are similar to the Open Systems Interconnection (OSI) concept [11].

3.6 IoT Forum Architecture

They proposed three different types of IoT architecture. Processors, Applications, and Transport [11].

3.7 Qian Xiaocong, Zhang Jidong Architecture

They proposed a three-tiered Internet of Things architecture: perception, transport, and application. Similar to a three-layer design, the perception layer gathers information from devices. Similar to the network layer of the three-layer design, the transportation layer is in charge of giving carriers access to networks, including broadcasting, data, OFC, mobile, and fixed phone networks. The application layer manages smart homes, healthcare, remote nursing, patient monitoring, safety, defense, smart cars, smart traffic, smart agriculture, smart industries, and logistics. [11].

3.8 Kun Han, Dacheng Zhang, Shurong Liu & Ying Han's Architecture

They stated that SSME Development research was being conducted [11].

3.9 Distributed Internet-like Architecture for the IoT (DIAT)

The capabilities of the IoT infrastructure are divided into three levels. Object virtualization is handled by the Virtual Object Layer (VOL), service composition and execution by the Composite Virtual Object Layer (CVOL), and service creation and administration by the Service Layer (SL) [18].

3.10 Zhang, M., Sun, F., and Cheng, X. Architecture

In [12], the authors proposed a novel six-layer architecture, which has six layers: coding, information gathering, information access, network, information integration, and application service. Study in [19] conducted a development of a theoretical framework and conceptual model. The components of the previously stated architectures are compiled in Table 1.

Table 1: Components of various proposed IoT architecture models

IoT Architecture Model	Components
3-Layer Architecture	• Perception Layer • Network Layer • Application Layer
SOA-based architecture	• Objects • Object Abstraction • Service Management • Service Composition • Applications
5-Layer Architecture	• Perception Layer • Network Layer • Middleware Layer • Application Layer • Business Layer
IOT forum architecture	• Processors • Transportation • Applications
International Telecommunications Union (ITU) architecture	• Sensing layer • Access layer • Network layer • Middleware layer • Application layer
European FP7 research project	• Roots – Interoperable technologies • Trunk – Potentially necessary set of enablers or building blocks • Leaves – Enables the creation of a maximal set of interoperable IoT systems
Qian Xiaocong, Zhang Jidong architecture	• Perception layer • Transportation layer • Application layer
Kun Han, Shurong Liu, Dacheng Zhang, and Ying Han architecture	• Near field communication • Network equipment management • High-speed Internet
Distributed Internet-like Architecture for the IoT (DIAT)	• Virtual Object Layer (VOL) • Composite Virtual Object Layer (CVOL) • Service Layer (SL),

https://doi.org/10.59222/ustjet.4.1.1

Table 1: Continued

IoT Architecture Model	Components
Zhang, M., Sun, F. and Cheng, X.	• Coding layer • Information acquisition layer • Information access layer • Network layer • Information integration layer • Application service layer

4. IoT Component

IoT has many diverse components, which can be grouped into the following categories:

4.1 Hardware

The vast majority of the hardware that will power the Internet of Things already exists and is widely used. RFID, NFC, and sensor networks are the most important hardware infrastructure components [5][11]. They are also a part of IoT communication technologies, as shown in Figure 3.

4.1.1 Radio-Frequency Identification (RFID)

RFID is a technology that enables short-distance communication. It is one of the most essential features of embedded communication technology. RFID uses electromagnetic waves to detect and track tags linked to various devices. RFID tags hold device-specific data electronically.

Active tags may function hundreds of meters distant from an RFID reader and are powered locally. The energy from radio waves released by an RFID reader in the vicinity is used by passive tags. RFID tags do not need to be in the reader's line of sight. As a result, it can be embedded within a tracked device. RFID tracking object utility was developed and applied to supply chain management, retailing, logistics, aviation, food safety, security, e-health, and public utilities [5]. Vehicles are tracked down the assembly line using RFID tags that are affixed to them during manufacture. Pharmaceuticals with RFID tags are monitored via a repository. RFID tags allow for the tracking, counting, and identification of pets and animals. Contrariwise, RFID-tagged apparel at store guards against theft. RFID can be used to trigger a variety of events because it also serves as an actuator [11].

4.1.2 Electronic Product Code (EPC)

Auto ID Center created the first Electronic Product Code in 1999 at MIT. It's an RFID tag that stores a 64- or 98-bit code electronically. EPC codes provide the entire product specifications, such as the product's unique identity, serial number, year of production, manufacturer information, full technical and commercial specifications, and EPC type [11]. Items in RFID systems are recognized by their EPC. However, because the EPC code is only an item identifier, much like the barcode, it cannot be accessed by Internet addresses [5].

4.1.3 Barcode

A barcode is a specific means of presenting data in a machine-readable format. Barcodes represent data with parallel lines of varying lengths and spacing. To encode letters and integers, a variety of space and variable-width bar combinations can be used. In numerous ways, RFID outperforms barcodes. RFID does not require a direct line of sight. Because radio waves are used, the reader does not have to be physically there. A barcode requires a straight line of sight. Because it is an optical technology, the reader must be present to utilize it [11].

4.1.4 Near Field Communication

Near Field Communication (NFC) is a short-range wireless technique used for exchanging data at very small distances or device touching between two electronic devices. It is the most recent RFID-based technology that is standardized in ISO / IEC 18092. Electrical gadgets can communicate up to 10 cm distant thanks to NFC technology. It uses high-frequency bands up to 13.56 MHz and transmits data at 424 Kbit/sec. Furthermore, three transmission modes are supported by NFC: 1) When writing data into a smart poster, for example, Reader-Writer Mode enables an NFC device, like a smartphone, to read or write data in NFC tags. 2) Secure transactions, including cellular purchases, may be shown on smartphones thanks to Card Emulation Mode. 3) Similar to exchanging business cards, Peer-to-Peer Mode enables data transfer between two NFC devices when they are close [20].

4.1.5 Wireless Sensor Network

Wireless sensor networks are made up of semi-distributed, dedicated sensors that are spaced at equal intervals to monitor the environment. These sensors collect, record, and store data in a centralized server. Light, sound, motion,

https://doi.org/10.59222/ustjet.4.1.1

speed, temperature, humidity, pressure, pollution, vibration, and quantity are just a few of the environmental variables that WSN can track. Similar to wireless ad hoc networks, wireless sensor networks (WSNs) rely on wireless connections and instantaneous network construction to enable wireless data transmission. With a communication, sensing, actuation, and storage unit, every node in a WSN functions as a transceiver. In addition, each node serves as a power source that includes an antenna, microcontroller, interfacing circuit, memory, and battery [11].

WSN is composed of several sensing nodes that use multi-hop wireless technology to interact with one another. The outputs of sensor nodes' sensing are usually sent to a limited number of sinks, just one, because a sensor might perceive but not act. Actuators conduct actions that impact an item or its surroundings, whereas sensors determine the status of an object or its surroundings. Actuators can damage the environment by releasing radio waves, light, sound, or even stink. Sensor/actuators networks (SANETs), which are IoT SANET targets, are the result of the integration of sensors and actuators. These networks enable things to interact with humans while remaining aware of their environment [5].

4.2 Middleware

Communication protocols and IoT middleware are being developed to connect various devices and systems via the Internet [21]. A middleware layer, which stands between the operating system and applications, is an important software layer for concealing technical information. It serves as a layer of abstraction between applications and IT infrastructure. As a result, application developers will spend more time developing IoT apps [5]. This may be accomplished without the need to write separate code for different devices and data types. Middleware includes application servers, web servers, content management systems, and a variety of other technologies that help developers create and distribute applications. Middleware services include message-oriented middleware, object request brokers, data integration, enterprise application integration, and enterprise service buses. Middleware is used by developers to get around problems with wireless sensor networks. Developers can integrate many applications with hardware and operating systems by using middleware apps for wireless sensor networks [11].

Three types of IoT middleware have been implemented to enable IoT: cloud-based, actor-based, and service-oriented architecture (SOA). IoT-based SOA

employs a layered architecture [21]. The suggested middleware solutions vary significantly in terms of programming abstraction levels (local or node level, global or network level), design methodologies (event-based and database-based), and implementation domains (WSNs, RFID, M2M, and SCADA). [5]. To enable interoperability across various kinds that interact in various communication formats, the researchers suggested the use of semantic middleware. The capacity of computers to share information is known as semantic interoperability. It is necessary to have data federation, computational logic, knowledge discovery, inference, and synchronization across different information systems [11].

4.3 Operating Systems (OSs)

IoT devices' battery life and hardware capabilities are constrained. As a result, many gadgets cannot run mature operating systems that are widely used. IoT OS code has to be tuned for Transmission Control Protocol/Internet Protocol (TCP/IP) capabilities to facilitate simple communication with the global internet. Therefore, to manage resources across several communication levels, an IoT operating system needs to be extremely efficient. To create a platform that supports the newest protocols and standards for tomorrow's intelligent IoT, academics and practitioners must continuously improve IoT OS. It may be challenging to manage the heterogeneity of IoT devices, but IoT operating systems need to be able to handle a variety of hardware boards, devices, and architectures [22]. A de facto common operating system is necessary for resource-constrained IoT devices to meet the many applications and operational requirements of heterogeneous networks [5].

IoT operating systems are classified as either open source or closed source (packaged). Examples of open-source operating systems include uClinux, Android, Brillo, RIOT, FreeRTOS, TinyOS, OpenWSNnuttX, eCos, mbedOS, and the L4microkernel family. Whereas, ThreadX, QNX, VxWorks, Wind River Rocket, PikeOS, embOS, Nucleus RTOS, Sciopta, LiteOS Hawei, and others are examples of closed-source operating systems. Because IoT is a new field of study, there is no single dominant IoT operating system. There are few IoT professionals, and most developers, researchers, and businesses are still learning [5]. A complete IP networking stack comprising the industry-standard User Datagram Protocol (UDP), TCP, and Hypertext Transfer Protocol (HTTP) is offered by the majority of IoT operating systems. It also supports the latest standards, such as Constrained Application Protocol (CoAP), Routing over

https://doi.org/10.59222/ustjet.4.1.1

Low Power and Lossy Networks (ROLL), and Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN) [22]. Table 2 illustrates an overview of IoT OSs.

Table 2 lists the salient characteristics of many IoT operating systems that are often utilized by the research community. IoT OS support is crucial for widely deployed IoT-constrained devices. Table 3 lists the board architectures produced by several vendors, along with the IoT operating systems that support them [22].

Table 2: Overview of IoT OSs

IoT OS	Min RAM	Min ROM	C Support	C++ Support	Multi-Threading	Architecture	Scheduler
Tiny	<1 kB	<4 kB	No	No	Partial Support	Monolithic	Cooperative
Contiki	<2 kB	<30 kB	Partial Support	No	Partial Support	Monolithic	Cooperative, Preemptive
RIOT	~1.5 kB	~5 kB	Yes	Yes	Yes	Microkernel	Tickless, Preemptive, Priority based
Zephyr	~2 kB to ~8 kB	~50 kB	Yes	Yes	Yes	Nanokernel, Microkernel	Preemptive, Priority based
MbedOS	~5 kB	~15 kB	Yes	Yes	Yes	Monolithic	Preemptive
brillo	~32 MB	~128 MB	Yes	Yes	Yes	Monolithic	Completely Fair

5. Communication Technologies of IoT

Communication technologies are essential to the successful deployment of Internet of Things systems. In the modern world, the range of connectivity options available to apps is nearly overwhelming. They are predicated on products and systems that are linked to the Internet of Things. The primary IoT connectivity technologies are depicted in Figure 3, for instance [8]. Current communication technology can be divided into three categories: standards, spectrum, and application scenarios. There are two types of communication standards: long-range and short-range. The communication spectrum is divided into two categories: licensed spectrum and unlicensed spectrum.

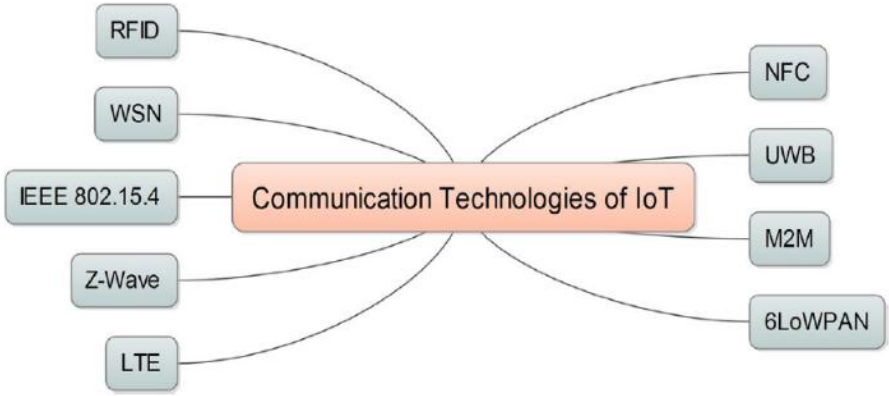


Figure 3: Communication technologies of IoT

Sensors, backhaul networks, and deployment scenarios can all be used in IoT device application scenarios. There are several different wireless communication standards in use today. They are divided into two groups: standards for both short- and long-distance communication. Near-field communications (NFC) devices, Bluetooth, ZigBee, Z-Wave, and passive and active radio frequency identification (RFID) systems are examples of short-range standards. Objects up to 100 meters away can be detected using short-range standards. Long-distance communication protocols can span tens of kilometers or more. Low-power wide-area (LPWA) communication technologies like Sigfox, LoRa, and NB-IoT are used in long-distance communication. The LPWA consumes less electricity and has a large coverage area [21]. Table 3 depicts a summary of the various communication technologies used for IoT communication.

Table 3: Communication technologies

Technology	Year of discovery	Standard	Downlink/ uplink	Range (in meters)	Operating frequency (in MHz)
RFID	1973	Wireless	100 kbps	2	0.125–5876
NFC	2004	ISO 18092	106, 212 or 424 Kbits	<0.2	13.56
Bluetooth	1994	Wireless	720 Kbps	10	2450
IEEE 802.15.4	2003	6loWPAN	250 Kbps	30	826, and 915
6loWPAN	2006	Wireless	250 Kbps	30	915

https://doi.org/10.59222/ustjet.4.1.1

Table 3: Continued

Technology	Year of discovery	Standard	Downlink/ uplink	Range (in meters)	Operating frequency (in MHz)
LTE	1991	3GPP, LTE, and 4G	100 Mbps	35	400–1900
Z-Wave	2013	Wireless	100 kbit/s	30	868.42, and 908.42
UBW	2002	IEEE 802.15.3	11–55 Mbps	10-30	2400
M2M	1973	Open for all communication protocols	50–150 Mbps	5-20	1-20
WSN	1970	Packet-based communication	1.37 Mbps	300	900

6. IoT Protocols

IoT devices usually possess a single or multiple network interfaces, as their primary function is to be Internet-connected. IoT utilizes a variety of low-power radio technologies such as IEEE 802.15.4 (ZigBee), Z-wave, Sigfox, Neul, Bluetooth Low Energy (BLE), and NB-IoT, in addition to traditional systems like Ethernet. There needs to be an open standard for providing seamless and efficient internet connectivity between those various wired and wireless technologies. IoT stacks must be scalable, dependable, internet-based, and configurable to respond to the requirements of heterogeneous IoT applications [5] [12]. To assist and simplify the work of service providers and application developers, several IoT standards have been proposed. The World Wide Web Consortium (W3C), the Internet Engineering Task Force (IETF), EPCglobal, the Institute of Electrical and Electronics Engineers (IEEE), and the European Telecommunications Standards Institute (ETSI) have all formed groups to develop Internet of Things protocols. Each application will have its own preferences, even though protocols compete to be the most widely used choice for connected objects. A functional prototype and a perfect solution are frequently separated at this point. For example, the wireless communication technology you choose must be precisely appropriate for its intended purpose. It is challenging to choose among wireless technologies because each one has its own set of benefits and drawbacks. As a result, new protocols with characteristics that meet the needs of connected objects, like low power consumption, low throughput, wide range, simplicity of implementation, and so forth, have emerged [34]. As shown in Table 4, our

analysis showed that nearly all protocols were grouped by the Internet of Things architecture's fundamental layer.

However, standardized procedures are not the end of the story. It serves as a springboard for further investigation into other unresolved issues that must be resolved to achieve global IoT. Numerous challenges remain unanswered, including those related to energy efficiency, sleeping nodes, scalability, security, interaction with cloud services, resource representation, integration with existing web service technologies and tools, interoperability with other wireless standards, semantics use, maintainability, and many more [5].

Table 4: IoT protocols in each layer

Category	Sub-Category	Protocols
Application Protocols	—	DDS, CoAP, AMQP, MQTT, MQTT-SN, XMPP, RESTFUL, WebSocket
Service discovery	—	mDNS, DNS-SD
Infrastructure Protocols	Network Layer Routing Protocols	RPL, P2P-RPL, CORPL, CARP, AODV, LOADng and AODv2
	Network Layer Encapsulation Protocols	6LoWPAN, IPv4/IPv6, 6TiSCH, ZigBee IP, IPv6 over G.9959, IPv6 Over Bluetooth Low Energy, IPv6 over NFC, IPv6 over MS/TP– (6LoBAC), IPv6 over DECT/ ULE, IPv6 over 802.11ah
	Data Link Layer Protocols	IEEE 802.15.4e (TSCH), IEEE 802.11 ah - wifiHallow, WirelessHART, Z-Wave, INGENU RPMA (IEEE 802.15.4k), Bluetooth Low Energy, Zigbee Smart Energy, DASH7, HomePlug, G.9959 (~Z-Wave), LTE-A, LoRaWAN, Weightless, DECT/ULE
	Communication technologies	Bluetooth - BLE, ZigBee, Z-Wave, 6LoWPAN, Wifi-ah (HaLow), LTE-A or eMTC (3GPP), EPCglobal, 2G(GSM),3G,4G, 5G (3GPP), Weightless-N/-W/-P, Tread, RFID, NFC, LoRaWAN, SigFox, Neul, Dash7, WirelessHART, EnOcean, DigiMesh, Ingenu, ANT & ANT+, NB-IoT (3GPP)
Influential Protocols	—	IEEE 1888.3, IPSec, IEEE 1905.1

7. IoT Applications

In terms of flexibility, the Internet of Things has considerable potential for social, environmental, and economic benefits. Some IoT-based concepts include mobility, smart buildings and houses, smart grid, environmental

https://doi.org/10.59222/ustjet.4.1.1

and public safety monitoring, industrial processing, healthcare and medicine, agriculture and breeding, and independent living [19]. All of these applications involve us in some way. These programs' availability is now heavily reliant on their usage, which is critical given their numerous benefits. Their presence and utility have just reached a crucial level. It is not erroneous to state that the Internet's future is dependent on the concept and vision of IoT, which essentially drives us into the future [8]. Figure 4 represents a range of IoT application areas that will be described in the next subsections.

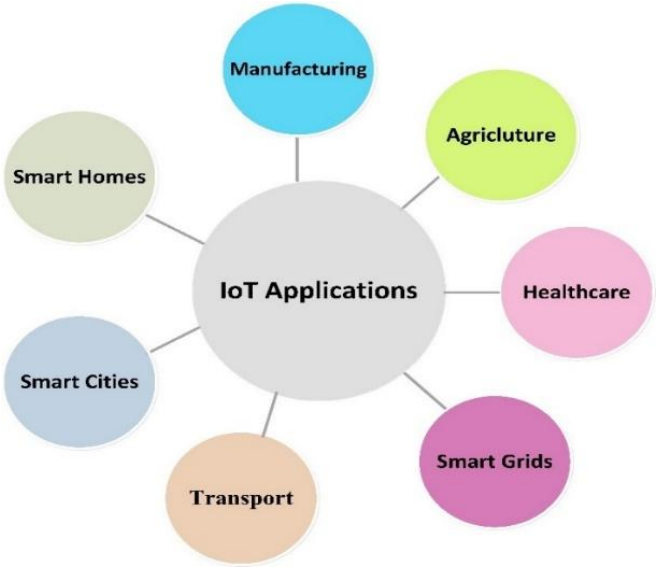


Figure 4: IoT applications

7.1 Smart Home/Building

A Smart Home or Building is a living environment with lighting, heating, and other electronic devices, just like any other living environment. The ability to control them remotely from a smartphone or computer makes a significant difference. The concept of smart homes/buildings has emerged as a result of connecting various devices to the Internet in recent years [8].

7.2 Smart Cities

Smart cities are one of the most significant IoT applications, since they strive to optimize the utilization of public resources and the quality of services given to inhabitants. In this context, sensors are embedded throughout buildings, roads, smart vehicles, and other structures to better traffic management,

weather adaptability, sun-following lighting, household issues that may be averted with alerts, and so on [24]. IoT technology may be used to track anything in a given region. Sensors can be integrated into residences, urban infrastructure, transportation, power networks, and services. This will help support a smart city that is built on continuous sensor data monitoring. For example, by tracking automobiles using IoT, street lighting may be controlled to conserve electricity [38][42][46].

7.3 Intelligent Transportation Systems (ITS)

ITS are the transportation systems of the future, to integrate people, roads, and intelligent cars via advancing embedded and communication technology. For instance, by linking and distributing intelligent processors across the infrastructure and within automobiles, we can increase the safety, environmental friendliness, and convenience of transportation. The four main parts of ITS are the ITS monitoring center, the station subsystem (roadside equipment), the vehicle subsystem (which includes GPS, RFID reader, OBU, and communication), and the security subsystem. To improve driving efficiency, safety, and enjoyment, connected cars are becoming increasingly important. Vehicular wireless networks provide three forms of communication: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-person (V2P), also known as vehicle-to-pedestrian. But recently, a new communication technique known as V2G (car-to-grid) has emerged, with the primary purpose of supplying electric vehicle charging via smart grid power distribution [27]. To improve present technology, several scholars have addressed a wide range of issues about traffic and traveling from one location to another [8][41].

7.4 Smart Grid

An electrical distribution network that uses digital communication technology to track and react to variations in local demand is known as a "smart grid". It is frequently referred to as a digital technology that permits two-way communication, which means that after sensor observations, users may submit their electrical requests and vice versa. The grid distributes power based on demand estimates. The distribution network is powered by smart grid technologies [8]. To coordinate power output in response to end-user demand, energy production centers and end users are connected via an integrated network, sometimes referred to as advanced metering infrastructure (AMI). This network is the cornerstone for a smart grid. The primary goal is to

https://doi.org/10.59222/ustjet.4.1.1

maximize energy production and improve the overall quality of the customer experience [24]. Additionally, it will significantly reduce the demand for unnecessary rubbish. In addition, IoT may be used to monitor specific islands or organizations in various microgrids, particularly in databases and other areas where energy is constantly required. Both grid-related properties are linked in these networks [38].

7.5 Healthcare

The development of the healthcare sector has been greatly impacted by the Internet of Things (IoT), which has led to a greater effort to create platforms at the hardware and underlying software layers [23]. In the medical field, the Internet of Things (IoT) is utilized to track the physiological conditions of patients. Direct data collection from the patient's body may be sent to the doctor via the integrated sensors. With this technology, the patient may be in constant communication with the doctor even if they are cut off from the hospital's centralized system. Due to the aging of the population, IoT applications centered around healthcare are currently among the most promising technologies that have a big influence on society [24] [25].

7.5.1 IoT Applications for Elderly Care

Global healthcare systems are under more pressure from the aging population in terms of operating expenses, and the Internet of Things (IoT) and wearable technologies have the potential to lower stress levels and raise the standard of medical treatment. In addition to lessening the strain on healthcare systems and operational costs, these technologies have the potential to enhance the quality of life for senior citizens. From 8.5 percent in 2015 to 12 percent in 2030 and 16.7 percent by 2050, the percentage of the world's population that is elderly is predicted to increase [26]. This group frequently needs additional medical resources, such as medicine, nurses, or physicians, particularly if they wish to maintain their independence. The increase in the elderly population and their medical needs has presented several new issues to the healthcare system, including growing healthcare expenses and the incidence of chronic diseases. Financial and human resource constraints may limit older people's access to high-quality healthcare services. People can use wearable devices, which are Internet of Things systems, to monitor their physiological data and physical activities. Because they contain sensors and analytical algorithms, these devices can monitor, assess, and steer their users' behavior, movement, or vital signs [26] [25].

7.5.2 Using IoT in COVID-19

The most significant worldwide public health emergency since the 1918 influenza pandemic is the present possibility of a pandemic brought on by a new coronavirus that causes severe respiratory illness. Several ongoing initiatives and studies are being carried out to prevent the virus's spread. In this regard, it has been demonstrated that IoT technology offers a secure and efficient way to fight the COVID-19 epidemic. Numerous research groups have been working quickly since the pandemic's start to use a variety of technologies to counteract this worldwide threat, with IoT technology leading the way in this area. In the instance of COVID-19, early diagnosis, patient monitoring, and adherence to established guidelines after patient recovery are utilized to minimize the possible transmission of COVID-19 to others using IoT-enabled/linked devices/applications [27]. IoT can help predict future cases of this disease by using a statistical method. The internet-based network makes it easy to monitor all high-risk individuals. This approach measures biometrics such as blood pressure, heart rate, and glucose levels. If this technology is used properly, researchers, clinicians, governments, and academics may work together to enhance the environment for battling this sickness [28] [25].

7.6 IoT Applications in Agriculture

The use of IoT in agriculture has received a lot of interest from the scientific community [29]. Giving farmers automation and decision-making tools that seamlessly integrate products, information, and services is the aim of IoT use in agriculture to increase productivity, quality, and profitability [21]. Even while Asian scientists make up the majority of the articles, several large-scale international pilot projects, such as IoF2020, AIOTI, SmartAgriFood, SMART AKIS, and, more recently, SmartAgriHubs, try to implement comparable IoT technology in the European agricultural industry. Furthermore, a similar program called Australia's Accelerating Precision Agriculture to Decision Agriculture (P2D) supports additional major investments to assist farmers in the transition to smart farming [29].

Precision IoT approaches for precision agronomy in smart cities are part of precision agriculture, and one of the main uses of IoT technology in agriculture is urban agriculture. Other IoT applications include agricultural drones, which are reasonably priced drones equipped with advanced sensors that provide farmers with creative ways to lower crop damage and boost yields,

https://doi.org/10.59222/ustjet.4.1.1

and intelligent greenhouses, which include hydroponic and small-scale aquaponic systems. Furthermore, another use of IoT technology is vertical agriculture, which enables the management of soil moisture and water content using computers or mobile devices like smartphones and tablets. Last but not least, certain applications integrate IoT and AI. One example is Malthouse, an AI system that enables the prescription of schedules and settings in precision farming and food processing [30].

7.7 Manufacturing

In recent years, technological advancements, innovations, and breakthroughs have brought about significant changes to the global industrial environment. Industry 4.0, the fourth industrial revolution, aims to employ advanced technology to transform conventional industries into intelligent ones. Smart factories and intelligent production environments are the outcome of Industry 4.0's ability to integrate physical assets into networked digital and physical processes. The deployment of Industry 4.0 has benefited immensely from the rapidly developing Internet of Things (IoT) [31]. Industry 4.0 is a combination of the Internet of Things (IoT) paradigm and the idea of Cyber-Physical Systems (CPSs). CPSs connect physical items in the actual world and provide digital descriptions of them. This data, which is kept in data objects and real-time-updatable models, provides the item a second identity and serves as its "digital twin." The dynamic nature of these digital twins makes it possible to apply services that were previously unimaginable across the whole product lifespan, from production to disposal [32][45].

One promising technology for supply chain management and industrial process automation is Industrial IoT (IIoT) [45]. The IIoT uses cutting-edge technologies like WSN, automation, big data, and machine-to-machine (M2M) communication to create an intelligent industrial environment. Increasing production, efficiency, reliability, and product control is the main goal of IIoT [24]. Industry 4.0 and IoT have the potential to offer a vast array of contemporary solutions, applications, and services, despite their infancy in terms of development, acceptance, and deployment. Consequently, they have the potential to provide significant personal, professional, and economic opportunities and benefits shortly, as well as to improve the quality of life [31][45].

8. IoT Open Issues, Challenges, and Future Research Directions Numerous

Numerous obstacles must be overcome to realize the IoT vision. These issues are also a challenge for IoT developers in today's advanced smart tech society. The challenges and demand for advanced IoT systems grow in lockstep with technological advancement. As a result, IoT developers must anticipate and address new problems [35]. Figure 5 depicts the current state of open issues and challenges in IoT. In the following subsections, this section investigates the priority IoT challenges, open issues, and future research directions.

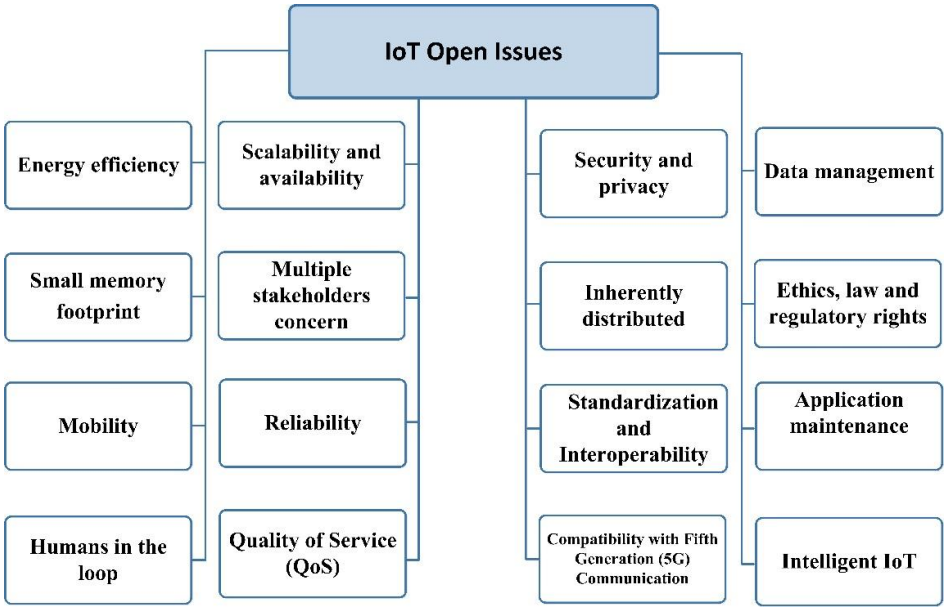


Figure 5: Open Issues of IoT

8.1 Energy Efficiency

Energy efficiency is a very important aspect of the Internet of Things. Resources are scarce for the vast majority of IoT devices. It thus has to run on a battery or other restricted sources of energy. IoT deployment locations are of a vast range and are challenging, even in quite remote locations. Because the Internet of Things network is so massive, IoT operating systems have to be power-efficient such that IoT devices will keep working for years. An IoT technology known as Radio Duty Cycling (RDC) is employed to improve power efficiency. In addition to the RDC, efficient methods are needed for obtaining precise mote synchronization[22] [40].

https://doi.org/10.59222/ustjet.4.1.1

8.2 Small Memory Footprint

A complete TCP/IP stack and low memory footprints of an IoT OS that can run on highly constrained devices are required to achieve seamless interoperability with the ubiquitous internet. Low memory optimization of modules is not difficult, and functionality will remain intact. It requires designers and developers to abide by coding rules that provide high configurability and modularity [22].

8.3 Mobility

Another barrier to successful IoT implementation is mobility, as the majority of applications are based on a mobile interface. Because data mobility necessitates connectivity. As a result, a failure in connectivity among non-stationary devices is frequently interpreted as IoT incapability due to the inability to transfer data from the source to the destination [8][40][42][46].

8.4 Humans in the Loop

IoT applications that replicate human behavior are a huge challenge since they have to replicate the intricate behavioral, psychological, and physiological traits of humans. To understand the intricate interdependencies and intrinsic needs between humans and IoT applications, new research has to be formulated in an effort to incorporate human behaviors into IoT application development. Human-object dependencies and interactions have not yet been aligned, though. Humans-in-the-loop have an enormous advantage: integration of models for various human activities and assistive technologies within the home of elderly citizens, say, can cure their ailments. [36].

8.5 Scalability and Availability

If new devices, equipment, and services can be added to a system without affecting its performance, it is scalable. Managing an extremely large number of devices with different memory, processing capacity, storage capacity, and bandwidth is the greatest challenge in IoT. Another significantly important aspect to take into account is accessibility. Scalability and availability need to be addressed together in the IoT layered architecture [40][42]. As they offer sufficient support to expand the IoT network by adding more devices, processing power, and storage as required, cloud-based IoT solutions offer an excellent example of scalability. The establishment of an unbroken IoT system that serves global demands, nevertheless, is achievable because

of this global distributed IoT network. Another significant challenge is the accessibility of resources for actual artifacts, irrespective of their location or when they were utilized. In order to utilize their resources and services, most small IoT networks are loosely connected with global IoT platforms. Supply is therefore a significant problem. Availability of certain services and resources may be affected as a consequence of utilizing various means of data transmission, e.g., satellite communication. Therefore, a reliable and independent medium of data conveyance needs to be established to make the resources and services perpetually available [35][46].

8.6 Multiple Stakeholders' Concerns

IoT application creation involves an enormous number of stakeholders with various concerns and expectations. Patel and Cassouc recognized domain experts, software designers, application developers, device developers, and network managers as significant stakeholders in IoT application development. These stakeholders must address concerns related to the many phases of an IoT application's life cycle, including design, implementation, deployment, and evolution. The lack of processes for handling the myriad stakeholders' concerns, and the particular experience and proficiency required by stakeholders to find components and comprehend the system, all contribute to the challenges of IoT application development. [36].

8.7 Reliability

The overall objective of enhanced reliability is to enhance the success ratio of IoT services by enhancing their data transmission capability. It becomes the deciding factor. A set of checksums will therefore be implemented throughout the hardware and software of the IoT infrastructure. Keeping the infrastructure robust against system failure and the threat of intrusion is one of the biggest challenges in IoT [8].

8.8 Quality of Service (QoS)

Because IoT applications are being integrated into our daily lives increasingly and are used sometimes in emergency conditions with no or negligible tolerance to faults and errors, the quality of the entire system is very crucial and must be evaluated very thoroughly before it is released to guarantee that the system is of quality [36][42]. Quality of service (QoS) is a quantification that evaluates the reliability, efficiency, and performance of IoT devices, systems, and architecture. Reliability, cost, energy efficiency, security,

https://doi.org/10.59222/ustjet.4.1.1

availability, and service time are core QoS needs of IoT systems. An intelligent IoT system should meet the demands of the QoS standards. Furthermore, QoS parameters of any IoT service or device must be defined beforehand to ensure its reliability. Moreover, maybe users can define their demands and requirements [35]. There are different approaches to QoS assessment; however, according to White et al., there is a trade-off between quality parameters and approaches. To counter this trade-off, high-quality models must be implemented. Some of the high-quality models, including OASIS-WSQM and ISO/IEC25010, may be utilized for analyzing the methodologies that have been used for QoS. These models provide a wide range of quality factors that are more than adequate for assessing QoS for IoT services [35]. However, evaluating quality attributes such as performance is a significant challenge because it is dependent on the performance of many components as well as the underlying technologies [36][46].

8.9 Security and Privacy

Two of the most important and formidable challenges in IoT are security and privacy, due to a variety of threats, cyberattacks, risks, and vulnerabilities. Inadequate authentication and authorization, poor firmware, software, and web interfaces, and poor transport layer encryption are a few of the reasons for device-level privacy issues. Security and privacy are key determinants in building trust in IoT systems in a variety of ways [35]. Health care, intelligent homes, intelligent cities, and other critical systems require high privacy and security. Data integrity, authentication, and access processes remain an issue [22][25][39].

By shifting from fingerprint sensors to face recognition, an embedded Internet with face recognition can minimize the coronavirus pandemic issue. Micro-segmentation approaches are employed to address security issues. IoT is a great future outlook that makes systems reactive with high efficiency, flexible with custom-made capabilities, and low in cost [40]. To prevent security threats and attacks, security mechanisms must be embedded at every layer of IoT architecture. To ensure the security and privacy of IoT-based systems, several protocols have been developed and efficiently deployed on every layer of the communication channel. Secure Socket Layer (SSL) and Datagram Transport Layer Security (DTLS) are cryptographic protocols that are used between the transport and application layers to provide security in various IoT systems. Some IoT applications, however, need the application

of various technologies to secure communication among IoT devices. Also, if wireless technologies are used in communication within the IoT system, the system is exposed to security attacks. Hence, some methods need to be incorporated in order to detect malicious activity as well as self-healing or recovery. Privacy, nonetheless, is a critical issue allowing users to feel safe and relaxed when using IoT solutions. Thus, authentication and authorization must be maintained in a secure network to facilitate communication among trusted parties [35]. A blockchain optimal solution is among the most promising solutions to solve security and privacy in the Internet of Things. In addition, the network solutions implemented need to be regularly examined to find and solve issues. For utmost network security, rapid development, deployment, testing, and adjustment to newly established security standards need to be made [22][39]. Blockchain is a promising technology that will be widely utilized to protect data in a variety of IoT applications, including healthcare [25], transportation [45], UAV [42][46], 6G [44], industrial IoT [45], and many others [25][42].

8.10 Inherently Distributed

IoT applications are typically distributed over a number of constituent systems. The majority of the IoT application components will be distributed via fog or cloud. Those parts of the application that enable end users to interact with the IoT system are usually developed independently, e.g., a web, mobile, or desktop application, even if the IoT device gathers data and performs real-time analytics. In addition, IoT applications may be dispersed over a wide range of geographical areas. The conventional approach to handling all of these software components with centralized development processes can be outdated due to their distributed nature. Moreover, developing and deploying distributed applications with the capacity to make reliable decisions based on non-centralized resources is not necessarily easy [36]. Blockchain technology is one of the promising technologies for designing and implementing distributed applications.

8.11 Standardization and Interoperability

Interoperability refers to the ability of different IoT devices and systems to communicate information. It does not matter which hardware or software is being used; the transmission of data is not impacted. Interoperability is an issue because there is a wide variety of technologies and solutions being implemented in the creation of IoT [35]. Standards and protocols to help

https://doi.org/10.59222/ustjet.4.1.1

enable communication between billions of IoT devices have not yet been created. Technical, syntactic, semantic, and organizational terminology must be compatible. Technical interoperability refers to the creation of infrastructure and protocols to facilitate communication between IoT devices. It is usually associated with the hardware and software components of the Internet of Things ecosystem. Data formats addressing syntactical interoperability include JavaScript Object Notation (JSON), Extensible Markup Language (XML), comma-separated variables, and electronic data interchange as a standard syntax for data exchange [5]. Semantic interoperability addresses how to understand information shared by people. Interoperability of an organization is the ability to communicate and share information effectively over different infrastructures, geographic locations, and cultural norms. All systems thus have to have export capabilities or API access, which returns standard formats (usually XML and JSON), and legacy systems must, if possible, have the right exchange gateways [21]. As interoperability is so important, many interoperability management systems have been proposed by researchers.

These solutions can be implemented with virtual networks/overlays, adapters/gateways, service-oriented architectures, and other forms of technologies. While interoperability management solutions mitigate the burden on IoT systems to some extent, there exist some interoperability challenges that could be addressed in future research [35].In order to facilitate interoperability among billions of IoT devices and services, more efforts will be made to advance open standards [21].

8.12 Compatibility with Fifth & Sixth Generations (5G & 6G) Communication

Despite the fact that the high-speed communication system is rapidly evolving, major innovations are frequently stymied by some of the most frequently encountered issues in 5G and 6G communication techniques for IoT-based implementations. Enabling physical layer modulation techniques, some of the most prevalent problems are the timely processing of different inputs and outputs, and error control code. Although several IoT projects have been initiated. Some elements of the Internet of Things need to be developed further. A steady increase in interest from varied academia, industries, and other concerned organizations pertaining to or representing directly or indirectly the arena of IoT keeps generating expectations with resultant perpetuation of

issues in most cases, unable to fulfill even the basic demands and functional capabilities of IoT.[8][44].Information-Centric Networking (ICN) for D2D IoT Communication employing NDN instead of IP communication is a topic of potential in the future, and replacing IP with content remains an issue [37] [41].

8.13 Data Management

IoT heterogeneous devices tend to generate a large amount of data in varying formats and velocities. Big data and IoT are inseparable because of the massive amounts of unstructured data that are created by IoT devices. Big data processing, storage, and analysis are thus crucial in coming up with meaningful reports that can be used in decision-making. This can substitute hypothesis-driven research for data-driven research. New data analysis techniques that are efficient and precise will be required in the future to come up with new solutions [22][42]. IoT applications collect and analyze data, which is usually used in making crucial decisions. Numerous reasons, including sensor failure, deliberate entry of incorrect data by users, timing delays in data delivery, and incorrect data format, can render the data imperfect. As a result, IoT application developers must devise methods for detecting the presence of invalid data, as well as novel techniques for capturing the relationship between the data collected and the decision to be made [36][46].

8.14 Ethics, Law, and Regulatory Rights

With the growth of IoT, various practical issues have been solved, but at the same time, created tremendous moral and legal issues. Some of the challenges include the security of data, the protection of privacy, safety, and trust, and usability of data. The majority of consumers of IoT support government regulations and laws on data protection, privacy, and safety, as they lack trust in IoT devices. Therefore, this issue must be addressed in such a way that the faith of the public in IoT systems and devices is upheld and enhanced. There are rules and regulations that guarantee that moral standards and values are adhered to and that no law is broken. Laws are limitations that are imposed by the government, but ethics are what people abide by. That is the only difference between the two. Laws and ethics, however, seek to discourage people from acting unlawfully and to establish standards and quality [35].

https://doi.org/10.59222/ustjet.4.1.1

8.15 Application Maintenance

Massive distributed networks with huge devices that interact in complex and affluent ways will power IoT applications. There is concern regarding the likelihood of deploying applications that offer adaptive and corrective maintenance because IoT applications will be dispersed across a vast geography. The software on the devices will be in a continuous need to be updated and debugged. On the other hand, there are some problems that arise during maintenance activities. There is a significant privacy and security threat in remote debugging and program upgrades for devices. Also, interactive debugging could be challenging because of these devices' limited bandwidth [36].

8.16 Intelligent IoT

Sophisticated IoT (I-IoT) will play a central role in the widespread use of IoT in everyday life. Researchers have only recently begun to study and apply smart artificial intelligence (AI) in IoT. Machine learning (ML) has been brought to the center stage in research in neural networks and image processing. Its potential and application in IoT are yet to be tapped. Machine learning (ML) algorithms need to be reformulated to be applied to IoT-constrained devices [22].

9. Conclusions

The Internet of Things (IoT) links multiple devices from anywhere, resulting in a network of diverse gadgets. Internet of Things devices include computers, smartphones, household appliances, industrial systems, e-health devices, surveillance equipment, and sensors for precision agriculture. This article investigated recent advances, architectures, components (hardware, middleware, and OSs), communication technologies, protocols, and applications, assisting readers and researchers in understanding the core advances of IoT and their recent applications. Furthermore, the paper identified IoT priority challenges and open issues, providing a guide for those leading IoT initiatives and revealing opportunities for future IoT research. Future work of this paper will address the rest of the topics and issues of IoT, such as security, privacy, energy, enabling technologies, data storage, and analysis. IoT confronts increasingly difficult challenges as a result of its complex environment and resource-constrained devices.

References

[1] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[2] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, Nov. 2021, doi: 10.1109/ACCESS.2021.3129697.

[3] "Searching in Internet of Things: Vision and Challenges - IEEE Conference Publication." https://ieeexplore.ieee.org/abstract/document/5951906 (accessed Oct. 18, 2018).

[4] K. Barboutov et al., "Ericsson Mobility Report," Jun. 2017. [Online]. Available: https://www.ericsson.com/49de56/assets/local/reports-papers/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf

[5] E. A. Shammar and A. T. Zahary, "The Internet of Things (IoT): a survey of techniques, operating systems, and trends," *Library Hi Tech*, vol. 38, no. 1, pp. 5–66, Jan. 2019, doi: 10.1108/LHT-12-2018-0200.

[6] S. Dange and M. Chatterjee, "IoT Botnet: The Largest Threat to the IoT Network," in *Data Communication and Networks*, vol. 1049, Singapore: Springer, 2020, pp. 137–157. [Online]. Available: https://doi.org/10.1007/978-981-15-0132-6_10

[7] Rasheed Ahmad, Izzat Alsmadi, "Machine learning approaches to IoT security: A systematic literature review," *Internet of Things*, vol. 14, p. 100365, Jun. 2021, doi: 10.1016/j.iot.2021.100365.

[8] A. Khanna and S. Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review," *Wireless Pers Commun*, vol. 114, no. 2, pp. 1687–1762, Sep. 2020, doi: 10.1007/s11277-020-07446-4.

[9] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT)*, 2012 10th International Conference on, 2012, pp. 257–260.

[10] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[11] P. Goyal, A. K. Sahoo, and T. K. Sharma, "Internet of things: Architecture and enabling technologies," *Materials Today: Proceedings*, vol. 34, pp. 719–735, Jan. 2021, doi: 10.1016/j.matpr.2020.04.678.

https://doi.org/10.59222/ustjet.4.1.1

[12] M. Zhang, F. Sun, and X. Cheng, "Architecture of Internet of Things and its key technology integration based on RFID", in *Computational Intelligence and Design (ISCID)*, 2012 Fifth International Symposium on, 2012, vol. 1, pp. 294–297.

[13] Z. Yang, Y. Yue, Y. Yang, Y. Peng, X. Wang, and W. Liu, "Study and application on the architecture and key technologies for IOT," in *Multimedia Technology (ICMT)*, 2011 International Conference on, 2011, pp. 747–751.

[14] N. Niknejad, W. Ismail, I. Ghani, B. Nazari, M. Bahari, and A. R. B. C. Hussin, "Understanding Service-Oriented Architecture (SOA): A systematic literature review and directions for further investigation," *Information Systems*, vol. 91, p. 101491, Jul. 2020, doi: 10.1016/j.is.2020.101491.

[15] S. K. Mishra and A. Sarkar, "Service-oriented architecture for Internet of Things: A semantic approach," *Journal of King Saud University - Computer and Information Sciences*, Oct. 2021, doi: 10.1016/j.jksuci.2021.09.024.

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[17] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved," in *Applied Sciences and Technology (IBCAST),* 2014 11th International Bhurban Conference on, 2014, pp. 414–419.

[18] C. Sarkar, S. A. U. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *Internet of Things (WF-IoT*), 2014 IEEE World Forum on, 2014, pp. 508–513.

[19] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," *Expert Systems with Applications*, vol. 133, pp. 97–108, Nov. 2019, doi: 10.1016/j.eswa.2019.05.014.

[20] M. L. Hamzah, Y. Desnelita, A. A. Purwati, E. Rusilawati, R. Kasman, and F. Rizal, "A review of near field communication technology in several areas," *Revista ESPACIOS*, vol. 40, no. 32, Sep. 2019, Accessed: Mar. 23, 2022. [Online]. Available: *http://www.revistaespacios.com/a19v40n32/19403219.html*

[21] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758–3773, Oct. 2018, doi: 10.1109/JIOT.2018.2844296.

[22] Y. B. Zikria, S. W. Kim, O. Hahm, M. K. Afzal, and M. Y. Aalsalem, "Internet of Things (IoT) Operating Systems Management: Opportunities, Challenges, and Solution," *Sensors*, vol. 19, no. 8, Art. no. 8, Jan. 2019, doi: 10.3390/s19081793.

[23] I. Alam et al., "A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV," *ACM Comput.* Surv., vol. 53, no. 2, p. 35:1-35:40, Apr. 2020, doi: 10.1145/3379444.

[24] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The Future of Healthcare Internet of Things: A Survey of Emerging Technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020, doi: 10.1109/COMST.2020.2973314.

[25] W. A. N. A. Al-Nbhany, A. T. Zahary and A. A. Al-Shargabi, Blockchain-IoT Healthcare Applications and Trends: A Review, in *IEEE Access*, vol. 12, pp. 4178-4212, 2024, doi: 10.1109/ACCESS.2023.3349187.

[26] M. A. M. Sadeeq and S. Zeebaree, "Energy Management for Internet of Things via Distributed Systems," *Journal of Applied Science and Technology Trends*, vol. 2, no. 02, Art. no. 02, Apr. 2021, doi: 10.38094/jastt20285.

[27] T. Syy, M. S, and M. F, "Internet of things (IoT) applications for elderly care: a reflective review," *Aging clinical and experimental research*, vol. 33, no. 4, Apr. 2021, doi: 10.1007/s40520-020-01545-9.

[28] M. Nasajpour, S. Pouriyeh, R. M. Parizi, M. Dorodchi, M. Valero, and H. R. Arabnia, "Internet of Things for Current COVID-19 and Future Pandemics: an Exploratory Study," *J Healthc Inform Res*, vol. 4, no. 4, pp. 325–364, Dec. 2020, doi: 10.1007/s41666-020-00080-6.

[29] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, "Internet of things (IoT) applications to fight against COVID-19 pandemic," *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, vol. 14, no. 4, pp. 521–524, Jul. 2020, doi: 10.1016/j.dsx.2020.04.041.

[30] A. Villa-Henriksen, G. T. C. Edwards, L. A. Pesonen, O. Green, and C. A. G. Sørensen, "Internet of Things in arable farming: Implementation, applications, challenges and potential," *Biosystems Engineering*, vol. 191, pp. 60–84, Mar. 2020, doi: 10.1016/j.biosystemseng.2019.12.013.

[31] R. Gómez-Chabla, K. Real-Avilés, C. Morán, P. Grijalva, and T. Recalde, "IoT Applications in Agriculture: A Systematic Literature Review," in *ICT for Agriculture and Environment*, Cham, 2019, pp. 68–76. doi: 10.1007/978-3-030-10728-4_8.

[32] G. Lampropoulos, K. Siakas, and T. Anastasiadis, "Internet of Things In The Context Of Industry 4.0: An Overview," *International Journal of Entrepreneurial Knowledge*, vol. 7, no. 1, pp. 4–19, 2019.

https://doi.org/10.59222/ustjet.4.1.1

[33] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[34] S. Elhadi, A. Marzak, N. Sael, and S. Merzouk, "Comparative study of IoT protocols," *Smart Application and Data Analysis for Smart Cities (SADASC'18)*, 2018.

[35] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 1, p. 111, 2019, doi: 10.1186/s40537-019-0268-2.

[36] I. S. Udoh and G. Kotonya, "Developing IoT applications: challenges and frameworks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 2, pp. 65–72, Jun. 2018, doi: 10.1049/iet-cps.2017.0068.

[37] MN Ali, AT Zahary, MA Areqi, IP and ICN Networking in D2D_IoT Communications: A Comparative Study, *Sana'a University Journal of Applied Sciences and Technology*, Vol. 2 No. 2 (2024), https://doi.org/10.59628/jast.v2i2.940.

[38] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Computer Networks*, vol. 141, p. 199, Mar. 2018, doi: 10.1016/j.comnet.2018.03.012.

[39] EA Shammar, AT Zahary, AA Al-Shargabi, An attribute–based access control model for Internet of Things using hyperledger fabric blockchain, Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/6926408.

[40] Nagajayanthi, B. Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective. Wireless Pers Commun 123, 3661–3697 (2022). https://doi.org/10.1007/s11277-021-09308-z

[41] M. A. Areqi, A. T. Zahary and M. N. Ali, "State-of-the-Art Device-to-Device Communication Solutions," in *IEEE Access*, vol. 11, pp. 46734-46764, 2023, doi: 10.1109/ACCESS.2023.3275915.

[42] A. A. Baktayan, A. Thabit Zahary and I. Ahmed Al-Baltah, "A Systematic Mapping Study of UAV-Enabled Mobile Edge Computing for Task Offloading," in *IEEE Access*, vol. 12, pp. 101936-101970, 2024, doi: 10.1109/ACCESS.2024.3431922.

[43] Leonardo B. Furstenau, Yan Pablo Reckziegel Rodrigues, Michele Kremer Sott, Pedro Leivas, Michael S. Dohan, José Ricardo López-Robles, Manuel J. Cobo, Nicola Luigi Bragazzi, Kim-Kwang Raymond Choo, Internet of Things: Conceptual network structure, main challenges and future directions, Digital Communications and Networks, Volume 9, Issue 3, 2023, Pages 677-687, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2022.04.027.

[44]Al-Matari, N.Y., Zahary, A.T. & A. Al-Shargabi, A. A survey on advancements in blockchain-enabled spectrum access security for 6G cognitive radio IoT networks. Sci Rep 14, 30990 (2024). https://doi.org/10.1038/s41598-024-82126-y.

[45]M. Alabadi, A. Habbal and X. Wei, "Industrial Internet of Things: Requirements, Architecture, Challenges, and Future Research Directions," in *IEEE Access*, vol. 10, pp. 66374-66400, 2022, doi: 10.1109/ACCESS.2022.3185049.

[46]Baktayan, A.A., Zahary, A.T., Sikora, A. et al. Computational offloading into UAV swarm networks: a systematic literature review. J Wireless Com Network 2024, 69 (2024). https://doi.org/10.1186/s13638-024-02401-4.

https://doi.org/10.59222/ustjet.4.1.1