IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 3, 2020, accepted June 12, 2020, date of publication June 16, 2020, date of current version June 26, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3002932*

# A Survey on Trend and Classification of Internet of Things Reviews

**AZANA HAFIZAH MOHD AMAN[1], ELAHEH YADEGARIDEHKORDI[2], ZAINAB SENAN ATTARBASHI[3], ROSILAH HASSAN[1], (Senior Member, IEEE), AND YONG-JIN PARK[4], (Life Senior Member, IEEE)**

[1]Center for Cyber Security, Faculty of Information Science and Technology, The National University of Malaysia, Bangi 43600, Malaysia
[2]Center for Software Technology and Management, Faculty of Information Science and Technology, The National University of Malaysia, Bangi 43600, Malaysia
[3]School of Computing, Universiti Utara Malaysia, Sintok 06010, Malaysia
[4]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu 88400, Malaysia

Corresponding author: Azana Hafizah Mohd Aman (azana@ukm.edu.my)

This work was supported by the Research under Grant FRGS/1/2019/ICT03/UKM/02/1, Grant GGPM-2019-030, and Grant PP-FTSM-2020.

**ABSTRACT** The Internet of Things (IoT) is shaping the current and next generation of the Internet. The vision of IoT is to embed communication capabilities with a highly distributed, ubiquitous and dense heterogeneous devices network. This vision includes the adaptation of secure mobile networks, anytime, anywhere, by anyone or anything with new intelligent applications and services. Many efforts have been made to review the literature related to the IoT for the benefit of IoT development. However, many issues need to be addressed to overtake the full potential of the IoT. Therefore, this paper aims to classify and standardize IoT research areas by considering review papers that were published between 2010 and 2019. This paper analyzes a total of 95 related reviews, which were manually selected from databases based on 6 chosen areas. This paper presents the trends and classification of IoT reviews based on 6 research areas, namely, application, architecture, communication, challenges, technology, and security. IoT communication research has been dominating the trends with 21% of total reviews and more than 100% research growth in the last 10 years. Hence, this paper can provide useful insights into specific emerging areas of IoT to assist future research.

**INDEX TERMS** IoT applications, IoT architectures, IoT challenges, IoT communication, IoT security, IoT technology.

## I. INTRODUCTION

A Cisco report [1] forecasted that by 2030, approximately 500 billion devices will embrace sensors and will be associated with the Internet. It is stated that the Internet of Things (IoT) is the network that links these devices for data communication. These smart devices produce data that IoT services and applications cumulate, evaluate, and distribute for further processes. The IoT network carries a variety of data formats with different protocols for different applications using different technologies. IoT technologies evolve and mature as they become part of the changing needs of people's everyday lives. Preserving security and confidentiality for data in IoT is critical, because the IoT environment has many challenges due to its lossy or constrained identity.

The associate editor coordinating the review of this manuscript and approving it for publication was Vyasa Sai.

The IoT phenomenon has rapidly emerged into a necessary ecosystem in which data, processes, humans, things and the Internet are associated with each other. Machine-to-Machine (M2M) [2] networks will increase by approximately 8.5 billion by year 2022 [3]. Half of the total M2M connections will derive from automation appliances, tracking applications and security monitoring. Smart transportation will be equipped with applications for Internet access, entertainment, automatic parking and diagnostics, autonomous driving, and navigation, which will become the fastest-growing industry segment.

Due to the number of linked devices, it is forecasted that global M2M IP communication will grow by 21.3 EB, from 3.7 EB per month in 2017 to more than 25 EB in 2022 [1]. This growth will produce a larger amount of traffic than the number of connections due to an increment in video applications usage from M2M connections. Considering this trend,

future communication will be blended with IoT devices and connections. Smart phones have become the dominant hub for future communication and will represents almost 45% of global IP traffic by 2022 [1]. This trend reveals the influence of smartphones on how people use the Internet to access data. This countable impact of IoT trends is generating new network necessities and demands. In addition to IoT traffic evolution implications, the IoT has promoted hybrid network revolutions and widespread awareness for network security enhancements [4], [5].

Until now, many IoT review papers have been conducted based on specific aspects of the IoT without any standard or generalization classification [6]–[107]. For example, a review of the communication area was conducted by [6], [52], [101]–[103]. [6] reviewed the IoT sensor network energy efficiency; [52] addressed the Bluetooth low energy (BLE) beacon; [102] highlighted the Information Centric Network (ICN)-based IoT, [103] conducted IoT communication for smart devices; and [101] reviewed various communication protocols in the IoT. Regarding smart cities, [7], [36] and [105] focused on the smart home and industrial perspective; [7] presented IoT industry applications, [36] covered different aspects of IoT in smart homes; and [105] reviewed possible technological movements of the IoT and the IoT influence on industrial communication. Other specific areas of focus are IoT challenges [8], IoT security [9] and IoT applications [104].

Hence, these IoT review papers have covered different IoT related areas that comprise protocols, technologies, application, frameworks, security, communication, architecture, challenges, etc. [6]–[105]. However, none of the existing review studies proposed a general and standard classification of these significant aspects of IoT. Thus, this paper aims to classify and standardize IoT research areas by considering review papers that were published between 2010 and 2019. This paper analyzes these research trends while presenting ideas and the benefits of identifying research gaps by classifying the IoT research areas. This paper also reveals the relationship between significant elements and components by mapping the elements to the areas and classification. Possible future research trends for each of the areas are also discussed.

The structure of this paper is divided into eight sections, as shown in Table 1. Section II delivers the methodology that was utilized to select and categorize the papers. Section III provides the overall trend for IoT reviews from 2010 to 2019. Section IV describes the IoT review trend for related standards and architecture layers. Section V describes the IoT review trend for applications in the areas of healthcare, transportation, and smart environments. Section VI describes IoT the review trend for technology, including hardware, middleware and cloud platforms. Section VII describes the IoT review trend for IoT communication, globally and locally, and interdevice and intradevice communication. Section VIII describes the IoT review trend for security, which covers vulnerability, attack, defense and mitigation.

**TABLE 1. Paper organization.**

| Section | Description |
|---|---|
| Section I | Introduction |
| Section II | Methodology |
| Section III | Internet of Things Reviews Trend |
| Section IV | Internet of Things Architecture |
| Section V | Internet of Things Applications |
| Section VI | Internet of Things Technology |
| Section VII | Internet of Things Communication |
| Section VIII | Internet of Things Security |
| Section IX | Internet of Things Challenges |
| Section X | Conclusion |

Section IX describes IoT challenges for all areas. The final section is the conclusion in Section X.

## II. METHODOLOGY

This paper followed systematic procedures that were proposed by [106] for reviewing the related studies. The process generally involved three stages, namely, 1) planning, 2) conducting and 3) reporting. The planning stage is the crucial part because it involves identification and scoping and includes search strategy, development, evaluation, inclusion/exclusion, classification, quality assessment, visualization, and validity (descriptive/theoretical). The conducting stage is a process that was implemented during the planning stage and systematically recorded. The reporting stage is the general structure and includes the introduction, related work, research method, results, and conclusion.

The planning stage of this paper is divided into 4 main parts: identification, eligibility, screening and included. This paper has considered two famous databases, namely, IEEE Xplore [107] and Science Direct [108], for searching review papers. The initial identification search started with keyword, year and article cluster filtering options. The following keywords were applied: Internet of Things review, IoT review, IoT survey, and Internet of Things survey. The chosen article cluster types are journal article and review article. The selected years range from 2010 to 2019. The initial identification produced a total of 283 articles. In the eligibility part, which involves an extraction process and is known as the exclusion phase, to implement a valid selection process, only full length articles from highly reputable journals that are indexed in Web of Science (WoS), Science Citation Index Expanded (SCIE) from Quartile 1 (Q1) are included, which produced a total of 164 articles. Further exclusion involves a screening part and an evaluation of title and abstract; only comprehensive review papers are selected, which produced 141 articles. The final part is the included part, which involves quality assessment and classification according to the 6 chosen areas—application, architecture, communication, technology, security and challenges—which produced a total of 95 articles. Of the final 95 selected papers, 87% were obtained from IEEE Xplore and 13% were obtained from Science Direct. The article selection procedure is shown in Fig. 1.

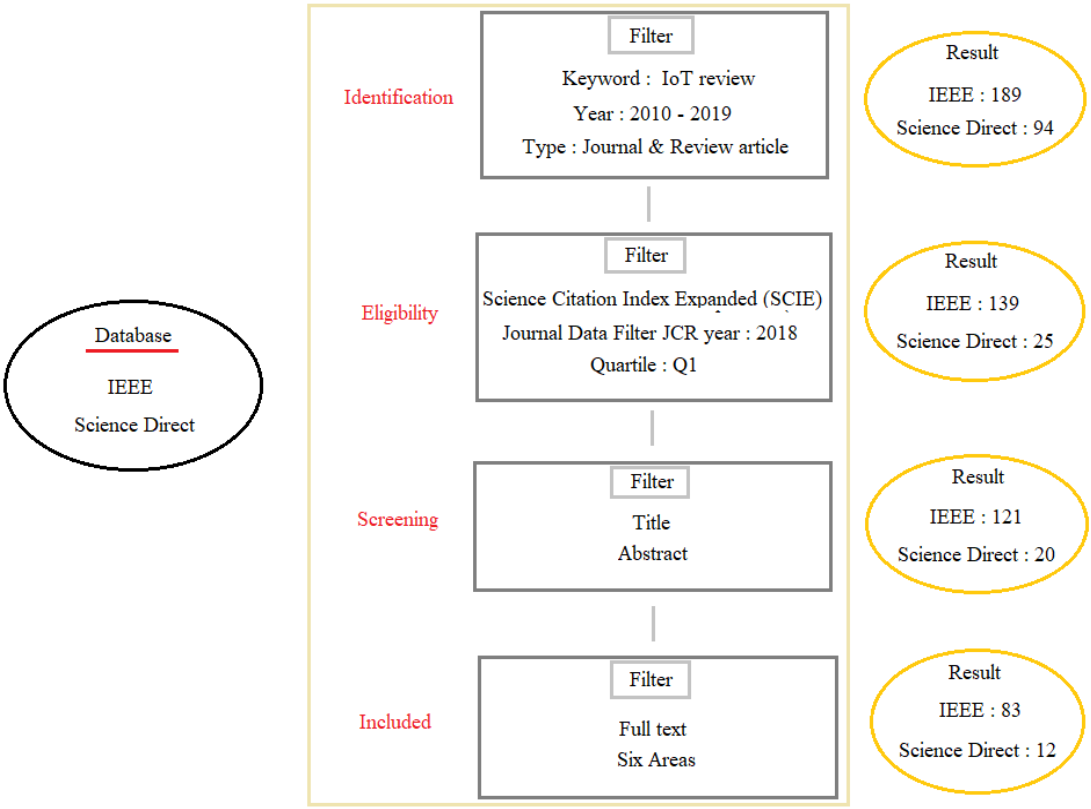


**FIGURE 1.** Methodology for review paper selection.

**TABLE 2.** IoT review areas.

| Area | 2010 – 2016 | 2017 – 2019 |
|---|---|---|
| Application | [7], [10]–[14], [17] | [24], [30], [33], [34], [36], [38], [39], [42], [45], [46], [47], [49], [52], [53], [57], [58], [60], [61], [63]–[66], [70], [71], [75], [77], [80], [81], [84], [85], [92], [95], [97], [100] |
| Architecture | [10], [11], [18], [20], [22] | [24], [30]–[32], [37], [38], [40], [44], [46], [56], [57], [62]–[64], [67], [68], [73], [75], [78]–[80], [86]–[90], [94], [100] |
| Challenges | [8], [11], [15], [16], [18]–[21] | [25], [26], [28]–[30], [42], [44]–[48], [54], [57], [63], [76]–[79], [95], [99] |
| Communication | [6], [10], [12], [13], [18], [23] | [24], [27], [28], [31], [32], [34], [37]–[42], [44], [46], [49], [52]–[56], [58], [60], [63], [64], [67]–[74], [78], [86]–[88], [93]–[95], [97], [99], [100] |
| Security | [9], [11], [13], [15]–[16], [19] | [27], [32], [34], [35], [37], [43], [44], [54], [57], [62], [63], [68], [75], [78]–[81], [83]–[91], [94], [96], [98] |
| Technologies | [10]–[12], [14], [18], [20], [23] | [29], [30], [33], [35], [39]–[42], [45], [48], [50], [51], [53], [57]–[62], [65], [66], [68]–[70], [74], [77], [84], [89], [92], [93], [95] |

## III. INTERNET OF THINGS CURRENT REVIEW TREND

A three-tier pyramid view of the trend and classification of the selected review papers is shown in Fig. 2. Tier 1 is the main topic, which is the IoT Review. In Tier 2, six areas are discussed in the IoT reviews, namely, application, architecture, technologies, communication, security, and challenges, as shown in Table 2. In Tier 3, the technical aspects are highlighted in each of the areas. In the application area, most of the reviews emphasize the industry or functionality of the IoT [7]. In the reviews of the architecture area, the explanations focus on the layer and protocol involved. In the technology area, the review discussions focus on the recent available hardware, middleware, and platform [11]. In the area of communication, the reviews analysis included the range coverage, network topology and IP-based or non-IP-based architecture [24]. Another emerging area in the IoT review is the security area, which highlighted four famous issues: vulnerability, attack, defense and mitigation [27]. A continuously discussed area comprises the challenges, which encompasses current and future issues of the 5 areas. Table 2 lists all the selected review papers. The papers are sorted by year, from 2010 to 2016 and from 2017 to 2019.

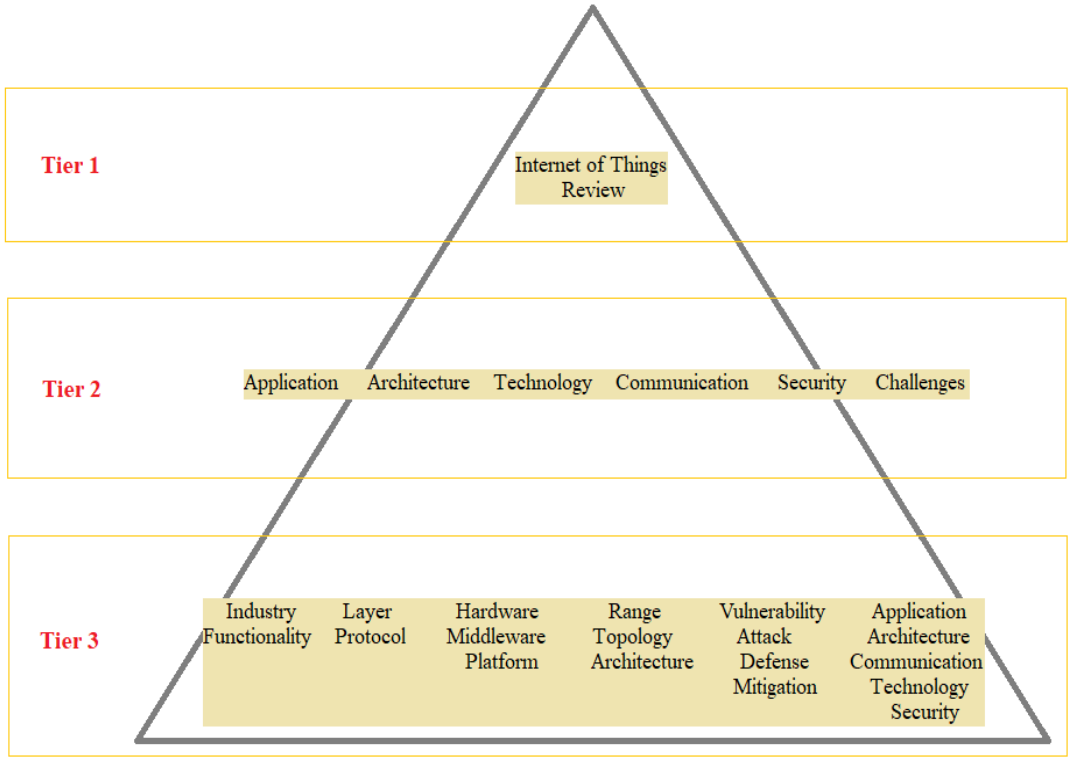


**FIGURE 2.** Three-tier hierarchy.

Comparing the first few years with the recent years, there is a large increment in the IoT reviews with an increment greater than 100% for the application, architecture, communication, technology, challenges, and security areas. In the last 10 years, the percentages of increment for the areas of application, architecture, challenges, communication, security and technology are 483%, 460%, 111%, 760%, 300% and 343%, respectively. This trend shows a parallel with the forecasted results according to [1]–[5]. From 2017 to 2019, most researchers are interested in communication followed by application. Technology, security, and architecture have gained nearly the same interest. The lowest total number of reviews were obtained for the area of challenges, which also gained the lowest percentage of increment. This analysis is illustrated in Fig. 3 and Fig. 4.

Four major characteristics of the IoT are identified in [6]–[100], namely, heterogeneity [30], dynamic [54], scalability [19] and interoperability [20], as described in Table 3.

Fig. 5 shows the mapping between trends and classification of IoT reviews and the IoT characteristics in Table 3. The areas and characteristics are interrelated. The communication, technology, and security areas cover the heterogeneity characteristic, while the areas of application, security, and communication cover the dynamic characteristic. The architecture area has an important role in the scalability characteristic. The areas of architecture, communication, and technology cover the interoperability characteristic. Details for each area will be explained further in each section.

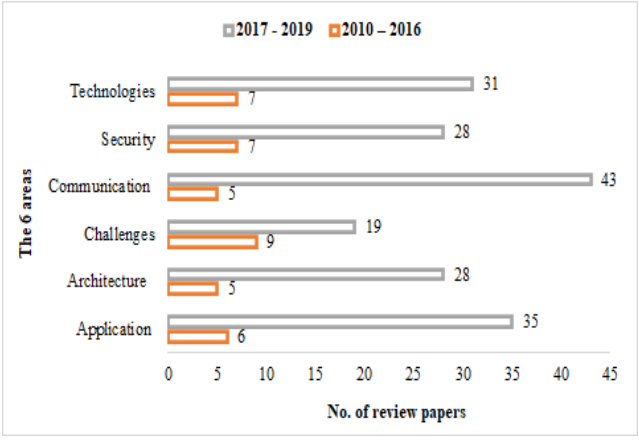


**FIGURE 3.** Trend and classification of IoT reviews 2010-2019.

## IV. INTERNET OF THINGS ARCHITECTURE

No standard IoT architecture is employed by all applications or technologies. Each technology has a unique framework and claims its best practice [4]. However, a draft of the IoT architecture framework for smart cities and a smart grid architecture standard were proposed by IEEE from 2018 – 2019 [109] and [110]. The IoT can be complex because it is heterogeneous and broad regarding the scalability in terms of addressing and delivering. IoT architecture must include devices, networks, and applications to seamlessly interoperate to produce smart outcomes with security

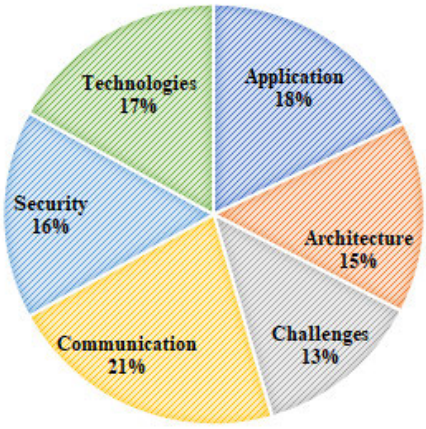


**FIGURE 4.** Classification percentage for IoT reviews 2010-2019.

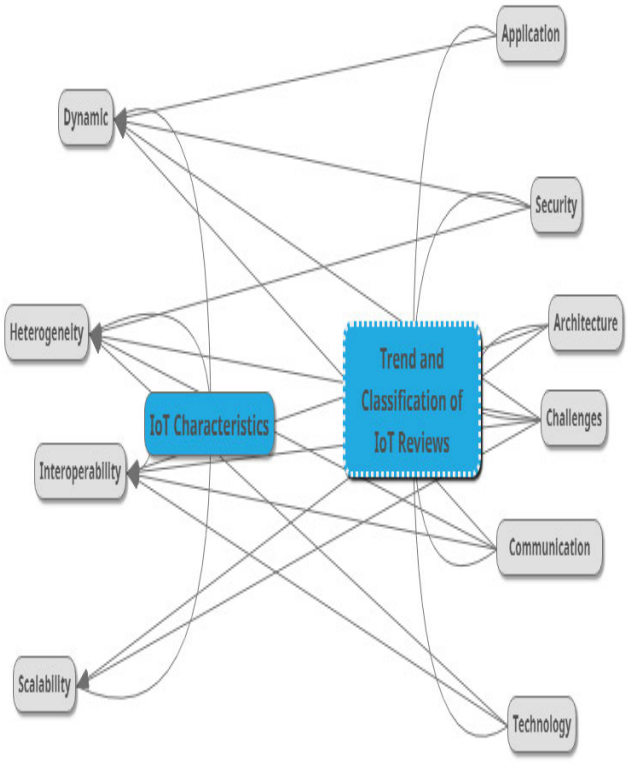


**FIGURE 5.** Mapping of IoT review trends and classification with IoT characteristics.

considerations and deliver data according to user acceptance services by connecting things. IoT architecture contains few layers of technologies, protocols, and standards for IoT communication, as revealed by the papers in the architecture area in Table 2. These layers help different technologies communicate with each other by allowing the scalability, heterogeneity, and interoperability of IoT implementation in many scenarios.

Currently, the trend of IoT architecture reviews is either based on the OSI layer or the TCP/IP layer; samples of 3-layer, 4-layer and 5-layer architectures are illustrated

**TABLE 3.** IoT significant characteristics.

| Characteristic | Description | Area |
|---|---|---|
| Heterogeneity | Devices are heterogeneous due to differences in technology platforms and network environment. | Communication, Security, Technology |
| Dynamic | Up and down times vary, which makes the devices dynamically connected and/or disconnected to a service. | Application, Security, Communication |
| Scalability | Devices are connected to each other depending-on the application purposes, which range from small number of devices scale to large number of devices scale. | Architecture, Technology |
| Interoperability | Devices from different architecture and technologies are able to communicate with each other, which enables network accessibility and compatibility to ease of applications and services. | Architecture, Communication, Technology |

**TABLE 4.** Six types of IoT architecture layers.

| Layer | Article |
|---|---|
| 7 layers | [57], [79] |
| 6 layers | [30], [40], [87], [94] |
| 5 layers | [11], [24], [30], [31], [64], [78], [79], [94] |
| 4 layers | [10], [11], [38], [63], [64], [67], [75], [78], [80], [89], [90] |
| 3 layers | [20], [31], [32], [44], [62], [68], [78], [86], [88], [100] |
| Specific layer | [18], [31], [37], [46], [56], [68], [73], [79], [80] |

in Fig. 6 and referenced in Table 4. The layers are further explained as the top layer, middle layer and bottom layer in the remainder of this section. Six types of classifications are discussed: 7 layers [57], 6 layers [30], 5 layers [11], 4 layers [10] and 3 layers [79]. Few surveys specifically discuss certain layer [46] based on services and functions.

The percentages of the trend for the IoT architecture layers review, according to the layers classification, are shown in Fig. 7. Most researchers choose 5-layer architecture surveys; the lowest surveys employ 7 and 6 architecture layers. To generalize and standardize the architecture layers of the IoT, this paper disregards the differences among the services and classified the functions of all possible layers into three layers, namely, top layer, middle layer and bottom layer. The classifications of the top, middle and bottom layers are based on the protocol and functions requirement by the layers. The top layer is mainly employ for the user functions requirement, the middle layer is utilized for the network functions requirement and the bottom layer is designated for the hardware functions requirement.

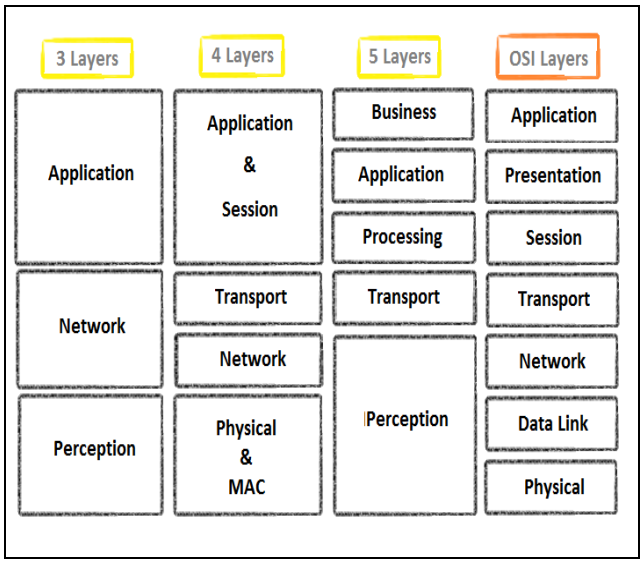


**FIGURE 6.** IoT architecture and OSI layers.

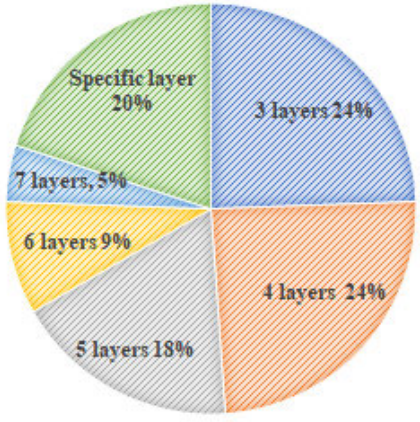


**FIGURE 7.** Trend of IoT architecture layers.

The top layer is the user management layer, which includes the application [24], business [78], interface [10], support [78], or service/data layer [10]. This layer handles the entire IoT system and the business and process rule engines. Hence, this layer manages and controls data presentation and formatting for objects and systems interaction. The rule engines activate the logics with automated interactive processes to enable a more responsive IoT system. Compared to the standard TCP/IP, the top layer is based on Hyper Text Transfer Protocol (HTTP) communication. For IoT communication, however, this layer is based on IoT communication, such as Message Queue Telemetry Transport (MQTT) or Constrained Application Protocol (CoAP).

The middle layer, which is also known as the platform, falls in the area of network communication, including the network layer [75], transport layer [37], middleware layer [90] or Internet layer [63]. This layer is able to provide various services to the lower and top layers and is accountable for connections to other smart devices and network nodes, such as gateways, servers or routers. This layer handles sensor data transmission, packet routing and processing via networks such as ZigBee, Wi-Fi, radio frequency identification (RFID), Bluetooth Low Energy (BLE), Near Field Communication (NFC), local area network (LAN), and ultra-wideband or wide area networks (WANs) such as GSM, GPRS and LTE. For routing in the middle layer, the Internet Engineering Task Force (IETF) Routing over Low Power and Lossy Networks (ROLL) working group has developed a routing protocol for Low Power and Lossy Networks (LLNs), which is referred to as RPL.

The bottom layer is considered the adaptation layer [87], physical/MAC layer [44], infrastructure layer [100], sensing layer [78] or perception layer [44]. This layer is the interconnection of the sensor physical devices and digital communication. On the bottom layer, the sensors sense and gather information, such as physical parameters or identifiers about the environment. The sensors have the competency to obtain quantities values for temperature, speed, air quality, humidity, flow, pressure, electricity and movement. The quantities value is translated to a signal, a machine language.

In Table 5, the layers from the architecture in Table 2 are allocated according to the top, middle and bottom layer functions of Table 6. Table 6 summarizes the top, middle and bottom layers functions and possible current protocols. Fig. 8 illustrates the mapping relationship among the number of layers, layer reviews and suggested 3-layers classification.

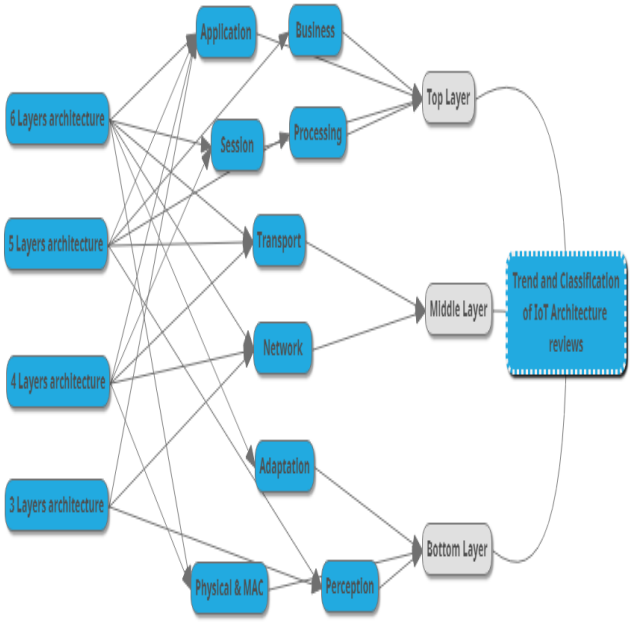


**FIGURE 8.** Classification of IoT architecture reviews.

Even though there is no standard for IoT architecture and framework, the Institute of Electrical and Electronics

**TABLE 5.** IoT architecture layers.

| Layer | Paper | Top Layer | Middle Layer | Bottom Layer |
|---|---|---|---|---|
| Application | [31], [32], [38], [40], [44], [57], [63], [64], [67], [75], [78], [80], [86]-[90], [94], [100] | √ | | |
| Business | [78] | √ | | |
| Support | [67], [78] | √ | | |
| Service/Data | [67], [78] | √ | | |
| Transmission | [32], [64] | | √ | |
| Transport | [31], [40], [63], [64], [78], [87], [94] | | √ | |
| Middleware | [78], [90] | | √ | |
| Internet | [63] | | √ | |
| Network | [31], [40], [44], [64], [75], [78], [80], [87], [88], [90] | | √ | |
| Adaptation | [87] | | | √ |
| Physical/MAC | [31], [38], [44], [56], [68], [73], [86], [87], [89], [94] | | | √ |
| Infrastructure | [100] | | | √ |
| Sensing | [ 64], [75], [78], [80], [90] | | | √ |
| Perception | [32], [44], [78], [88] | | | √ |

**TABLE 6.** IoT layer classification with possible function and protocols.

| Layer Classification | Function | Protocols |
|---|---|---|
| Top: User | Decision support tools or social media or applications | AMQP, COAP, DDS, DNS-SD, MQTT, MDNS, REST, XMPP |
| Middle: Network | Integrates applications, networks and devices. Hide complexity from user (service or data composition, management and object abstraction) | UDP, IPV6/V4, RPL, DODAG |
| Bottom: Device | Physical infrastructure with multiple access and modulation techniques (edge nodes) | 6LOWPAN, LTE-A, EPCGLOBAL, ZWAVE, IEEE 802.15.4 |

**TABLE 7.** IEEE Standard related to IoT.

| Areas | Standard |
|---|---|
| Local and Metropolitan Area Networks\| (including PANs) | 802.1AS, 802.1Q, 802.15.4, 802.15.4e, 802.15.4f, 802.15.4g, 802.15.7, 802.11ad |
| Ethernet | 802.3, 802.3.1 |
| Information Technology (includes WLAN, WPAN,WRAN) | 802.11, 802.15.1, 802.15.2, 802.15.3c, 802.15.3, 802.15.4j, 802.15.5, 802.15.6, 802.22, 21450, 21451-1, 21451-2, 21451-4 |
| Air Interface for Broadband Wireless Access Systems | 802.16, 802.16p |
| Wireless Access in Vehicular Environments | 1609.2, 1609.3, 1609.4, 1609.11, 1609.12 |
| Local Area Network/Wide Area Network Node Communication Protocol to complement the Utility Industry End Device Data Tables | 1703 |
| Long Wavelength Wireless Network Protocol | 1902.1 |
| Health Informatics | 11073-10418, 11073-10420, 11073-10441, 11073-30300, 11073-30400 |

Engineers (IEEE) has provided related standards to be employed in IoT architectures. Table 7 shows some of the IoT related standards developed by IEEE. These standards cover information technology, health informatics, local and metropolitan area networks, Ethernet, wireless access, End-to End device data, etc.

This paper suggests that the IoT architecture classification comprise 3 main layers with regards to the IEEE standards and the communication protocols in Table 6 and 7. Possible research in IoT architecture must be able to match the 3-layer classification with functionalities and communication protocols. Any new architecture with specific functions will fall

under a particular layer, which will ease the interoperability and scalability of the IoT.

## V. INTERNET OF THINGS APPLICATION

Researchers indicate that the IoT is improving the quality of human life. Current IoT applications include smart home [7], healthcare [11], smart agriculture [38], transportation [10], smart cities [12], and smart industries [46]. The IoT has tremendous benefits for human life via its smart services. People are able to utilize almost every activity anywhere, anytime and enable instant decision-making for efficient management. The trend of IoT applications reviews are shown in Fig. 9. Healthcare is highlighted as the most researched application, followed by transportation and environment. Other areas include utility [47], military [57], safety [10], education [7] and financial [75].

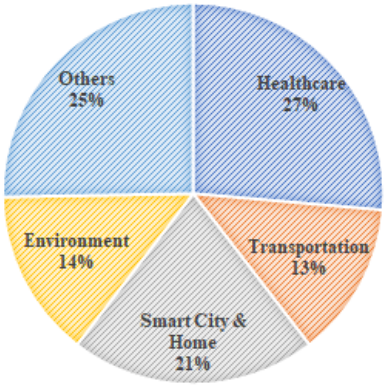


**FIGURE 9.** Trend of IoT applications reviews.

Table 8 summarizes the IoT application reviews of 3 major classifications, namely, transportation, healthcare, and smart environment. Reviews of the application areas in Table 2 revealed that surveys of IoT applications are conducted based on the services or functionality and industries where the application provides smart services. In recent years, most of these areas involve cloud platform and devices with sensors, as shown in Table 8.

Healthcare is among the main application area in the IoT that has gained interest from researchers, the public and industries. The advancement of the IoT has contributed many benefits in patient welfare and satisfaction, as well as hospital management and operations. Among the IoT-based technologies that are employed for healthcare are wearable devices that communicate with big data, cloud and fog computing and utilize the wireless body area network (WBAN) or RFID. These devices offer a desirable solution for mobile health applications and monitoring systems for many purposes, such as electrocardiogram, blood pressure, and oxygen saturation. Other healthcare applications are rehabilitation systems; management systems for inventory, medication and wheelchairs; diabetes prevention and adverse drug reaction. IoT devices enable doctors to continuously monitor patient health via remote monitoring without physical interaction.

For transportation application, some highlighted functionalities from the papers in Table 2 are smart parking, smart entertainment, driverless assistant, sensing systems, and route location identifiers. These solutions are able to provide safety, comfort and easy driving experiences while improving mobility communication while driving.

The concerns with IoT environmental applications include waste management, climate or weather monitoring, smart agriculture, and smart farming. Waste management has become an urgent issue in many parts of the world. There is confusion between garbage collection and waste management in some countries, but waste management helps to overcome this issue. Climate monitoring provides weather forecasts and secure life and properties. Smart agriculture and smart farming help to increase products at low cost.

Future cities are projected to transform drastically how people live, connect, and move in urban environments. Smart cities require smart real-time monitoring systems with universal connectivity, ubiquitous sensors and artificial intelligent data control and processing. By using IoT, smart cities are able to deploy different smart services to citizens, smart homes, and smart industries. This deployment helps to improve the usage of other smart resources and applications, such as healthcare, transportation, environment, and building. Another functionality is smart digital citizen identification, which is related to other functions and applications. IoT devices buildup automated control, monitoring, management, and maintenance for smart building and factory. IoT can be applied to various industries, such as the food industry, where automated systems can track, monitor, and trace food freshness quality along the supply chain to improve production, transportation and logistics.

Fig. 10 shows the classification mapping of IoT applications reviews and illustrates the relationship between the application classification and the most recent applied technology.

The IoT application classification is still growing due to services growth and additional or changes in requirement. Transportation, healthcare and smart environments have many functionalities and services to be explored. As new deceases are identified, new requirements are needed for healthcare applications. Transportation and the environment have to fulfill current user demand. Researchers must consider the dynamic characteristics of IoT applications.

## VI. INTERNET OF THINGS TECHNOLOGY

IoT technologies differ in terms of middleware [51], hardware [59] and cloud integration platforms [50]; some of these technologies are shown in Table 9. The sensor is the most popular IoT hardware, because IoT devices consist of sensors of boards with a microcontroller, microprocessor and network interface. The most prevalent IoT hardware boards are Rasberry Pi and Arduino. Table 10 shows the predominant IoT sensor technology with its functionalities and some of the available devices. IoT firmware is a low-level control

**TABLE 8.** Summary of IoT application reviews.

| Major Classification | Paper | Functions | Others |
|---|---|---|---|
| Transportation | [7], [10], [30], [33], [42], [46], [47], [53], [57], [63], [75], [84] | • Auto assist driving whenever the driver is unfocused.<br>• Intelligence traffic management with collision avoidance systems and augmented maps.<br>• Infrastructure monitoring that can provide process monitoring with location sensing and sharing.<br>• Indoor air quality monitoring to ensure the quality and safety of goods.<br>• Logistics temperature control and monitoring auto alert the temperate of warehouse and goods delivery.<br>• Vehicle auto diagnose whereby the necessary information are collected and diagnose to provide real-time alarms or emergencies to drivers. | • Communication - RFID, WSN, Wifi, 3G/4G/5G, LTE, NFC, ZigBee<br>• Technology - IoT cloud, actuators, visual marker, numeric identifier, RFID tags, mobile RFID readers, intelligent video cameras, sensors |
| Healthcare | [7], [10], [11], [13], [14], [24], [30], [33], [34], [42], [45], [46], [47], [53], [57], [60], [61], [70], [75], [81], [84], [85], [92], [97] | • Patient: Real-time position tracking, flow and motion monitoring, identification, authentication and data health collection, monitoring and mitigation of eating disorders<br>• Asset and medicine: Real-time inventory tracking, material tracking, assets management, automated data collection, telemedicine medication prescription and medicines storage/freezer quality monitoring.<br>• Services: Auto pre-emergency services, crowd monitoring, vital signs monitoring for high performance service center.<br>• Public: Auto alert and warn to public not to be exposed to UV sun rays. Decease warn and precautious to public. | • Communication - Wifi, 3G/4G/5G, LTE-A, BLE, ZigBee, GPS, NFC, RFID<br>• Technology - IoT cloud, sensors, accelerometers, gyroscopes, rotational vector, orientation, magnetometers sensor, biosignal monitoring, M2M Gateway, intelligent video cameras |
| Smart surroundings | [7], [10], [12], [30], [33], [34], [36], [38], [42], [45], [46], [47], [52], [53], [57], [60], [63], [64], [66], [71], [75], [77], [81], [84] | • Smart city: comfortable homes/offices, industrial plants, smart museum, smart gym<br>• Smart environments: diverging climate conditions, environment monitoring-food supply chain<br>• Smart Gym: training machine auto exercise profile, auto health parameter monitoring,<br>• Smart agriculture: water quality assurance, water supply, monitor irrigation in agricultural land, soil parameters, processing<br>• Smart homes/offices: shop floor device malfunction, automatic lighting, monitoring and alarm system, automate electrical switches for appliances, food traceability<br>• Smart factory/industry: monitoring of gases/chemicals/food during processes. Real-time monitoring of machinery, such as electrical systems, power consumption, smart metering, telemetry oil, brakes and lubricant reading, water pipeline, and corrosion state<br>• Smart security: intelligence image processing that tracks or identifies dubious activities, unauthorized entry and detects left or stolen items | • Communication - RFID, Wifi, 3G/4G/5G, LTE-A, BLE, ZigBee<br>• Technology – Sensors, actuators, logic automation, RFID tag, grid, metering, heating, ventilation, and air conditioning |

software for the IoT's specific hardware. The IoT firmware varies because the board or the microprocessors differ. Middleware enables communication among complex programs that were not originally intended to be connected. Hence, IoT middleware integrates these programs to smooth the IoT architecture communication example of recent middleware is FiWare. IoT functionalities that require middleware supports are shown in Table 11. Currently, the number of operating systems and software that can run with IoT is increasing. In this classification, both are considered cloud platforms. Current existing cloud platforms include AWS Amazon, Brillo, Azure and Carriots.

Fig. 11 maps the IoT technology reviews into three significant classifications: hardware, middleware and cloud platforms. The firmware and software are included in the middleware cluster. The mapping also highlights some of the recent IoT technology products from the reviews in Table 9.

Fig. 12 shows the trend of IoT technology reviews. Most surveys and reviews address hardware and cloud platforms. The lowest surveys entail middleware,

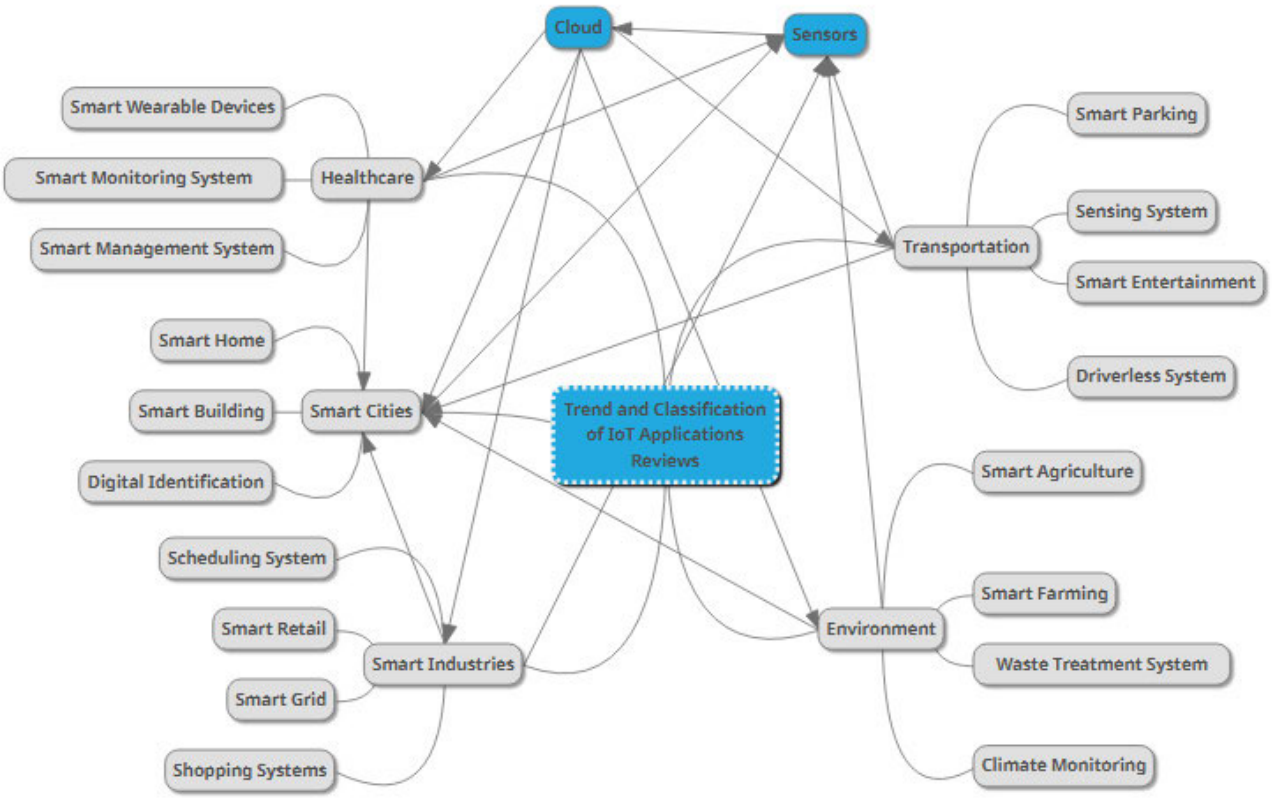


**FIGURE 10.** Classification of IoT application reviews.

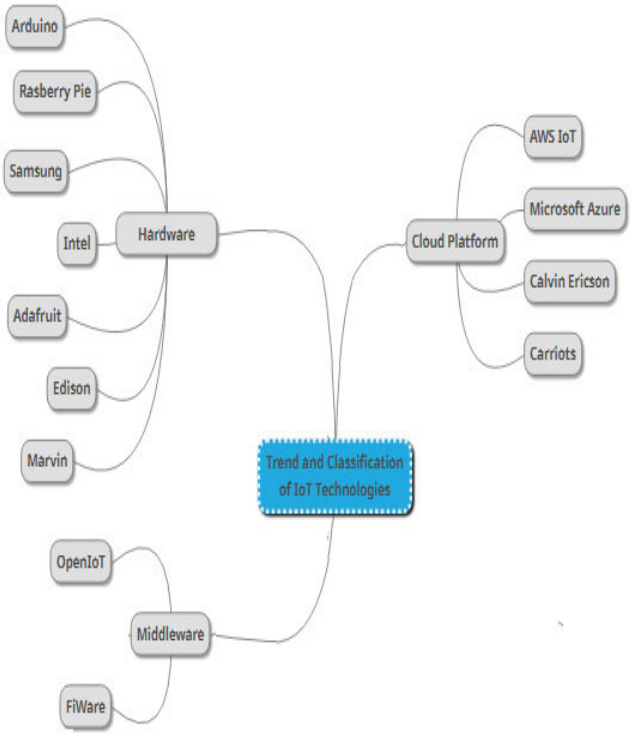


**FIGURE 11.** Classification of IoT technology reviews.

while software is included in the platform classification and firmware is included in the middleware classification.

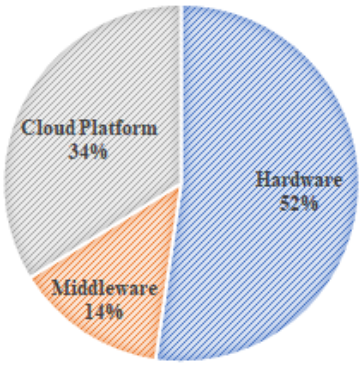


**FIGURE 12.** Trend of IoT technology reviews.

Cloud platforms are becoming popular technology as more hardware and software developers change to cloud services because they are user-friendly and cost-effective.

This paper has divided the IoT technologies classification into 5 areas, which comprise possible future research to satisfy the needs and requirements of the next generation. Any new research for IoT technology must allow and consider the heterogeneity and interoperability of IoT network and communication.

## VII. INTERNET OF THINGS COMMUNICATION

IoT communications involves many protocols that serve a specific architecture layer, whether it is IP-based or non-IP based. These protocols serve communication for

**TABLE 9.** IoT technology products: hardware, software and cloud.

| Classification | Product | [12] | [23] | [40] | [50] | [51] | [59] | [61] | [68] | [84] | [93] |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Hardware** | Arduino | √ | | | | | √ | √ | | | |
| | BeagleBone | | | | | | √ | | | | |
| | Carambola 2 | | | | √ | | | | | | |
| | Intel | √ | | | | | √ | | | | |
| | Raspberry Pi | √ | | | | | | √ | | √ | |
| | Samsung | | | | | | √ | | | | |
| | Tessel 2 | | | | | | √ | | | | |
| **Middleware** | Android Platform | | | | | | | | | | √ |
| | ARM mbed OS | | | | | √ | | | | | |
| | Brillo | | | | | √ | | | | | |
| | Contiki | | √ | | | | | | | | |
| | Intel System Studio | | | | | √ | | | | | |
| | Windows 10 IoT | | | | | | | | | | √ |
| | RIOT | | √ | | | | | | | | |
| | FiWARE | | | | √ | | | | √ | | |
| **Cloud Platform** | AWS IoT | | | | √ | | | | √ | | |
| | Microsoft Azure IoT | | | | √ | | | | | | |
| | Carriots | | | | √ | √ | | | | | |
| | Cloudplugs | | | | √ | | | | | | |
| | EVRYTHNG | | | | √ | √ | | | | | |
| | Google Cloud | | | √ | | | | | | | |
| | Thing Speak | | | √ | | √ | | | | | |
| | Sensor Logic | | | √ | | | | | | | |
| | Thing Plus | | | √ | | | | | | | |

**TABLE 10.** IoT sensor classification, functions and devices.

| Classification | Paper | Functions | Devices |
|---|---|---|---|
| Position, occupancy, and motion | [14], [29], [40], [45], [59], [60] | • Measures object's position any-axis.<br>• Identify the existence of entity (human or animal) in the observation area.<br>• Detect movement of entity (human or animal). | Potentiometer, inclinometer, proximity sensor electric eye. |
| Velocity, force, and pressure | [41], [51], [58] | • Measure and indicate object movements velocity along a straight line (linear) or rotation (angular).<br>• Measure and identify the magnitude threshold and the physical force applied. | Accelerometer, gyroscope, force gauge, viscometer, tactile sensor, barometer, bourdon gauge, piezometer |
| Flow and chemical | [10], [14], [29], [41] | • Identify and measure the rate of fluid flow.<br>• Identify and measure the concentration of chemicals. | Anemometer, mass flow sensor, water meter, breathalyzer, olfactometer, smoke detector |
| Acoustic and light | [29], [58] | • Measure sound or noise levels.<br>• Identify the presence of light. | Microphone, geophone, hydrophone, Infrared sensor, photodetector, flame detector |
| Humidity, temperature, and radiation | [11], [29], [30], [39], [48], [51], [57], [58], [59], [61] | • Detect and measure water vapor in the air.<br>• Sense radiations in the environment.<br>• Measure the degree of heat or cold. | Hygrometer, humistor, soil moisture sensor, Thermometer, calorimeter, temperature gauge, scintillator, neutron detector |

global networks, local networks or hybrid networks and are built to support the IoT communication requirements, regardless of whether the requirements of are interdevice or intradevice. Based on the reviews in Table 2, the IoT communication functionality can be classified according to the topology and communication range, as shown in Table 12.

**TABLE 11.** IoT middleware functionalities.

| Function | Paper | Description |
|---|---|---|
| Discovery | [20], [50], [51], [68] | Each device advertises the available service and existence before each connection. Hence, middleware lists the necessary information of the devices and its services in the form of application programmer interface. |
| Big Data | [20], [50], [51], [65], [93] | Integrating machine learning or artificial intelligence into the network of IoT, which involve physical connection to the cloud platform computation. The ability to connect to different types of clouds platform and heterogeneous autonomous devices. |
| Security | [20], [50], [51] | Implementing security management and controls, which involves user authentication and technology access. |

**TABLE 12.** IoT communication classification.

| Topology | Paper | Range | | Architecture | |
|---|---|---|---|---|---|
| | | Long | Short | IP based | Non-IP based |
| Global | [18], [24], [28], [34], [40], [42], [44], [53], [54], [55], [63], [64], [67], [68], [70], [72], [73], [78], [100] | Inter-device | | √ | |
| Local | [6], [12], [13], [23], [24], [27], [31], [37], [38], [39], [40], [41], [46], [52], [56], [60], [63], [64], [67], [69], [70], [73], [86], [87], [88], [93], [94], [95], [97], [99], [100] | | Inter/Intra-device | | √ |
| Hybrid | [10], [24], [34], [49], [58], [67], [71], [74] | Inter-device | Inter/Intra-device | √ | √ |

Regarding IoT dynamic communication, when there is a change in the attachment of a node or access technology from one point to another point, it is considered mobility. The mobility is differentiated as physical or logical mobility and is further differentiated by global and local, interdevices and intradevices. Each type of mobility involves a specific communication protocol depending on the architecture layer that is involved.

Global and local area networks for IoT communication require IP-based mobility management protocol. IPv6 is the most preferred protocol for IoT communication because it is scalable and stable. Current available IP-based mobility management is classified into two types, namely, host-based and network-based. Some of the available mobility managements are MIPv6, HMIPv6, PMIPv6, SPMIPv6, and CSPMIPv6. IoT global communication requires a border router to support IoT packets routing and sensor control. The sensor management control manages and stores a sensor's information and the attached router information. The control of IoT mobility depends on the mobility management architecture protocol regardless of whether it is host-based or network-based. If it is network based, an anchor router is equipped with a Mobility Anchor Module that can either reside at the Local Mobility Anchor (LMA) or Mobile Access Gateways (MAGs) with a scheme optimized transmission path and low handover delay.

Inter-device and intra-device communication involves bottom layer architecture communication and a change in access technology. The IEEE 802.15.4 protocol is designed to provide long life cycles for low-power device communication. The communication range classification, network topology and some of the communication protocol discussed by review papers are summarized in Table 13.

To enable smooth communication, most papers highlighted some important criteria for determining the proper type of communication technology to be used, such as the data rate, bandwidth, transmission range, operating frequency, and interoperability.

The IoT communication trend is shown in Fig. 13. Most reviews discussed global communication, which involves IP-based, long-range and inter-device communication. Fig. 14 shows the mapping classification of the IoT communication reviews. The mapping illustrates the relationship among the classification of IP-based, non-IP-based, short-range, long-range, global, local, interdevice and intradevice communication.

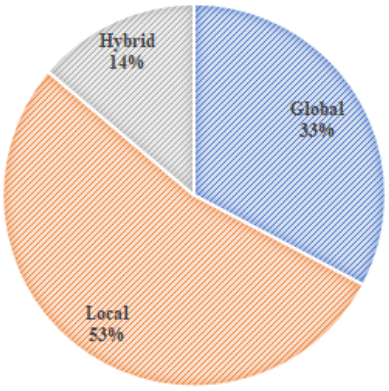


**FIGURE 13.** Trend of IoT communication reviews.

**TABLE 13.** IoT communication classification according to possible network topology.

| Classification | Communication | Description | Paper |
|---|---|---|---|
| Short-range<br>- IoT-PAN<br>- IoT-BAN | BLE | Bluetooth Low Energy A short-range and low energy consumption protocol. The architecture stack is similar to the standard Bluetooth technology and consists of a controller for physical and link layer implementation. | [39], [40], [41], [44], [52], [53], [58], [64], [64], [67], [69], [73], [86], [97], [100] |
| | ZigBee | Personal area network (PAN) on IEEE 802.15.4 standard and supports multihop routing. A cheap, reliable, and low-energy device communication solution with a very short range of 10–100 meters. | [24], [31], [39], [40], [41], [42], [44], [53], [56], [58], [67], [69], [86], [87], [93], [97] |
| | NFC | A wireless short-range, low-speed communication for two electronic devices. | [38], [63], [64], [67], [70] |
| | HaLow Wifi | New long-range and low-power consumption protocol compared to existing traditional WiFi. Allow IP-based connection and support large star-shaped networks. The lower is the frequency, extend the range with a lower data rate. | [39], [41], [42], [44], [46], [58], [60], [67], [70], [71], [93], [100] |
| | RFID | Electromagnetic fields or radio frequency protocol with different type of tagging device: active, semi and passive. Active tags read at a greater range compared to passive tag. The frequency ranges differ for low, high and ultra-high frequency RFID. | [10], [12], [13], [38], [44], [63], [63], [95], [99] |
| | 6LowPAN | IPv6 over low-power wireless PAN on IEEE 802.15.4 standard. Use gateway for device-to-device Internet communication to other IP-based devices. | [31], [41], [44], [71], [87], [88], [94] |
| Long-range<br>- IoT-WAN<br>- IoT-MAN | 3G/4G/5G | Digital generation for cellular network standard 5G is the latest generation with better speed and coverage | [18], [28], [40], [42], [44], [53], [58], [64], [67], [73], [74] |
| | LTE | Based on narrow band communication for large number of devices. The speed ranges between 40 kbps to 10 Mbps. | [18], [24], [28], [32], [40], [54], [55], [64], [67], [72], |
| | EC-GSM | A low-power WAN based on eGPRS. Support high-capacity, long-range cellular system with low energy and complexity. | [28], [40], [42] |
| | NB-IoT | A low-power WAN radio technology standard and subset of LTE technology. Support a wide range of cellular devices and services. | [24], [28], [32], [40], [42], [53], [55], [68], [71], [72] |
| | Sigfox | Based on narrow band communication with very long waves and long-range communication. Maximum of 12 bytes for each message up to 140 messages daily. | [24], [28], [32], [40], [42], [71], [72], [100] |
| | LoRaWAN | A long range communication with data rates between 0.3 kbps and 50 kbps. Support multiple applications of multiple wide area networks. | [24], [28], [32], [40], [42], [58], [68], [71], [74], [100] |
| | Weightless | Based on narrow band signals and hops across frequency bands; it supports cryptographic encryption and mobility | [28], [40], [42] |

This paper has classified IoT communication as non-IP-based and IP-based communication, which possibly consists of short-range and long-range communication that is connected locally, globally or a hybrid of both. Any new research for IoT communication must consider the dynamic, heterogeneity and interoperability characteristics of the IoT network and communication, and consideration of a hybrid connection is useful because it enables local and wide-range coverage of communication. Future research communication must also enable non-IP-based communication for global long-range interdevice communication and the possibility of using content or information centric-based communication.

## VIII. INTERNET OF THINGS SECURITY

The reviews of IoT security has significantly increased due to an increase in IoT applications and services. Security complicates hackers' lives because it protects a system from being compromised by them. Security reduces the probability that a treat will be compromised or reduces the security risk. The purpose of IoT security is to not only protect assets but also ensure communication privacy, confidentiality, availability, and integrity in the IoT ecosystem. Hence, IoT security has recently gained researchers' interest in studying the vulnerability [96], defense [43], attack [91] and mitigation [86] using the available simulator, emulator, and analysis platforms.

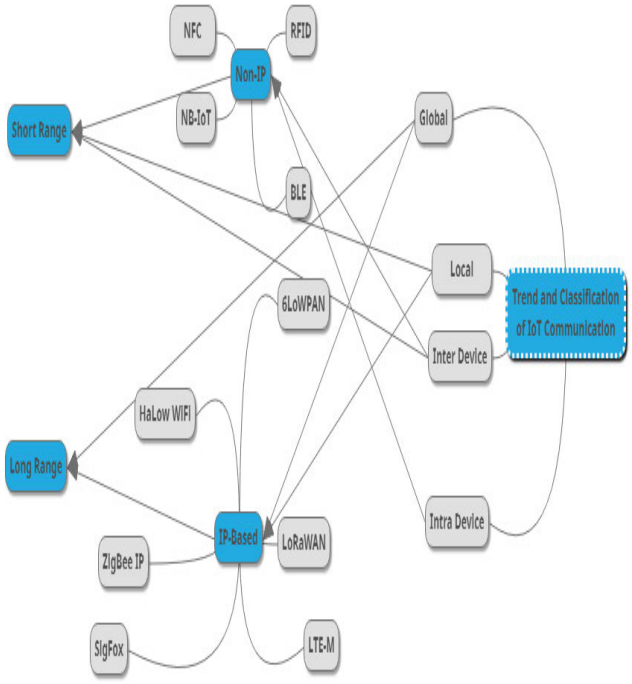


**FIGURE 14.** Classification of IoT communication reviews.

To protect IoT communication from being interrupted and exploited, security needs to be enforced across the architecture layers, from the bottom layer to the top layer. There are several mechanisms that can be applied to ensure security:

- All IoT devices that run on a network should be inclusive with authorize software.
- While operating IoT devices, they need to be authenticated to ensure that they are authorized on the network before transmitting and receiving data.
- Firewall IoT devices to filter packets that directly enter a device is the best approach because of limitation computations and memory capabilities.
- Ensure updates and patches are up to date.

In the heterogeneous dynamic interoperability IoT environment, more devices will be connected and produce a higher attack surface that can be exploited. Hence, IoT architecture, communication and technology development must include security. The applications and services must be robust and highly secure to provide trusted IoT management for scalable heterogeneous smart devices networking. Generally, to protect the privacy of data and prevent spoofing and tampering of data, a system must not depend on other systems for service robustness. Hence, imbedding technologies with secure IoT naming and data scheme is prudent. To ensure that IoT assets are fully functioning with robust services; the communication must be secure from any kind of attack. The trade-offs for availability, privacy, confidentiality, integrity and performance must be carefully deployed without requiring any specialized dependency.

IoT vulnerabilities interrelay with several dimensions. As the number of IoT connections and devices increases, the vulnerabilities also increase. Attacks or security threats are divided into internal or external attacks and can be further described as passive or active attacks. Possible attacks on IoT architecture layers are the jamming attack, tampering attack, exhaustion attack, collision attack, Sybil attack, packets modification attack, sinkhole attack, wormhole attack, spoofing attack, etc. Table 14 summarizes the vulnerabilities and attacks for architecture and technology.

There are several security principles that need to be enforced to defense and secure the communication framework, such as confidentiality, integrity, availability, authentication and manageability. IoT users need to be aware of data management mechanisms, end-to-end security, firewall and protocols of the level of security for architecture and applications. IoT communication must consider data security-centric measures with lightweight security and split buffers that require all content to be protected independently regardless of the destination or source providing and/or storing of all content. Data segmentation into multiple chunks, independently transact and routed with encryption can guarantee the integrity and privacy. The content-oriented security model is theoretically mitigating risk and avoiding certain nodes from being attacked because the address does not exist, hence minimizing vulnerability. This type of security model prevents a network from some of the well-known weaknesses or vulnerabilities caused by the Internet host-centric model of communication.

Fig. 15 shows the mapping classification of IoT security reviews (vulnerabilities, attacks, defense, and mitigation) and the four IoT review areas (technology, architecture, application and communication). While Fig. 16 shows the trend of IoT security reviews. Defense is the most discussed topic followed by mitigation.

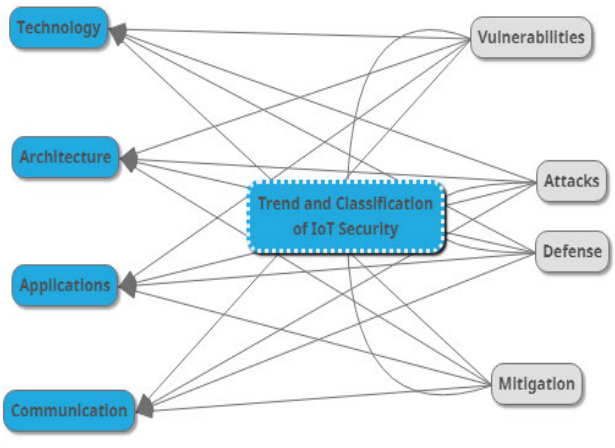


**FIGURE 15.** Classification of IoT security reviews.

This paper introduced 4 classifications of IoT security reviews, namely, attacks, vulnerabilities, defense and mitigation. Attacks and vulnerabilities are interrelated; hence, research is needed to perform penetration testing or ethical attacks to identify possible vulnerabilities. Any new research

**TABLE 14.** IoT categories security.

| Categories | Paper | Vulnerability | Attack |
|---|---|---|---|
| Architecture | [11], [32], [44], [62], [63], [75], [78], [80], [86], [87], [88], [89] [94] | • Device trust management auto connect that assume once a device is authenticated to the network then it is forever a trusted network.<br>• Unlawful device access and authorization by third-party applications. Interception of traffic to and from one or more device by intelligence agencies, allowing manipulation of data<br>• Susceptible to eavesdropping for private or sensitive data<br>• Routing information spoofing in order to manipulate all packets passing through the network.<br>• Selective forwarding, where an attacker may selectively forward packets or simply drop a packet.<br>• Distorting packet behavior to manipulate routing functionality.<br>• Illegal privileges escalation to get authentication and authorization for data access. | Privacy, Eavesdropping attack, Man-in-the-middle attack, Routing attack, Elevation of privilege, Sinkhole attack, Wormhole attack, Sybil attack |
| Technology | [11], [35], [62], [89] | • Erroneous environment physical trust within which the device is placed lead to physical attack to compromise the devices.<br>• Implementation errors or weaknesses including hardcoded credentials, cross-site scripting (XSS), unnecessary open ports, auto-enabled debugging functionality and delivery of private sensitive data in plaintext.<br>• Failure to authenticate remote commands or lack of authentication.<br>• Ignorance for maintenance and updates of firmware and software allowing malicious threats.<br>• Illegal cloning during the manufacturing process by an untrusted factory or compromised for software reverse engineering to allow cloning or modifications.<br>• Implementation of ingenuous device to either reduce the installation and operational costs or to purposely inflict damage. | Distributed Denial of Service (DDoS) attack, Cloning of things, Malicious substitution of thing, Firmware attacks, Extraction of private information |

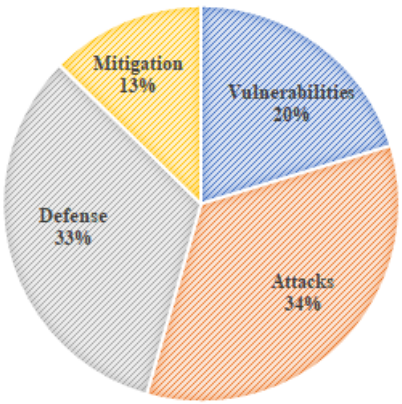


**FIGURE 16.** Trend of IoT security reviews.

for IoT security must consider the dynamic, heterogeneity and interoperability characteristics of the IoT. Future research must also consider light fidelity communication or information-centric networks that have specific data-centered communication, and therefore, are able to minimize network or communication threats and attacks.

## IX. INTERNET OF THINGS CHALLENGES

Ample research on IoT issues and challenges has been performed, as shown in Table 2. The challenges reviews are discussed in the areas of applications, technologies, architectures, and security. Some of the characteristics challenges of IoT are presented in Table 15, such as heterogeneous, dynamic, scalability, and interoperability.

**TABLE 15.** IoT challenges.

| Area | Paper |
|---|---|
| Application | [11], [46], [47] |
| Architecture | [8], [29], [30], [48], [63], [77], [78], [79] |
| Communication | [18], [21], [26], [42], [57], [77], [78], [95], [99] |
| Technology | [8], [20], [25], [45], [63], [77], [79] |
| Security | [15], [16], [19], [42], [44], [54], [57], [63], [76] |

Heterogeneous IoT systems consist of different types of technology, architecture, application, and security mechanism. Hence, to be able to run an IoT system with these specifications blended requires reliable communication in collecting data and decision-making. It is essential to maintain the system's service continuity and delivery, as well as the correct specifications. Communication response time, lossy network, service degradation and other performance issues must be considered. Because the IoT collects sensor data, computation and processes are performed by storage resources. Cloud platforms are the most common storage resources since they offer huge data handling and storage extension flexibility.

Because the IoT devices are energy-constrained devices, they constantly connect and disconnect from the access technology and multihop mobility due to short-range coverage. In global communication, IoT devices are mobile; therefore, devices move freely in the network with dynamic IP addresses. To allow this behavior, routing protocols have

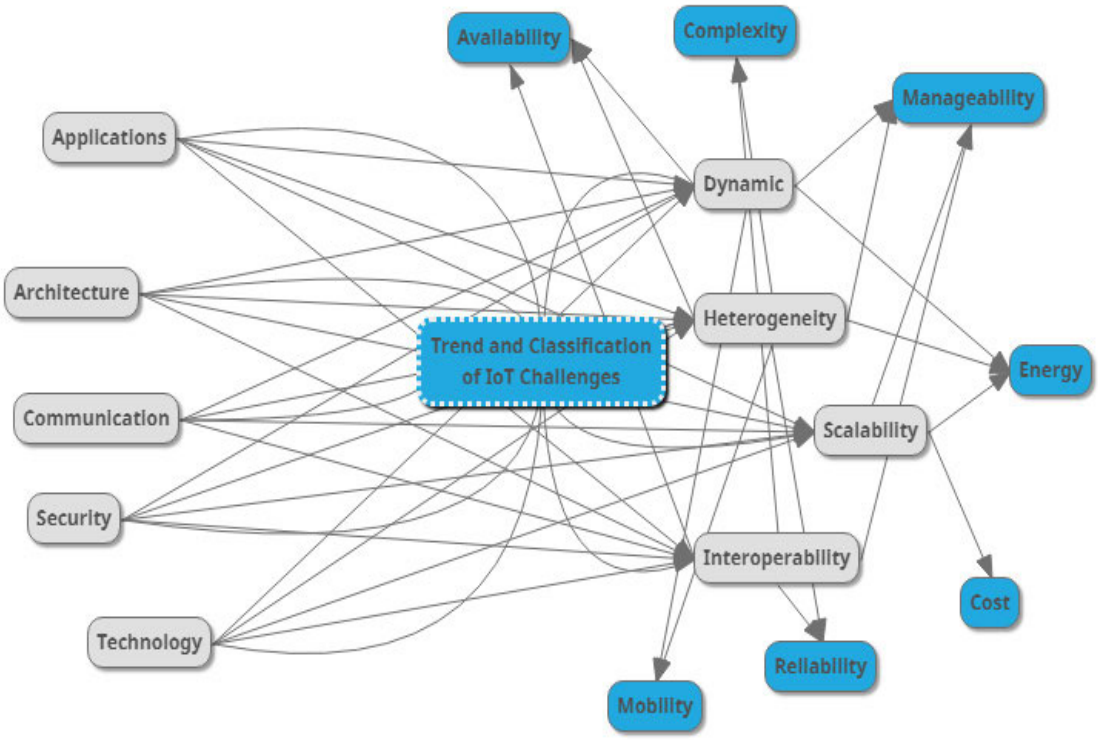


**FIGURE 17.** Classification of IoT challenges reviews.

to reconstruct the routing table for connection and disconnection, which causes network overhead. A change in access technology and service provider adds complexity since services are interrupted due to gateway changes. A unique address name and large space is needed to support vast dynamic IoT devices for addressing and identification.

Scalability is challenging due to the tremendous amount of IoT devices that become connected in a single IoT application. Managing device distribution and functionalities requires extensible operations. In addition to the scalability challenge, integrating protocols and standards is costly and complex; hence, reducing the cost and complexity is a massive challenge that needs to be solved. IoT devices also lack power harvesting technologies. The demand for long battery lifecycles of IoT devices and the requirement to embed or build-in devices complicates battery replacement. Therefore, collecting energy from natural sources, such as the Solar System, is a critical solution.

Interoperability of heterogeneous IoT networking is a challenge because a large number of different technologies, architectures, applications, communication protocols and security mechanisms are employed in IoT systems. Developers and manufacturers must deliver services without dependency to allow interoperability. Protocols are required to manage faults, configuration, accounting, performance and security of interconnected devices. Availability is important for interoperability, since both software and hardware must be accessible and compatible to allow continuous services, even when failures occur. In addition, these communication protocols must be compact enough to be embedded within the constrained IoT devices.

Fig. 17 and Fig. 18 show the classification of IoT challenges reviews according to 5 areas: application, architecture, communication, technology, and security. Fig. 17 highlights various interconnections for the 5 IoT review areas and the significant IoT characteristics (dynamic, heterogeneity, scalability, and interoperability) and challenges (availability, complexity, manageability, energy, cost, reliability, and mobility). As shown in Fig. 18, security and communication has become a controversial area of discussion for IoT challenges as the demand for quality of service in terms of privacy, security and performance increases.

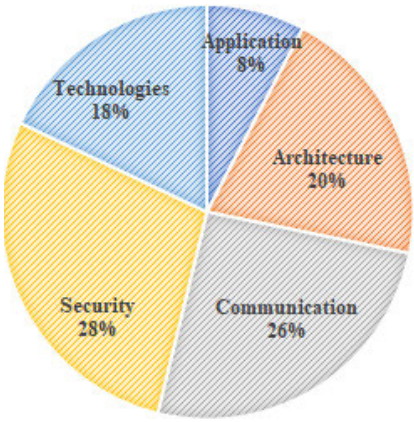


**FIGURE 18.** Trend of IoT challenges reviews.

As IoT research reviews has tremendously increased in the communication area in the last 6 years, [111]–[115] has shown some recent research in IoT application, communication, and technology. The following list details the possible future research trends for the IoT:

1) The technology design of the IoT that fully understands the IoT characteristics and requirements.

2) The paradigm shifts of the IoT communication trend towards information or content-centric networking with emerging of 5G networks.

3) The shift towards IoT applications with virtualized sensors as a service.

4) IoT environment with blockchain technology that focuses on security, networks, and applications.

## X. CONCLUSION

The current IoT reviews and classifications have revealed the next generation research areas. Many reviews and surveys have been conducted in the area of IoT applications, architecture, challenges, communication, technology and security. The IoT characteristics are grouped into four main identities: heterogeneous devices, scalable network, interoperability architecture and dynamic communication. IoT architecture is standardized to three main layers: top, middle and bottom layers. IoT hardware, middleware and cloud platform technologies enable secure, manageable, energy efficient and intelligent services. Among the trend of IoT applications and services are smart homes, smart cities, smart buildings, public safety, intelligence healthcare, smart transportation, smart vehicles, and smart agriculture. Designing an IoT network involves the design of sensors, where the processing, networking capabilities, communication and power consumption depends on the data analytics requested. In IoT networking, power, coverage range and interference are important.

More work is needed to be able to satisfy the global needs, especially in the areas of security, technology, and communications. For communication in the local IoT, the ZigBee protocol is preferable, whereas for global communication, Sigfox or Lora is preferable. The technologies solution must be able to interoperate with different communication protocols; the tradeoff is between the required resource and the provided functions. Several challenges have the potential to slow the development of IoT which include scalability, heterogeneous, dynamic, and interoperability. To reach its full potential, IoT applications must be independent, sensors must be self-sustaining, architecture must be stable, and communication must be secured. Researchers must collaborate to introduce IoT value to human life. This paper has fully represented the current and next trend and classification standard of the IoT.

## ACKNOWLEDGMENT

The authors are grateful to the Faculty of Information Science and Technology, The National University of Malaysia, for all the supports and contributions to this study.

## REFERENCES

[1] Cisco White Paper. Visual Networking Index: Forecast and Trends, 2017–2022, Feb. 2019. Accessed: Jul. 31, 2019. [Online]. Available: https://cyrekdigital.com/pl/blog/content-marketing-trendy-na-rok-2019/white-paper-c11-741490.pdf

[2] O. Garcia-Morchon, S. Kumar, and M. Sethi, *Internet of Things (IoT) Security: State of the Art and Challenges*, document RFC 8576, IRTF, Apr. 2019.

[3] D. Evans, "The Internet of Things: How the next evolution of the Internet is changing everything," Cisco Internet Bus. Solutions Group, CISCO, San Jose, CA, USA, White Paper, Apr. 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[4] R. Irons-Mclean, A. Sabella, and M. Yannuzzi, "IoT and security standards and best practices," in *Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT Book*. Indianapolis, IN, USA: Cisco Press, Jan. 2019.

[5] J. Harrop and P. Harrop, "Internet of Things (IoT) 2017–2027: Things that think: IP addressed sensor node systems," IDTextEx Res., Tech. Rep. [Online]. Available: https://www.idtechex.com/en/research-report/internet-of-things-iot-2017-2027/499

[6] A. A. Aziz, Y. A. Sekercioglu, P. Fitzpatrick, and M. Ivanovich, "A survey on distributed topology control techniques for extending the lifetime of battery powered wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 121–144, Feb. 2013.

[7] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on Internet of Things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, Jan. 2014.

[8] A. M. Ortiz, D. Hussein, S. Park, S. N. Han, and N. Crespi, "The cluster between Internet of Things and social networks: Review and research challenges," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 206–215, Jun. 2014.

[9] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, May 2014.

[10] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[11] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.

[12] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, Nov. 2015.

[13] D. He and S. Zeadally, "An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography," *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.

[14] C. F. Pasluosta, H. Gassner, J. Winkler, J. Klucken, and B. M. Eskofier, "An emerging era in the management of parkinson's disease: Wearable technologies and the Internet of Things," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 6, pp. 1873–1881, Nov. 2015.

[15] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[16] M. Asplund and S. Nadjm-Tehrani, "Attitudes and perceptions of IoT security in critical societal services," *IEEE Access*, vol. 4, pp. 2130–2138, 2016.

[17] D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani, and M. G. Pecht, "IoT-based prognostics and systems health management for industrial applications," *IEEE Access*, vol. 4, pp. 3659–3670, 2016.

[18] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[19] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 453–463, Aug. 2016.

[20] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 70–95, Feb. 2016.

[21] E. Soltanmohammadi, K. Ghavami, and M. Naraghi-Pour, "A survey of traffic issues in machine-to-machine communications over LTE," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 865–884, Dec. 2016.

[22] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[23] I. Khan, F. Belqasmi, R. Glitho, N. Crespi, M. Morrow, and P. Polakos, "Wireless sensor network virtualization: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 553–576, 1st Quart., 2015.
[24] C. A. Tokognon, B. Gao, G. Y. Tian, and Y. Yan, "Structural health monitoring framework based on Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 619–635, Jun. 2017.
[25] F. Alam, R. Mehmood, I. Katib, N. N. Albogami, and A. Albeshri, "Data fusion and IoT for smart ubiquitous environments: A survey," *IEEE Access*, vol. 5, pp. 9533–9554, 2017.
[26] A. Taufique, M. Jaber, A. Imran, Z. Dawy, and E. Yacoub, "Planning wireless cellular networks of future: Outlook, challenges opportunities," *IEEE Access*, vol. 5, pp. 4821–4845, 2017.
[27] H. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey," *IEEE Commun. Surveys Tuts.*, vol. 19., no. 4, pp. 2502–2525, 4th Quart., 2017.
[28] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.
[29] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 269–283, Feb. 2017.
[30] F. K. Shaikh, S. Zeadally, and E. Exposito, "Enabling technologies for green Internet of Things," *IEEE Syst. J.*, vol. 11, no. 2, pp. 983–994, Jun. 2017.
[31] C. M. G. Algora, V. A. Reguera, N. Deligiannis, and K. Steenhaut, "Review and classification of multichannel MAC protocols for low-power and lossy networks," *IEEE Access*, vol. 5, pp. 19536–19561, 2017.
[32] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.
[33] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.
[34] X. Liu, Z. Sheng, C. Yin, F. Ali, and D. Roggen, "Performance analysis of routing protocol for low power and lossy networks (RPL) in large scale networks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2172–2185, Sep. 2017.
[35] K. Bu, M. Weng, Y. Zheng, B. Xiao, and X. Liu, "You can clone but you cannot hide: A survey of clone prevention and detection for RFID," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1682–1700, 3rd Quart., 2017.
[36] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *J. Netw. Comput. Appl.*, vol. 97, pp. 48–65, Nov. 2017.
[37] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the Internet of Things: Big challenges and new opportunities," *Comput. Netw.*, vol. 112, pp. 237–262, Jan. 2017.
[38] J. M. Talavera, L. E. Tobón, J. A. Gómez, M. A. Culman, J. M. Aranda, D. T. Parra, L. A. Quiroz, A. Hoyos, and L. E. Garreta, "Review of IoT applications in agro-industrial and environmental fields," *Comput. Electron. Agricult.*, vol. 142, no. 1, pp. 283–297, 2017.
[39] I. Chew, D. Karunatilaka, C. P. Tan, and V. Kalavally, "Smart lighting: The way forward? Reviewing the past to shape the future," *Energy Buildings*, vol. 149, pp. 180–191, Aug. 2017.
[40] A. Ali, G. A. Shah, M. O. Farooq, and U. Ghani, "Technologies and challenges in developing machine-to-machine applications: A survey," *J. Netw. Comput. Appl.*, vol. 83, pp. 124–139, Apr. 2017.
[41] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 39–95, 1st Quart., 2018.
[42] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
[43] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A survey on network security-related data collection technologies," *IEEE Access*, vol. 6, pp. 18345–18365, 2018.
[44] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3496–3509, 4th Quart.,2018.
[45] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2923–2960, 4th Quart., 2018.
[46] F. Javed, M. K. Afzal, M. Sharif, and B. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2062–2100, 3rd Quart., 2018.
[47] S. Pattar, R. Buyya, K. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Searching for the IoT resources: Fundamentals, requirements, comprehensive review, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2101–2132, 3rd Quart., 2018.
[48] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.
[49] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 847–870, Apr. 2018.
[50] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, "A reference model for Internet of Things middleware," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 871–883, Apr. 2018.
[51] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, "Context-aware computing, learning, and big data in Internet of Things: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 1–27, Feb. 2018.
[52] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, "Ble beacons for Internet of Things applications: Survey, challenges, and opportunities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 811–828, Jan. 2018.
[53] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77454–77473, 2018.
[54] L. He, Z. Yan, and M. Atiquzzaman, "LTE/LTE-A network security data collection and analysis for security measurement: A survey," *IEEE Access*, vol. 6, pp. 4220–4242, 2018.
[55] Y. Miao, W. Li, D. Tian, M. S. Hossain, and M. F. Alhamid, "Narrowband Internet of Things: Simulation and modeling," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2304–2314, Aug. 2017.
[56] N. Choudhury, R. Matam, M. Mukherjee, and L. Shu, "Beacon synchronization and duty-cycling in IEEE 802.15.4 cluster-tree networks: A review," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1765–1788, Jun. 2018.
[57] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
[58] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on human-centered IoT-connected smart labels for the industry 4.0," *IEEE Access*, vol. 6, pp. 25939–25957, 2018.
[59] M. O. Ojo, S. Giordano, G. Procissi, and I. N. Seitanidis, "A review of low-end, middle-end, and high-end IoT devices," *IEEE Access*, vol. 6, pp. 70528–70554, 2018.
[60] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32258–32285, 2018.
[61] J. J. P. C. Rodrigues, D. B. De Rezende Segundo, H. A. Junqueira, M. H. Sabino, R. M. Prince, J. Al-Muhtadi, and V. H. C. De Albuquerque, "Enabling technologies for the Internet of health things," *IEEE Access*, vol. 6, pp. 13129–13141, 2018.
[62] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.
[63] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, Oct. 2018.
[64] B. N. Silva, M. Khan, and K. Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustain. Soc.*, vol. 38, pp. 697–713, Apr. 2018.
[65] O. Salman, I. Elhajj, A. Chehab, and A. Kayssi, "IoT survey: An SDN and fog computing perspective," *Comput. Netw.*, vol. 143, pp. 221–246, Oct. 2018.
[66] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[67] S. A. Shah, D. Z. Seker, M. M. Rathore, S. Hameed, S. B. Yahia, and D. Draheim, "Towards disaster resilient smart cities: Can Internet of Things and big data analytics be the game changers?" *IEEE Access*, vol. 7, pp. 91885–91903, 2019.

[68] A. M. Alberti, M. A. S. Santos, R. Souza, H. D. L. Da Silva, J. R. Carneiro, V. A. C. Figueiredo, and J. J. P. C. Rodrigues, "Platforms for smart environments and future Internet design: A survey," *IEEE Access*, vol. 7, pp. 165748–165778, 2019.

[69] L.-M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, "Deployment of IoV for smart cities: Applications, architecture, and challenges," *IEEE Access*, vol. 7, pp. 6473–6492, 2018.

[70] F. A. Awin, Y. M. Alginahi, E. Abdel-Raheem, and K. Tepe, "Technical issues on cognitive radio-based Internet of Things systems: A survey," *IEEE Access*, vol. 7, pp. 97887–97908, 2019.

[71] S. O. Olatinwo and T. Joubert, "Enabling communication networks for water quality monitoring applications: A survey," *IEEE Access*, vol. 7, pp. 100332–100362, 2019.

[72] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin, and U. M. Mbanaso, "Low-power wide area network technologies for Internet-of-Things: A comparative review," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2225–2240, Nov. 2019.

[73] Z. Ma, M. Xiao, Y. Xiao, Z. Pang, H. V. Poor, and B. Vucetic, "High-reliability and low-latency wireless communication for Internet of Things: Challenges, fundamentals, and enabling technologies," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7946–7970, Oct. 2019.

[74] M. Ghorbanian, S. H. Dolatabadi, M. Masjedi, and P. Siano, "Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures," *IEEE Syst. J.*, vol. 13, no. 4, pp. 4001–4014, Sep. 2019.

[75] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[76] N. Koroniotis, N. Moustafa, and E. Sitnikova, "Forensics and deep learning mechanisms for Botnets in Internet of Things: A survey of challenges and solutions," *IEEE Access*, vol. 7, pp. 61764–61785, 2019.

[77] I. U. Din, M. Guizani, S. Hassan, B. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019.

[78] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Sep. 2019.

[79] M. Aly, F. Khomh, Y.-G. Guéhéneuc, H. Washizaki, and S. Yacout, "Is fragmentation a threat to the success of the Internet of Things?" *IEEE Internet Things J.*, vol. 6, no. 1, pp. 472–487, Feb. 2019.

[80] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019.

[81] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[82] P. Fraga-Lamas and T. M. T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.

[83] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Jumaat, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of Internet of Things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019.

[84] M. Fahim and A. Sillitti, "Anomaly detection, analysis and prediction techniques in IoT environment: A systematic literature review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019.

[85] K. Riad, R. Hamza, and H. Yani, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86384–86393, 2019.

[86] V. Nguyen, P. Lin, and R. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915–51932, 2019.

[87] M. Malik, M. Dutta, and J. Granjal, "A survey of key bootstrapping protocols based on public key cryptography in the Internet of Things," *IEEE Access*, vol. 7, pp. 27443–27464, 2019.

[88] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2671–2701, 3rd Quart., 2019.

[89] W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain technology for applications in Internet of Things—Mapping from system design perspective," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8155–8168, Oct. 2019.

[90] C. Li and B. Palanisamy, "Privacy in Internet of Things: From principles to technologies," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 488–505, Aug. 2019.

[91] B. Pourghebleh, K. Wakil, and N. J. Navimipour, "A comprehensive study on the trust management techniques in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9326–9337, 2019.

[92] T. Alladi, V. Chamola, R. M. Parizi, and K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019.

[93] B. Qolomany, A. Al-Fuqaha, A. Gupta, D. Benhaddou, S. Alwajidi, J. Qadir, and A. C. Fong, "Leveraging machine learning and big data for smart buildings: A comprehensive survey," *IEEE Access*, vol. 7, pp. 90316–90356, 2019.

[94] A. Raoof, A. Matrawy, and C. Lung, "Routing attacks and mitigation methods for RPL-based Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1582–1606, 2nd Quart., 2019.

[95] S. S. Anjum, R. M. Noor, M. H. Anisi, I. B. Ahmedy, F. Othman, M. Alam, and M. K. Khan, "Energy management in RFID-sensor networks: Taxonomy and challenges," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 250–266, Feb. 2019.

[96] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning-based network vulnerability analysis of industrial Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6822–6834, 2nd Quart., 2019.

[97] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[98] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of Things: A comprehensive investigation," *Comput. Netw.*, vol. 160, pp. 165–191, Sep. 2019.

[99] A. Khanna and S. Kaur, "Evolution of Internet of Things (IoT) and its significant impact in the field of precision agriculture," *Comput. Electron. Agricult.*, vol. 157, no. 1, pp. 218–231, 2019.

[100] M. Abujubbeh, F. Al-Turjman, and M. Fahrioglu, "Software-defined wireless sensor networks in smart grids: An overview," *Sustain. Cities Soc.*, vol. 51, Sep. 2019, Art. no. 101754.

[101] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols: Review," in *Proc. 8th Int. Conf. Inf. Technol. ICIT)*, Amman, Jordan, 2017, pp. 685–690, doi: 10.1109/ICITECH.2017.8079928.

[102] I. U. Din, H. Asmat, and M. Guizani, "Review of information centric network-based Internet of Things: Communication architectures, design issues, and research opportunities," *Multimedia Tools Appl.*, vol. 78, pp. 30241–30256, Dec. 2019, doi: 10.1007/s11042-018-6943-z.

[103] A. Souri, A. Hussien, M. Hoseyninezhad, and M. Norouzi, "A systematic review of IoT communication strategies for an efficient smart environment," *Trans Emerg. Tel Tech.*, p. e3736, 2019. [Online]. Available: https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2Fett.3736, doi: 10.1002/ett.3736.

[104] A. Souri and M. Norouzi, "A state-of-the-art survey on formal verification of the Internet of Things applications," *J. Serv. Sci. Res.*, vol. 11, pp. 47–67, 2019, doi: 10.1007/s12927-019-0003-8.

[105] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017, doi: 10.1109/MIE.2017.2649104.

[106] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[107] *IEEE Xplore*. Accessed: Jan. 15, 2020. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[108] *Science Direct*. Accessed: Jan. 15, 2020. [Online]. Available: https://www.sciencedirect.com/search

[109] *IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)*, Standard IEEE P2413/D0.4.5, Dec. 2018, pp. 1–264.

[110] *IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)*, Standard IEEE P2413/D0.4.6, Mar. 2019, pp. 1–265.

[111] H. M. Jawad, A. M. Jawad, R. Nordin, S. K. Gharghan, N. F. Abdullah, M. Ismail, and M. J. A.-A. Shaeer, "Accurate empirical path-loss model based on particle swarm optimization for wireless sensor networks in smart agriculture," *IEEE Sensors J.*, vol. 20, no. 1, pp. 552–561, Jan. 2020.
[112] A. M. Jawad, H. M. Jawad, R. Nordin, S. K. Gharghan, N. F. Abdullah, and M. J. Abu-AlShaeer, "Wireless power transfer with magnetic resonator coupling and sleep/active strategy for a drone charging station in smart agriculture," *IEEE Access*, vol. 7, pp. 139839–139851, 2019.
[113] M. S. Islam, M. T. Islam, M. A. Ullah, G. K. Beng, N. Amin, and N. Misran, "A modified meander line microstrip patch antenna with enhanced bandwidth for 2.4 GHz ISM-band Internet of Things (IoT) applications," *IEEE Access*, vol. 7, pp. 12785–12786, 2019.
[114] H. Bello, Z. Xiaoping, R. Nordin, and J. Xin, "Advances and opportunities in passive wake-up radios with wireless energy harvesting for the Internet of Things applications," *Sensors*, vol. 19, no. 14, p. 3078, 2019.
[115] M. H. Homaei, E. Salwana, and S. Shamshirb, "An enhanced distributed data aggregation method in the Internet of Things," *Sensors*, vol. 19, no. 14, p. 3173, 2019.

**AZANA HAFIZAH MOHD AMAN** received the B.Eng., M.Sc., and Ph.D. degrees in computer and information engineering from International Islamic University Malaysia, Malaysia. She is currently working as Senior Lecturer at the Research Center for Cyber Security, Faculty of Information Science and Technology (FTSM), The National University of Malaysia, Malaysia. Her research interests include computer system and networking, computer information and network security, the Internet of Things (IoT), cloud computing, and big data.

**ELAHEH YADEGARIDEHKORDI** received the Ph.D. degree in information systems from Universiti Teknologi Malaysia (UTM), Malaysia. Her research interests include tourism management, cloud computing, the Internet of Things (IoT), mobile learning, and big data. Her contributions have been published in prestigious peer-reviewed journals and international conferences.

**ZAINAB SENAN ATTARBASHI** received the B.Sc. degree in electronic and computer engineering and the M.Sc. and Ph.D. degrees in information and computer engineering from International Islamic University Malaysia. She is currently a Senior Lecturer of computer networking with the School of Computing, Universiti Utara Malaysia. Her current research interests include cyber security, info-centric networks, network mobility, and the Internet of Things (IoT) connectivity.

**ROSILAH HASSAN** (Senior Member, IEEE) received the B.Sc. degree in electronic engineering from Hanyang University, South Korea, the master's degree in electrical engineering from Universiti Kebangsaan Malaysia, Malaysia, and the Ph.D. degree in mobile communication from the University of Strathclyde, U.K., in May 2008. She is currently an Associate Professor with the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia. Her research interests include mobile communications, networking, the Internet of Things (IoT), and big data. She is also an Active Member of the MySET and IET.

**YONG-JIN PARK** (Life Senior Member, IEEE) was involved in research and education with Hanyang University, Seoul, for over 30 years, where he became the Professor Emeritus, in 2010. He joined Waseda University, in 2010. He was the President of the Korea Institute of Information Scientists and Engineers, in 2003, the Director of Secretariat of Asia Pacific Advanced Network, from 1999 to 2003, and also the President of the Open Systems Interconnection Association, from 1991 to 1992. He visited the Department of Computer Science, University of Illinois at Urbana–Champaign, as a Visiting Associate Professor, from 1983 to 1984. He also visited the Computing Laboratory, University of Kent, Canterbury, U.K., from 1990 to 1991, as a Research Fellow. He is currently a Professor with the University of Malaysia Sabah. He was the IEEE Region 10 Director and a member of the IEEE Board of Directors, from 2009 to 2010. He is also a member of the IEEE MGA Nominations Appointments Committee, the IEEE Region 10 Advisory Committee, and the IEEE Japan Council Executive Committee. He is an IEICE Fellow.