IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 8 January 2023, accepted 24 February 2023, date of publication 28 February 2023, date of current version 6 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3250466

SURVEY

A Review on the Immediate Advancement of the Internet of Things in Wireless Telecommunications

KAMALRULNIZAM BIN ABU BAKAR[1], FATIMA TUL ZUHRA[2], BABANGIDA ISYAKU[1,3], AND SAPIAH BINTI SULAIMAN[4]

[1]Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia
[2]Department of Information Technology, Faculty of Science and Technology, Shaheed Benazir Bhutto University, Sanghar Campus, Sanghar 67450, Pakistan
[3]Department of Computer Science, Faculty of Computing and Information Technology, Sule Lamido University, Kano, Jigawa 700271, Nigeria
[4]Research Management Centre, Universiti Teknologi Malaysia, Johor Bahru, Johor 81310, Malaysia

Corresponding authors: Babangida Isyaku (Isyaku.babangida@utm.my) and Fatima Tul Zuhra (drfatima.tunio_sng@sbbusba.edu.pk)

This work was supported by the Universiti Teknologi Malaysia under Post-Doctoral Fellowship Scheme through Grant Q.J130000.21A2.06E03 and Q.J130000.2409.08G77.

ABSTRACT Internet of Things is emerging as an incredible future technology to improve the existing lifestyle from the research community, industry, and the public sector. The main intention of IoT is to create an efficient, interactive, and autonomous infrastructure for a safer and healthier world. Moreover, it grows faster day-to-day with the support of many other technologies, i.e. Cloud computing, Blockchain, Wireless Body Sensor Networks, Nanotechnology, and Artificial Intelligence for smart applications, including healthcare, environment, automotive industries, transportation, agriculture, etc. Nevertheless, managing big data is one of the challenging tasks due to the increased number of devices leading to various serious issues like security, privacy, accuracy, latency, scheduling, etc. Further, specific infrastructures with remarkable techniques are required to analyze the bulk of raw data to progress the quality of life and allow timely intervention through various capabilities, i.e., data capture, unique identification, actuation, communication, data mining, etc. In past literature, numerous reviews/surveys are presented that explore the technologies mentioned above as standalone and application specific. However, this paper aims to integrate all the mentioned technologies and deliver a clear vision to future researchers (*newcomers*) as a kick-start article to boost up and understand the status of the existing research through a comprehensive review of the Internet of Things and its evolution in wireless telecommunications from a general perspective. The most significant challenges and issues are highlighted to research further in these evolving domains.

INDEX TERMS Internet of Things, cloud computing, blockchain, artificial intelligence, wireless body sensor networks, nanotechnology.

I. INTRODUCTION

Industry 4.0 is a business paradigm introduced by the German government [1] that modernizes the way emerging technologies are being used in various application domains (such as healthcare, manufacturing, cybersecurity, system integration, robotics, cloud connectivity, retailing, etc.) based on the real-time data and connectivity [2], [3]. In industry 4.0, the Internet of Things (IoT) is a foundation for constructing industrial systems with numerous applications to enhance productivity and performance with less human error. IoT is a revolutionary technology that refers to a wireless network of interconnected devices that signifies the future of communication, computing, and intelligence. IoT is revealed as one of the ultimate expansions in the modern age, due to its speedy evolution in different fields. Long ago, from a computing perspective, only one system could perform a specified task. However, several systems were required for concurrent tasks. Throughout the years, various computing paradigms have been invented, from the client-server to IoT/Cloud-Fog/Edge

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

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

computing, that extensively contributes to the field of computing. In addition, the Internet plays a very significant role in our life by replacing the old manual systems with innovative automatic systems without human intervention.

Nevertheless, the entire network was communication and intelligence restricted. These restrictions somehow fade with IoT's speedy growth in different fields. Moreover, several technologies have become popular with the evolvement of IoT to promote global facilities and goods manufacturing networks in a variety of fields such as military, academia, industry/automotive industries (Industrial Internet of Things (IIoT)) [4], medical system [5], intelligent transportation systems [6], [7], smart grid [8], smart home [9], [10], smart cities [11], government, environment, security [12], [13] and agriculture [14], [15].

Wireless telecommunication is the electronic medium that permits these networks of physical objects to interchange data. Integrating the IoT and cloud computing, the Cloud of Things (CoT) provides high-quality, cost-effective, and ubiquitous services to extensive applications, i.e. healthcare and video surveillance. This way, the cloud infrastructure is an intermediate layer between the applications and things. It supports a system by which the billions of these IoT devices at the IoT layer upload their data to the cloud at the cloud layer to achieve a variety of on-demand services at the access layer. The amount of data is going through extremely fast growth; therefore, storing and processing big data is challenging as it increases with the number of devices. In this regard, security concern is considered a major cloud-based IoT network problem [12], [13]. However, inadequate security measures can result in data confidentiality, device authentication, and inappropriate system use. Although, integrating Blockchain with IoT has improved data transmission over the cloud. The rapid advancement of IoT in several domains also introduces research challenges strongly interrelated to the nature of IoT technology and makes them convenient, safe, healthy, comfortable, and economical [9], [16], [17], [18]. Over the years, Artificial Intelligence techniques have been used to implement security mechanisms for many emerging technology, including cloud and Blockchain. Integrating IoT and AI play a very important role in devising security mechanisms and providing accurate analysis by offering an intellectual and decision-making facility for a device to humans in IoT applications. Integrating IoT and Wireless Body Area Networks (WBAN) is also among the trending IoT research area. WBAN consist of various wearable sensors, which are the things from the network that poses other routing challenges due to their limited resource constraint. Quality of Service (QoS), heterogeneous data traffic load, quality of a transmission link, end-to-end delay, energy consumption, path loss, and network lifetime are the most common issues and challenges of a WBAN. A wide variety of routing protocols has been proposed in past literature to address these concerns. A thermal-aware, cluster-based, postured-based, QoS-aware, security-aware, and cross-layered are among the widely used solution in literature.

Conversely, various AI techniques have been implemented by many researchers in their IoT projects in CoT and Blockchain technology. However, AI faces challenges like resource constraints, artificial trust, privacy, centralized architecture, and insufficient training data. These challenges are the motive for this review paper.

This paper presents a comprehensive review of IoT technology and its evolution in wireless telecommunications from a general perspective to address this limitation. It conveys a clear vision to future researchers (*newcomers*) as a kick-start article to boost up and understand the status of the existing research. The basic idea behind this concept is the pervasive presence around us of a variety of things or objects - such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, and so on - that can interact with each other and cooperate with their neighbours to achieve common goals through unique addressing schemes. The review article briefly describes the entire concept of IoT technology.

Moreover, the different integrations of IoT are investigated to see how this technology shows a significant role emerging with cloud computing, blockchain, AI, Wireless Body Sensor Networks (WBSN), and nanotechnology in unbeatable/strong implementation of IoT-based networks via the most relevant literature. The most significant challenges and issues are highlighted that are still open for future research. The rest of the paper is organized as follows. Section II details the background of IoT technology. Section III reports the growth of IoT with different emerging technologies. Section IV summarizes the overall advancements of IoT with a discussion. Section V lists the most significant research challenges and issues. Finally, the conclusion of this paper is presented in Section VI.

II. BACKGROUND OF THE INTERNET OF THINGS

Kevin Ashton originally introduced the concept of the IoT in 1999 as ''uniquely identifiable interoperable connected things/objects with Radio Frequency Identification (RFID) technology'' [19]. Typically, IoT is a real-time and self-configuring Wireless Sensor Network (WSN) based on the numerous physical (sensing and monitoring) devices of different capabilities and sizes, such as vehicles, fitness trackers, smart motorbikes, security systems, computers, smart fire alarms, mobile phones, smart watches, medical sensors, RFID tags, actuators, smart door lock, electronic appliances, etc [14], [15], [20], [21], [22], [23]. These devices are interconnected via the Internet for a consistent appearance of the actual world to the alphanumeric world regarding data flow. This tendency is expected to speed up the future due to the maturity of Internet technology and network cost and hardware reduction. IoT grows with a 5-Generation (5G) wireless network to provide a wide variety of services around the world with increased data transmission rate and large-scale connections (10-100 times), communication capacity (1000 times), user experience, and lower cost and end-to-end delay (less than 1 ms) respectively [4], [24]. However, 6G (in early stages/will commercially launch in 2030) will

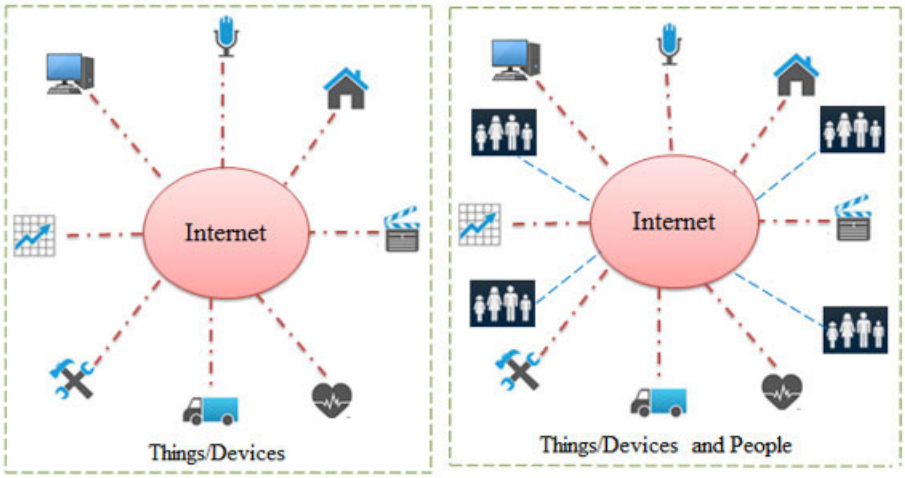

FIGURE 1. (a) Infrastructure of the IoT and (b) IoE.

fulfil the future expectations of IoT and overcome the limitations of the 5G network (will not support advanced IoT applications, i.e. virtual, augmented, and mixed realities) by providing full-dimensional wireless coverage, connections, and functions including caching, computing, communication, control, sensing, imaging, navigation, positioning [25].

Moreover, a Wireless Sensor Network (WSN) is a group of distributed sensor nodes with various capabilities, such as perceiving and transmitting raw sensor readings in various applications such as smart healthcare, city, grid, home automation, and supply chain. The entire layout of the network architecture of IoT is categorized as physical/sensing/perception, application/web, and network layer [26], [27], [28], [29], [30], [31]; however, some researchers have added two more layers, such as the business and middleware layer [32], [33]. The perception is the bottommost layer, further categorized as a perception network and nodes (controllers, sensors, gateways, etc.). All the data is obtained and handled at the perception node, whereas the control instructions are passed to the perception network. The intermediate network layer acts as a transmission medium (wired/wireless) which connects the perception and middleware layers via different connection protocols such as IPv6, 3-5G, etc. The middleware layer stores the data (obtained from the network layer) in the database and is responsible for service management. The application layer allocates global management to the end-users via web-based software/systems or mobile phones. It helps the end-users achieve a smarter lifestyle, business, healthcare, environment, home, city, transportation and automobiles, disaster management, social and entertainment system, etc. Besides, the topmost business layer manages the entire IoT system involving services and applications based on the obtained data from the application layer by constructing business plans, graphs, models, flowcharts, future business strategies, and actions.

Referring to Figure 1(a-b), IoT provides the Machine-to-Machine (M2M) interaction with short-range and long-range wireless technologies (such as ZigBee, Bluetooth, WiFi, Low Power Wide Area (LPWA)) by which the IoT devices have remotely interacted (connect, sensed and communicate) with each other via a network infrastructure and makes a more informed decision regarding the provision of the services via autonomous communication [9], [34], [35], [36], [37], [38], [39]. Moreover, the standard protocols of IoT networks are categorized based on application, service discovery, and infrastructure [40]. The application protocols are Message Queue Telemetry Transport (MQTT), Data Distribution Service (DDS), Extensible Messaging and Presence Protocol (XMPP), Constrained Application Protocol (CoAP), and Advanced Message Queuing Protocol (AMQP). Service discovery protocols are Domain Name Service – Service Discovery (DNS-SD) and Multicast DNS (MDNS). In contrast, the infrastructure protocols are Bluetooth Low Energy (BLE), IEEE 802.15.4, 6LowPAN, Routing Protocol for low power and Lossy networks (RPL), Long Term Evolution-Advanced (LTE-A), and Electronic Product Code-global (EPC). With the help of IoT, anyone can access anything or any service at any time and place using an Internet connection. However, the Internet of Everything (IoE) is one of the extended versions of IoT, which consists of things, data, people, and processes [41], [42]. In IoE, multidimensional devices are interconnected via the Internet involving People-to-People (P2P), M2M, and People-to-Machine (P2M) communication. People send and receive valuable information by using IoT-based devices/things over the Internet and might be unaware of available services, resources, and capabilities [43]. Moreover, IoT resource allocation corresponds to (i) things/nodes, i.e. storage capacity, computational resources, and energy resources, and (ii) communication channel i.e. load balancer, channel bandwidth, and traffic analyzer.

Furthermore, IoE extracts and examines the real-time data from various interconnected sensor nodes and is accessed online through cloud computing to fulfil the desired objectives [44], [45]. However, in IoT-based applications, managing (storing or processing) big data is one of the challenging tasks as it increases with the number of devices. Initially, big data was characterized by only one dimension, i.e. size, over the time it has been characterized by more than one dimension of big data analytics, such as (i) variety (structural heterogeneity), volume (magnitude), and velocity (data rate at which it is being generated and transmitted) [46], (ii) variability and complexity, veracity (accuracy) and value (attribute like low or high density) [47], (iii) volume, value, variety, and velocity [48] and (iv) variety, value, volume, variety, velocity, variability, and complexity [49] respectively. Since IoT devices assemble a substantial amount of data in a centralized form, which is being stored, processed, and transmitted by the IoT-based systems, these serious issues are caused, i.e., security, privacy, accuracy, latency, and management or scheduling.

There are a great number of survey and review papers presented in past literature. Some of them are presented in Table 1, which highlights, summarizes, and compares the existing articles with this article. These papers are application and technology-specific and explore various IoT applications, including IoT integration with cloud-Fog computing, blockchain, WSN/WBSN, AI, and nanotechnology. The majority of the integrated cloud-Fog-based IoT (FIoT) networks are reviewed in past literature that includes their architecture, applications, issues, challenges, and future directions, for instance, energy efficiency, resource allocation, protocol support, identity management, excessive data communication, etc. [50], [51], [52], [53], [54], [55], [56], [57], [58]. Researchers focus on security issues in blockchain-based IoT infrastructure and review various attacks and threats, blockchain solutions, and open challenges [12], [35], [59], [60]. State-of-the-art machine learning-powered techniques and security systems are presented in [28].

Furthermore, the IoT network is integrated with robotic technology and AI techniques [61]. This review paper explored AI, hypoconnectivity, converging sensing/actuating, and various issues and challenges of the Internet of Robotic Things (IoRT). On the other hand, IoT is integrated with wireless networks as IoMT [62], [63], [64], [65]. These review papers explore the hardware designs of sensors as emerging trends, issues, and challenges of wireless networks and various privacy and security attacks in IoMT infrastructure.

In addition, Al-Turjman [66] presents a survey on integrating IoT, AI and nanotechnology as IoNT that includes its overview, architecture, design factors, applications, and limitations from security in a big 5G network perspective. A review of loT, IoE, and IoNT that describes their basic concepts, issues, and challenges were presented in [42], [67]. Nayyar et al. [68] reviewed the entire concept of nano-networks and nano-machines. While the work in [69] details the concept, issues, challenges, and applications of nano-networks are reviewed from a big data perspective. A terahertz communication with MAC protocol is reviewed at nanoscale and macroscale networks [70], [71]. Besides, terahertz band communication systems are reviewed consisting of design, applications, issues, challenges, and current development [72], [73], [74].

While researchers are better with time, there is a lack of sufficient survey papers to incorporate the integration of IoT with several emerging technologies. In contrast to the existing papers, this work paper survey the integration of IoT cloud, fog computing, Blockchain, WBAN, AI, and Nanotechnology on different applications.

III. GROWTH OF INTERNET OF THINGS NETWORK

IoT is emerging and gaining more popularity with existing technologies to improve personal, social, and professional life. However, the characterization or definition of IoT may vary from technology to technology, while integration depends on their implementations. Each object is uniquely identified in the virtual depictions, and the data can be exchanged and processed frequently according to predefined techniques. Figure 2 shows the integrations of IoT and incredible technologies for smart applications described in detail in subsequent subsections.

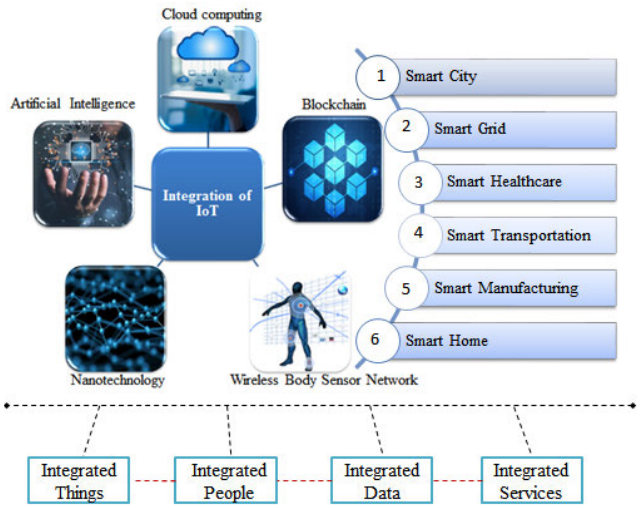

FIGURE 2. Integration of IoT and incredible technologies.

A. INTEGRATION OF IOT AND CLOUD COMPUTING

Cloud computing technology is an advanced computing services framework that provides the Internet-based distributed on-demand infrastructure to carry out higher-level services based on the user's requirements. It facilitates the innovative generation of applications by enabling suitable and pervasive on-demand network access (resources) to the computing developers (for instance, systems, servers, and storage utilities) with high performance and bandwidth and low latency and cost services. Moreover, a cloud is a huge space or

TABLE 1. Comparison with the existing review papers.

Author/Reference	IoT	Cloud-Fog Computing	Blockchain	WSN/WBSN	AI	Nanotechnology	Technological Aspect	Application Specific	Focused Area	
Aazam et al. [50-52]		✓	×	×	×	×				
Botta et al. [53]		✓	×	×	×	×	CoT/FoT		Integration of IoT and Cloud/Fog-computing	Concept, applications, issues and challenges
Stergiou et al. [56]		✓	×	×	×	×				
Dang et al. [57]		✓	×	×	×	×				
Sengupta et al. [12]	✓	×	✓	×	×	×	BCoT	✓	Integration of IoT and Blockchain	Security attacks and threats
Khan & Salah [35]		×	✓	×	×	×				
Fernandez-Carames & Paula Fraga-Lamas [59]		×	✓	×	×	×				
Ferrag et al. [60]		×	✓	×	×	×				
Tahsein et al. [26]		×	×	×	✓	×	AI+IoT		Integration of IoT and AI-machine learning	
Vermesan et al. [61]		×	×	×	✓	×	IoRT		Integration of IoT, AI, and Robot sensing/actuating, and hypoconnectivity	Concept, issues and challenges
Manogaran et al. [62]		×	×	✓	×	×	IoMT		Integration of IoT and Wireless Sensor Networks	Concepts, applications, sensor designs, and privacy and security attacks
Alsubaei et al.[63]		×	×	✓	×	×				
Al-Turjman et al. [64]		×	×	✓	×	×				
Qureshi & Krishnan [65]		×	×	✓	×	×				
Al-Turjman [66]		×	×	×	✓	✓	AI+IoNT		Integration of IoT and AI, and Nanotechnology	Intelligence, security attacks and privacy
Rizwan et al. [69]		×	×	×	×	✓	IoNT		Integration of IoT and Nanotechnology	Concept, application requirements, issues and challenges of nano-machines and terahertz band
Miraz & Ali [42, 67]		×	×	×	×	✓				
Nayyar et al. [68]		×	×	×	×	✓				
Ghafoor et al. [70, 71]		×	×	×	×	✓				

TABLE 1. *(Continued.)* **Comparison with the existing review papers.**

This work	✔	✔	✔	✔	✔	✔	All	×	Integration of IoT and cloud computing, blockchain, AI, WBSN, and nanotechnology	communication Concept, architectures, platforms, issues and challenges based on each integration with existing literature, and open issues for future research

collection of datacenters categorized into different deployment models such as private, public, hybrid, and multi-cloud [75], [76]. For instance, a private cloud is a copyrighted network that constructs and upholds its reserved underlying cloud infrastructure. This data centre provides the hosted service with restricted access and authenticates permission settings to the limited subscriptions.

Cloud computing refers to the data processing, storing, and programming over the Internet by infusing more and more as a bonus into various aspects of our daily life (web services like searching, email, websites, Microsoft office 365, calendar, backup, streaming, video and photo storage, automatic updates, online education and many more). In contrast, a public cloud sells services to all users available online. A hybrid cloud combines public and private clouds, whereas a multi-cloud combines multiple private, public, and hybrid clouds. However, few most significant services are provisioned by cloud technology, such as software, hardware, infrastructure, platform, and function as a service [77], [78], [79], [80], [81].

Several organizations, companies, and individual developers use the cloud to store data and access various services. Some of the most famous companies, like Amazon, Google, and Microsoft, organize their data centres (as hardware services) to support their business and provide purchasable services. Moreover, Software service is typically termed Software as a Service (SaaS) that facilitates the online application based on subscriptions by hosting different software in the cloud infrastructure where everything is managed online via a cloud provider. The Infrastructure as a Service (IaaS) service, also called cloud hosting, provides services on rent, i.e., operating systems, storage, servers, networks, and a virtual machine by which many customers can share one partition in a server while the Platform as a Service (PaaS) provides a database, operating system, and all significant supporting application software for testing, developing, managing, and delivering. For instance, creating mobile or web apps quickly, accessing the libraries, and controlling the setup settings of the software.

Nevertheless, the Function as a Service (FaaS) is provisioned during task execution. In [82], the entire concept of the genomics cloud is presented along with its design, implementation, computing, storage, and analysis software. In addition, a technical solution is also proposed for constructing a genomics cloud by using a public cloud, common workflow language, object storage system, network-attached storage, and docker based on IaaS/PaaS or high-performance computing hardware.

Cloud computing has features like IoT, such as computational capability, energy efficiency, service, storage, and applications over the Internet [56]. The integration of the IoT and cloud computing is named the Cloud of Things (CoT) [50], [51], [52], and by this integration, both cloud and IoT fulfil the gap/limitations like restricted storage, scope, and applications over the Internet. Furthermore, CoT provides high-quality, cost-effective, and ubiquitous services to extensive applications, i.e., healthcare, video surveillance, smart home, smart cities, smart energy, smart grid, smart logistics, automotive and smart mobility, environmental monitoring, and many more [53, 79, 83-85]. In CoT, a cloud infrastructure acts as an intermediate layer between the applications and things. It is considered a significant support system by which the billions of devices at the IoT layer upload their data to the cloud at the cloud layer to achieve a variety of on-demand services at the access layer. The amount of data is going through extremely fast growth; therefore, storing and processing big data is challenging as it increases with the number of devices. Cai et al. [86] have categorized big data into four classes: huge scale dynamic, high multisource heterogeneity, inaccurate, and low-level with weak semantics data. Consequently, IoT Big Data Applications (IoTBDAs) are requisite to be more capable of analyzing the dynamic data streams (online and offline) and static knowledge regarding

TABLE 2. Most common issues and challenges of CoT.

Issues	Protocol support- As the sensors work on various protocols, i.e. ZigBee, WirelessHART, 6LOWPAN, IEEE 1451, etc. Some protocols have been supported by the gateway device, while some might not have support. Introducing new services and maintaining Quality of Services (QoS) in terms of delay, packet loss ratio, bandwidth, and jitter. Energy efficiency- Heavy data communication consumes a high amount of energy. Resource allocation- This has to be mapped based on the type of sensor being used and the frequency of data generation. Identity management- Mapping of unique identification (ID) as the communicating nodes over the Internet need an ID. Formal deployment of IPv6- Assigning IPv6 would not be beneficial unless an efficient and standardized IPv4-IPv6 co-occurrence mechanism is adopted. Data security, privacy and excessive data communication. Heterogeneity of devices, platforms, operating systems, and services.							
Possible Suggestions	Having standardized protocols in the gateway and a uniform way of service discovery and dynamic prioritization. Transmission of a sample packet from the newly added node. Having efficient usage of energy and sleep mode. Also, sensors generate power from the environment, i.e. air, solar energy, and vibration. Assigning IPv6 addresses and IPv4-IPv6 synchronicity and smooth transitioning towards IPv6 must be considered. Sensitive data should be stored in a virtual storage server placed inside the trusted user's country region. Smart gateway supports the better consumption of network and cloud resources. Unifying platforms and middleware, interoperable programming interfaces for copying with data diversity.							
Challenges		**Privacy**	**Large-scale**	**Security**	**Reliability**	**Legal and social aspects**	**Performance**	**Heterogeneity**
	Smart home				✔		✔	✔
	Healthcare	✔	✔	✔	✔	✔	✔	✔
	Video surveillance			✔	✔		✔	✔
	Smart cities	✔		✔	✔	✔	✔	✔
	Smart grid	✔		✔	✔	✔	✔	✔
	Smart logistics		✔		✔	✔		✔
	Smart mobility			✔	✔		✔	✔
	Environmental monitoring		✔	✔	✔		✔	✔

the physical world to support real-time decision-making [87], [88].

Although the cloud infrastructure played a role in reducing the problem to some extent as it is processed with on-demand resources efficiently by incorporating a geographically centralized controller for processing, storage, and information retrieval [89]. Due to its centralized location, a massive amount of devices/users and distant datacenters from the user's proximity leads the latency-sensitive and real-time service requests towards network congestion, bandwidth consumption, context awareness, large round-trip delay/latency, service quality degradation, etc. [58], [78]. The entire efficiency of a network is based on the locations of the cloud's datacenters, as the private clouds provide local coverage and are infrequently affected because these are managed and prolonged considerably wide areas for providing smart city services. However, public clouds provide global coverage and are much affected because their data centers are far from users, even in another country or continent. Table 2 presents the most common issues and possible suggestions of the cloud-based IoT network. Most commonly cloud users experience many security vulnerabilities and threats such as user identity management, data access control, system complexity, reliability, infrastructure, and physical security, misconfiguration of software, encryption, and device heterogeneity [77], [89], [90].

Furthermore, various encryption algorithms have been proposed in past literature, such as asymmetric and symmetric key algorithms [80]. The Rivest Shamir and Adleman (RSA) is an asymmetric or public key algorithm that considers different keys for the decryption and encryption of messages and consumes the longest encryption time and memory size. In contrast, the Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish are symmetric key algorithms considering a single key for decryption and encryption. It has been observed that the AES algorithm takes

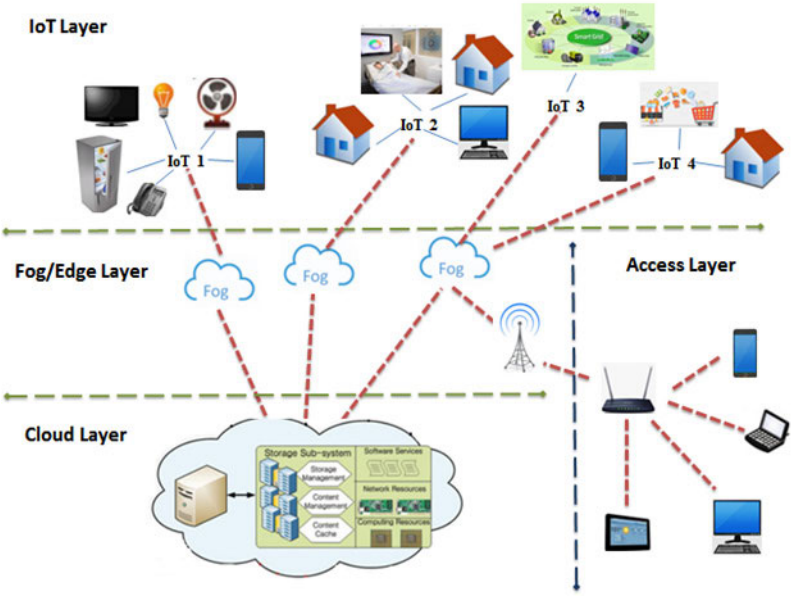

FIGURE 3. Integration of IoT and cloud-fog computing.

less execution time, the DES algorithm takes the least encryption time, and the Blowfish algorithm has the least memory requirements. A Lightweight Smartcard Based Secure Authentication (LS-BSA) method has been proposed based on the elliptic-curve cryptosystems, mapping, and fuzzy verifier [91].

The seamless data connectivity is established over a secure network having lightweight operations such as Hash-based Message Authentication (H-MAC) and bitwise XOR. Another, Smart Card-based secure Addressing and Authentication (SCSAA), is proposed for smart homes [92]. The proposed scheme modifies the IPv6 protocols based on two folds: assigning distinct authentication, i.e., 64-bit interface identifier to devices and preventing unauthorized access via secret session key. In addition, an efficient two-level service configuration method is introduced that integrates chaos-gauss-based particle swarm optimization and K-mean clustering with the objective of utmost QoS stability and collaboration capability in open and dynamic cloud manufacturing environments [93]. At first, the K-mean algorithm clusters the candidate services with QoS stability to minimize search space, and then the chaos sequence initiates the particle swarm optimization. It considers the gauss perturbation operator to find the optimal service composition.

Moreover, another computing paradigm, i.e., Edge/Fog computing, has been proposed as an extended version of cloud computing that provides faster/low latency computational services at the edge network for the delay-sensitive IoT-based applications/fifth-generation (5G) wireless systems [94], [95], [96]. The edge network includes edge servers, edge devices (routers, bridges, wireless access points, base stations, etc.), and end devices (smart devices, mobile phones, etc.), as shown in Figure 3. Since, Fog is a configuration that distributes the communication, computation, storage, and control and carries all the benefits of cloud computing at the Fog/Edge layer to the nearer end users/devices [54], [58], [97]. The Fog computing applications are categorized into two groups; real-time (healthcare, gaming, video streaming, accident prevention, and smart traffic light system) and near real-time (smart city, grid, and vehicle, data retrieval, and traffic flow maintenance) [6, 55, 98]. Specifically, in the manufacturing industry, Fog computing assists local processing with acceptable communication delay to interaction systems and robots, however; its deployment faces many challenges, i.e., security, heterogeneity, programmability, and interoperability [99].

Moreover, Liu et al. [100] categorized the issues and challenges of the Fog computing environment based on various modules such as application (interface, reliability, and fault tolerance), processing (latency and resource-restricted), infrastructure (heterogeneity and virtualization), security (authentication, security protocols, and privacy access control), monitor (attack and infect detection), storage (data protection), management module (resource, energy and updating management). Table 3 shows some security issues based on the components of the Fog infrastructure. In IoT-based applications, devices may connect/select various remote cloud servers or Fog nodes to offload their tasks while ensuring the QoS requirements. However, resource allocation in Fog computing is challenging due to the rapid growth of intensive computation and restricted processing power of the Fog nodes. To facilitate Fog computing in IoT-based applications (FoT), an effective resource allocation method is required that efficiently allocates the Fog computing resources to the IoT devices. In past literature, many different Fog computing-based systems have been proposed

TABLE 3. Security issues based on the components of the fog infrastructure.

Security issues	Fog components				
	Network infrastructure	User devices	Virtualization infrastructure	Service infrastructure (edge)	Service infrastructure (core)
Man-in-the middle	✔				
Denial of Service	✔		✔		
Rogue gateway attacks	✔				
Privacy leakage			✔	✔	✔
Privilege escalation			✔	✔	
Physical damage				✔	
Virtual machine manipulation		✔	✔	✔	✔

to provide reliable data and optimize the entire network performance in terms of increasing the Quality-of-Experience (QoE) and decreasing the total cost of IoT-based system, aggregate delay, energy consumption, and computation time by considering the task offloading issue in Fog computing [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111].

B. INTEGRATION OF IOT AND BLOCKCHAIN

Blockchain is one of the most industrial technologies that enable the movement or transfer of digital assets/currencies from one individual to another and provides improved interoperability, privacy, and security to IoT-based networks [112]. The word ''block'' refers to the records/datasets or digital information, and ''chain'' leads to storage in a public database. In other words, an individual blockchain comprises a systematic list of nodes and connected links [113]. This record-keeping technology was introduced in 2008 [114] as a Peer-to-Peer (P2P) decentralized and distributed public ledger that keeps the transactions (time, date, and purchase or amount with the participant's identity or username) in a sequence of blocks [115], [116]. The composite layer of a blockchain involves five different sublayers: data, network, consensus, incentive, and service sublayer [117]. The data sublayer assembles the encrypted data from the perception layer (IoT devices deployment) with a digital signature via a unique cryptographic code, i.e., hash function and asymmetric cryptographic algorithms. At the network sublayer, a peer connection runs based on virtual or physical links between nodes. A block of transactions is shared and verified between peers. If that block is valid, it can only be further propagated over the network. The consensus sublayer distributes the consensus for the trustfulness validation of a block via consensus techniques, i.e., Ripple, Proof of Stake (PoS), Tendermint, Algorand, Proof of Work (PoW), Delegated POS (DPOS), Proof of Elapsed Time (PoET), Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) [12, 118-122]. The incentive sublayer handles all the currency-related issues, such as digital currency creation, distribution, rewarding mechanism, transaction cost, and policy designing. While the service sublayer provides blockchain-based services to a diversity of applications, such as financial and Social services, academics, web, e-business, healthcare, stock market, crypto-currency, risk management, security and privacy, and IoT [117], [123], [124], [125], [126], [127], [128], [129]. However, blockchain systems are categorized into three groups: private, public, and consortium. In addition, Private blockchain systems are managed by a single organization, public blockchain systems (Bitcoin) are decentralized by which every node keeps a record of all transactions. In contrast, consortium blockchains are hybrid systems that imply private and public blockchain systems. Moreover, the blockchain system is an irreversible process because all the transactions are done with Bitcoin that cannot be void and neglected. Each block on the Bitcoin blockchain stores up to 1 MB of data depending on the size of the transactions and discriminates by the hash. Once any new transaction occurs, it must be verified and stored in a block with a hash, then added to a blockchain and available to the public.

Moreover, the physical machine or hub acts as a participant node interconnected through the Internet/cloud named BlockChain of Things (BCoT) [59], [60]. The BCoT is one of the core technologies of industry 4.0 and has some characteristics such as autonomy, resilience, scalability, and security [130]. BCoT has various applications in industry 4.0, such as healthcare, smart grid/cities, transportation, manufacturing, government sector, energy management, banking and payment, insurance, digital supply chain, recruitment, and voting. However, a smart conceptual contract is introduced in an IoT environment with discriminating consensus based on practical byzantine fault tolerance protocol to minimize the delay and consensus prejudice issue [131]. The participant nodes perform the validation process through the verification and endorsement phases. The blockchain hubs are private; they do not share any information regarding the previous/ongoing transactions and ensure teamwork in the entire validation process using cryptographic software. Since Security is a major challenge in IoT networks, the lack of security measures can suffer data confidentiality, device authentication, and inappropriate systems use. However, the security attacks in IoT are categorized into four main groups

TABLE 4. Various attacks in IoT-based networks.

Attacks	Perception layer	Application layer	Network layer	Processing layer	Effects
Network Attacks	----	----	Traffic analysis attack, wormhole, Sybil, unauthorized access and RFID spoofing, routing information, selective forwarding and reply attack	----	Data leakage, message destruction, unfair resource allocation, network congestion and data privacy violation
	----	----	Denial and distributed denial of services attack		Network crashes and network flooding
Physical Attacks	Tampering, malicious code injection, fake node injection, sleep denial attack, permanent denial of service and RF interference/jamming	----	----	----	Resource destruction, sensitive information access, communication blockage and node shutdown
	Side channel attack		----	----	Collect encryption keys
Data Attacks	----	----	Data inconsistency		Data inconsistency
		----	Data Breach	Unauthorized access	Data leakage and data privacy violation
Software Attacks	----	Worm, spyware, virus, trojan horses and adware	----	Malware	Infect data and resource destruction

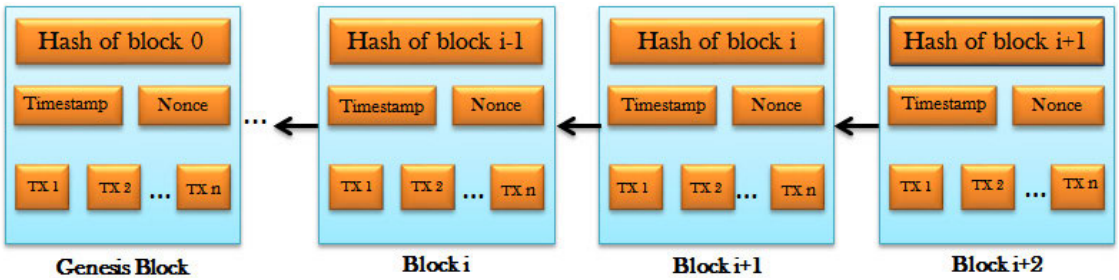

FIGURE 4. Model of a Blockchain.

such as network, physical, data, and software attacks (as shown in Table 4).

Besides, privacy and time accuracy are significant aspects of the blockchain in all application scenarios. Due to the irreversible nature of the ledger and malicious nodes' influence, BCoT is facing some critical and challenging issues, such as time synchronization or slow consensus/consistency, and high resource consumption. Further, blockchain can address the issues mentioned above through data encryption, immutability, auditability, transparency, and operational resilience [132]. Network attacks at network and processing layers are traffic analysis attacks, wormhole, Sybil, unauthorized access, RFID spoofing, routing information, selective forwarding, reply attacks, denial and distributed denial of services attacks with data leakage, message destruction, unfair resource allocation, network congestion, and data privacy violation respectively. Table 5 summarizes and differentiates various types of blockchain systems and the most common applications based on their requirements and challenges.

Data attacks at network and processing layers include data inconsistency, breaches, and unauthorized access with data leakage and privacy violation. Moreover, the physical attacks

TABLE 5. Various features, security requirements and challenges of the BCoT.

Merits	Layers	Characteristics	Types			Applications	Security Requirements	Security Challenges
			Private	Public	Consortium			
Reliability	Data Sublayer	Decentralization	Centralized	Decentralized	Partial Decentralized	Smart Grid	Availability, integrity, confidentiality, privacy and non-repudiation	Heterogeneity, data sensitivity and privacy, scalability, vulnerabilities associated with information system technology
Traceability	Network Sublayer	Immutability	Alterable	Immutable	Partial Immutable	Healthcare	Authentication, confidentiality and privacy	Mobility heterogeneity and resource limitations
Autonomic	Consensus Sublayer	Non-repudiation	Refusable	Non-Refusable	Partial Refusable	Transportation	Authentication, privacy and availability	Diversity of attacks, heterogeneity and high mobility
Interoperability	Incentive Sublayer	Transparency	Opaque	Transparent	Partial Transparent	Smart Cities	Availability, integrity, confidentiality and authentication	Data management, high level of heterogeneity and scalability
	Service Sublayer	Traceability	Traceable	Traceable	Partial Traceable	Manufacturing	Availability, integrity, confidentiality and authentication	Resource limitation, cyber-physical attacks, scalability and safety challenges
		Scalability Flexibility	Superior	Poor	Good			
		Permission	Permissioned	Permissionless	Permissioned			

at perception and application layers are tampering, malicious code injection, fake node injection, sleep denial attack, permanent denial of service, RF interference/jamming, and side channel attack with resource destruction, sensitive information access, communication blockage, and node shutdown and collect encryption keys respectively. In contrast, the software attacks at application and processing layers are a worm, spyware, virus, trojan horses, adware, and malware with infective data and resource destruction effects. Various security techniques are proposed to prevent the attack from guaranteeing data protection with various security services, such as integrity, confidentiality, authenticity, availability, privacy, and non-repudiation.

Figure 4 presents an example blockchain diagram that consists of consecutive associated blocks. Each block comprises the hash value of the previous/parent block, timestamp, random number/nonce for the hash verification, and datasets/data packets (several transactions (TX1-n)). Besides, the Blockchain constantly updates with every transaction and appends a new block at the end of the blockchain by the reverse reference indicating the parent block. This ensures the entire blockchain's integrity to the first/genesis block. While Figure 5(a) shows an example scenario of a supply chain blockchain, an end-to-end system involves various stages like manufacturing, shipment, dissemination, retail, and consumer. The product status is monitored and recorded from manufacturer to consumer at every production stage.

Consequently, it leads to improved inventory management and customer engagement. Also, the system's efficiency increases, and fraudulent and error activities decrease. Another blockchain-based eHealthcare system has been proposed for WBAN to provide a low-power and secure healthcare solution [133]. Figure 5(b) shows the blockchain-based healthcare network scenario based on doctors, care-taker, patients, and various services such as self or remote monitoring, uploading patient reports, real-time observation, ambulance for emergencies, etc. The distributed ledger shares patient reports and prescriptions with every interconnected participant. Consequently, blockchain provides the secure interaction and storage of data, respectively.

In the past few years, blockchain technology has attracted enormous manufacturing and academic research consideration due to its capability to permit decentralized distributed systems and provide trust in connections for various activities. Moreover, various blockchain-based protocols/techniques are proposed in past literature that solve the time synchronization [124], [134], [135], [136], [137], [138], [139] and device authentication issue by ID-based, ID/password-based, certificate-based, cryptography-based, MAC address-based, and P2P/

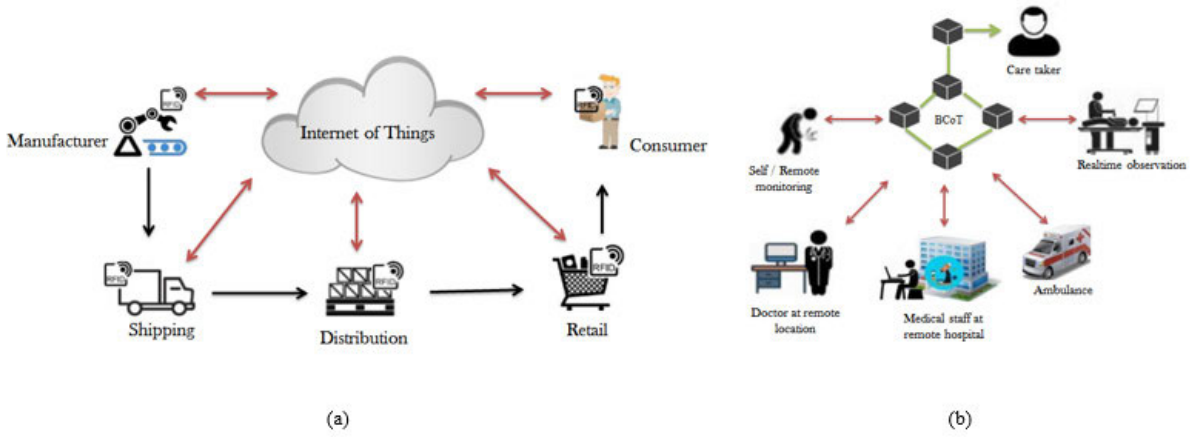

FIGURE 5. (a) Retail and (b) Healthcare example network scenarios of the BCoT.

blockchain-based [140]. A platform selection method is introduced to select a suitable blockchain platform to develop an enterprise system [141]. The proposed method consists of four phases such as (i) identification and registration of blockchain platforms, (ii) selection of suitable blockchain platform via a simple multi-attribute rating technique, (iii) evaluation of the selected system in terms of capability analysis, tools, libraries, system architecture, and domain-specific applications, and (iv) validation of the proposed enterprise solution. Consequently, Hyper-ledger Fabric was considered as the most suitable blockchain platform to develop complex enterprise projects.

A blockchain-based IoT system is proposed to configure and control IoT-associated devices by using Ethereum [142]. It is a public blockchain-based platform that combines the blockchain with the computing system. It facilitates a computing environment for the developers to write, compile and run their code on its virtual machine. By having this platform, IoT devices are configured, authenticated via managed public key infrastructure, and updated their behaviour. In their proposed work, an experiment was conducted between a few devices (smartphone, electricity meter, light bulb, and air conditioner), and smart contracts were written to store the data. The keys are managed via a cryptosystem, in which the private and public keys are stored in individual devices and Ethereum.

However, Danzi et al. [135] proposed a blockchain-based architecture for IoT to solve the time synchronization issue. The proposed architecture categorizes the data traffic among IoT devices and blockchain networks. In addition, a traffic model is proposed to extract the synchronization time and minimum bandwidth, whereas two protocols have been established to provide security to the network. Fan et al. [124], [134] proposed a secure blockchain-based synchronization scheme for IoT to solve the time synchronization or announcement issue. In the proposed scheme, multiple time sources prevent single-point failure or centralization. In addition, a blockchain structure is proposed to minimize malicious attacks, latency, and communication overhead by transmitting a few messages during the synchronization procedure.

Machando and Frohlich [143] proposed a blockchain-based IoT architecture to verify data integrity. The proposed architecture is categorized into three stages: IoT, Fog, and Cloud. The IoT stage consists of actuators, sensors, gateways, Proof-of-Trust (PoT), and Trustful Space-Time Protocol (TSTP). The Fog stage creates cryptographic digests (with Proof-of-Luck (PoL) algorithm) and provides fault tolerance to IoT data. The cloud permanently stores the IoT data (using blockchain consists of cryptographic digests). Hong [140] proposed a blockchain-based authentication scheme for IoT to get secure authentication. In the proposed scheme, node authentication is analyzed by the device authentication, non-repudiation, and device integrity method. A simple hash operation is required to operate low-performance IoT devices.

Moreover, the privacy issue is solved by private contract (programmable contract), anonymization (removal of Personally Identification Information (PII) before data transmission), encryption (public and private keys), mixing (combining and merging transactions), and differential privacy technique (noise addition) [144]. Recently, a Distributed Ledger Technologies (DLT) trading system is proposed to provide a smart data trading solution based on the Narrow Band connectivity [145]. For the proposed DLT system, three different data trading protocols are proposed Selling on Demand (SoD), Buying on Demand (BoD), and General Trading (GT). However, the cost of each protocol is analyzed with Narrow Band connectivity. Honar Pajooh et al. [146] proposed a blockchain-based multi-layer security framework with a reliable mechanism for IoT networks. The proposed framework categorizes the entire cellular network into three different layers. Each layer consists of (i) IoT network and various clusters with local authorization and authentication, (ii) cluster head and sink nodes with local blockchain hyper ledger fabric, and (iii) base stations with global blockchain and sophisticated security approaches,

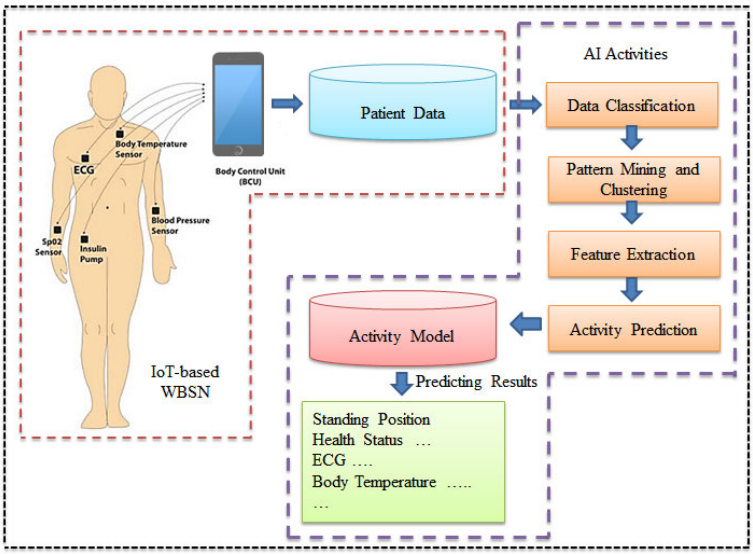

FIGURE 6. Health prediction based on the patient data.

respectively. Consequently, improves communication efficiency, security, and credibility assurance.

C. INTEGRATION OF IOT AND ARTIFICIAL INTELLIGENCE

Artificial or machine intelligence is the most famous and outgrowing technology that plays a marvellous role in making smart or intelligent decisions. Artificial Intelligence (AI) refers to human-like intelligence; any machine that acts like a human is called an AI-based/ intelligent machine. Using their well-designed learning techniques, intelligent machines can automatically execute various functions such as learning, perceiving, reasoning, natural language processing, and resolving complex problems [147]. The robust AI-based intelligence is obtained from machine learning, deep learning, fuzzy logic, semantic/neural network, and data fusion techniques to provide instinctive resource provision [148], [149], [150], [151]. The main aim of the techniques mentioned above is to acquire hidden knowledge by processing the raw data. The main aim of the fusion of IoT and AI is to create a smarter environment via intelligent decisions on historical and real-time data feeds. This would improve the cities, offices, human health, homes, roads, forests, traffic management, prediction of accidents, emergencies, and crime, etc. The environmental data is perceived to make the smartest decisions for better automation, productivity, wealth, efficiency, and accuracy. Moreover, IoT devices accumulate a huge amount of data, and to analyze the hidden insights of accumulated data, AI techniques play a very important role in providing accurate analysis by offering an intellectual and decision-making facility for a device to humans in IoT applications. The importance of AI in IoT can be perceived in the current endeavours in the computing world, such as sensor fusion, image and voice recognition, predictions, event processing, localization, etc. [152], [153], [154], [155], [156], [157], [158], [159]. In IoT-based healthcare applications, an AI module consists of different sub-modules: user identification, data analysis, behaviour recognition, service formation, and provision. The data analysis is further categorized into four activities: data classification, training, modelling, and prediction. Figure 6 represents an example diagram of AI and IoT-based Wireless Body Sensor Network (WBSN) integration. Referring to Figure 6, the patient's health status (i.e. ECG, body temperature, etc.) is monitored while the variations in the readings/patterns indicate the patient's activity (moving, walking, standing, running, etc.).

Guo et al. [151] proposed a hybrid service architecture, i.e. Artificial intelligence-based Semantic IoT (AI-SIoT), to support heterogeneous devices and intelligent services. The AI-SIoT is based on three stages: resource provision, service management, and infrastructure. The infrastructure (first stage) consists of all smart devices such as smartphones, smart appliances, smart vehicles, wearable devices, smart medical systems, RFID-tagged items, smart monitoring systems, etc. At this stage, data is monitored and forwarded to the next service management stage for further investigations. The service management stage is further categorized into the AI, IoT platform, and semantic analysis modules. Once the smart devices are managed, and the acquired data is analyzed, resource providers offer different services with the association of cloud to the smart cities, homes, grids, offices, etc.

Moreover, machine and deep learning have gained more appreciation in the past few years while dealing with IoT-based data to provide intelligence to IoT devices. These are the promising techniques of AI commonly used for extracting accurate information from IoT devices. Furthermore, with the machine learning technique, machines can learn from a multifaceted phenomenon, i.e., experience or

TABLE 6. Frequently used AI algorithms.

	Method/Algorithm	Purpose	Benefits	Drawbacks
Supervised Learning	NB / Bayes' theory	Classification	High accuracy and efficient in terms of computation.	Unable to deal with large data
	Neural Networks (NNs)	Regression and classification	Efficient in terms of dealing with high-dimensional datasets without training.	Difficult to determine the number of neurons and layers.
	SVM		High accuracy with linear and non-linear data sets.	Expensive in terms of computation and memory.
	K-NN		Robust and negligible cost.	High time consumption
Unsupervised Learning	K-Mean	Segmentation	Efficient in terms of handling and assigning large datasets and objects to clusters, respectively.	Difficult to determine the number of clusters and random selection of centroids.
	Self-Organizing Maps (SOMs)		Efficient in terms of mapping/prediction and dealing with a high-dimensional dataset.	Inefficient in terms of parallelization of a huge dataset and high computational cost.
	Gaussian Mixture Model	Classification	Flexible cluster covariance and categorize non-sequential behavior.	Expensive in terms of computation and mixture models.
Reinforcement Learning	Multi-Armed Bandit (MAB)	Action selection	Error correction without any delay.	Expensive in terms of large time horizon and arm switching cost.
	Q-learning	Sequential decision making	Datasets are not necessary and can tolerate variations.	Expensive in terms of computation and data convergence.
	Deep Reinforcement Learning (DRL)	Composite target function	Dealing with large states with high performance.	Expensive in terms of computation
Other	Transfer Learning (TL)	Prediction	Save training time	Non-adaptive to change
	Convolutional Neural Network (CNN)		Efficient in making automatic decisions with high accuracy.	Large training data is required with high dimensional cost.
	Deep Neural Network (DNN)	Feature extraction	Robust with massively parallel computing.	A large volume of data is required with various parameters, topology, and training methods.

training examples, without any programming. The key of the machine learning model is to provide training data to a learning algorithm to generate a new group of rules (new algorithm) based on the acquired inferences. The learning approach is categorized into four classes: supervised, unsupervised, semi-supervised, and reinforcement [7], [160]. However, Table 6 describes the most common AI/learning algorithms frequently used in integrated IoT networks with their usage, benefits, and drawbacks. In supervised learning, the predefined data (labeled data with the desired outcomes) is given and can be achieved by classification (for instance, image classification, diagnostic and fraud detection via Naiıve Bayes (NB), Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Association Rule (AR)) and regression approach (for instance, weather forecasting and prediction via a neural network, decision tree, and ensemble learning). While in unsupervised learning, unlabeled data (not predefined data) is given, and the algorithm needs to identify itself. Unsupervised learning can be achieved by dimensionality reduction (big-data visualization and structure discovery) and clustering approach (for instance, marketing and segmentation). Semi-supervised learning is a hybrid approach, combining both supervised and unsupervised learning. Semi-supervised learning can be achieved by a semi-supervised classification and clustering approach (for instance, web-content grouping and speech analysis). Whereas reinforcement learning is based on experiences/trials, has no explicit outcome, and responds in terms of punishment and rewards. This kind of learning is achieved by model-based and non-model-based on/off approaches, such as traffic control, robotics, and resource management.

The reinforcement learning provisions security to the IoT-based devices via Deep Q-Network (DQN), Q-learning, Dyna-Q, and Post Decision State (PDS) [26]. The basic machine learning technique has a few fundamental limitations, such as a rich dataset is required for the training data model, and the entire procedure may not involve full coverage of various aspects of the data. However, in this regard, the deep learning technique has (an extended version of machine learning) been proposed to address the existing issues of the machine learning techniques by controlling a large amount of data and extracting significant high-level features to enhance the prediction accuracy [160]. Moreover, IoT devices generate semi-labelled or unlabeled data in IoT applications. Machine learning algorithm performs well on labelled data, however; a deep learning algorithm exploits the unlabeled data to acquire valuable configurations unsupervised configurations. The main aim of deep learning is to promote learning and analytics in the IoT field, such as self-driving, vehicle,

voice, face, thumb, finger, food and pattern recognition, fire, weather, and emergency prediction [150], [161].

In the past few years, various AI techniques have been implemented by many researchers in their IoT projects [164], [165], [166], [167], [168], [169]. However, AI faces challenges like resource constraints, artificial trust, security, privacy, centralized architecture, and a lack of enough training data [154]. In this regard, Alam et al. [149] examined some data mining algorithms for IoT-based data. In their conducted research, SVM, Linear Discriminant Analysis (LDA), KNN, NB, Artificial Neural Networks (ANNs), C5.0, C4.5, and Deep Learning ANNs (DLANNs) algorithms are used. Referring to the outcomes, it has been proved that the DLANN and ANN are computationally expensive and have high accuracy, while C5.0 and C4.5 are memory efficient and have higher processing speeds and accuracy. Another machine learning-based health detection system is proposed that considers logistic regression and SVM and predicts the patient's stress level by detecting the heart rate variations [162]. In contrast, Diedrichs et al. [163] proposed a machine learning-based prediction system to predict forest events by using training regression and existing machine learning algorithms.

Baracaldo et al. [164] presented a machine learning-based detection approach to detect poising attacks and filter the poisonous data to train the supervised learning model. Moreover, a machine learning-based optimization mechanism is proposed to improve the QoE in Multimedia IoT (MIoT) and obtain user satisfaction [165]. The proposed optimization mechanism is based on the data fusion of MIoT and QoE named QoE Data Fusion (QoEDF). QoEDF involves two phases: multimodal data fusion and the QoE optimization model. In the first stage, a multimodal data fusion method is introduced for QoE mapping between a controllable network-based system and uncontrollable user data. While in the second stage, an intelligent QoE optimization model is proposed using the fused results.

Recently, Azeem et al. [166] reviewed the symbiotic relationship between industry 4.0 and machine learning. They emphasized the concept of artificial intelligence towards machine learning, big data, and industry 4.0. The design principles of machine learning in industry 4.0 are classified as interconnection, modularity, real-time capability, virtualization, autonomy, and specialized assistance. In addition, they analyzed the existing practice and the impact of machine learning in industry 4.0. Moreover, Chen et al. [167] proposed an integrated framework based on the diffusion of innovation theory and technology organization and environment framework to discover the success factors that impact AI adoption in China's telecom industry. These factors include organizational capabilities, external environment, and advanced aspects of AI. To verify the proposed framework, the telecom companies of China are surveyed to analyze the data using the structural equation modeling technique. It supports firms for resource allocation and decision-making while adopting AI solutions in the telecom industry.

Likewise, a deep learning-based IoT-oriented infrastructure has been introduced to create a secure smart city [154]. The proposed infrastructure is based on Software Defined Network (SDN), blockchain, and a deep learning approach. Rodrigue et al. [155] proposed a deep learning-based diagnostic system to diagnose various skin lesions, i.e., melanoma and nevi. The proposed system is based on the transfer learning and existing neural network models as resource extractors such as MobileNet, Visual Geometry Group (VGG), Inception-ResNet, Extreme Inception (Xception), Neural Architecture Search Network (NASNet), Inception, Residual Networks (ResNet), and Dense Convolutional Network (DenseNet). However, SVM, K-Nearest Neighbors (KNN), and Perceptron Multilayer (MLP) are used for lesion grouping. Furthermore, the Micro-Controller Unit-based Network (MCUNet) is proposed to optimize the inference engine and deep learning model design/neural architecture to minimize memory consumption [153]. A Privacy-aware and Asynchronous Deep Learning (PADL) structure is introduced to train the deep neural networks and maintain the privacy of data obtained from different data group sites [156]. In PADL, Layer-wise Importance Propagation (LIP) algorithm and Advanced Asynchronous Optimization (AAO) protocol are proposed. Initially, LIP computes the significance of the model's weight to broadcast a local model to the cloud server, then AAO practices the universal updates. Moreover, the Optimal Deep Learning-based Convolutional Neural Network (ODL-CNN) is proposed for Face Sketch Synthesis (FSS) to provision the suspicious identification procedure [157]. In ODL-CNN, Improved Elephant Herd Optimization (IEHO) algorithm is used to optimize the various parameters of DL-CNN i.e. batch size, no. of hidden layers/nodes, and learning rate. IoT-associated cameras are used to capture the surveillance videos then ODL-CNN draws the sketches and compares them with the professional eye-witnessed sketches. In this way, the suspects are recognized by the sketches with an extreme resemblance.

Furthermore, blockchain technology is incorporated with AI techniques to analyze the big data in IoT. Rathore and Park [168] proposed the BlockDeepNet system to achieve high accuracy and acceptable computational overhead and latency. The proposed system is based on deep learning and blockchain techniques. Deep learning is executed at the IoT device level to get enough data and overwhelm the privacy leak, while blockchain is employed to certify the integrity and confidentiality of IoT. The BlockSecIoTNet ecosystem is proposed to detect attacks in IoT networks [169]. The proposed ecosystem comprises SDN, blockchain, mobile edge, and Fog computing. SDN provides an optimal detection model by which the data traffic is monitored and analyzed. However, the blockchain provides a decentralized detection system to prevent attacks/single-point failure issues. Moreover, mobile edge and Fog computing support attack detection and mitigation at the Fog and edge levels.

Rathore et al. [170] presented the Extreme Learning Machine-based (ELM) Semi-supervised Fuzzy C-Mean

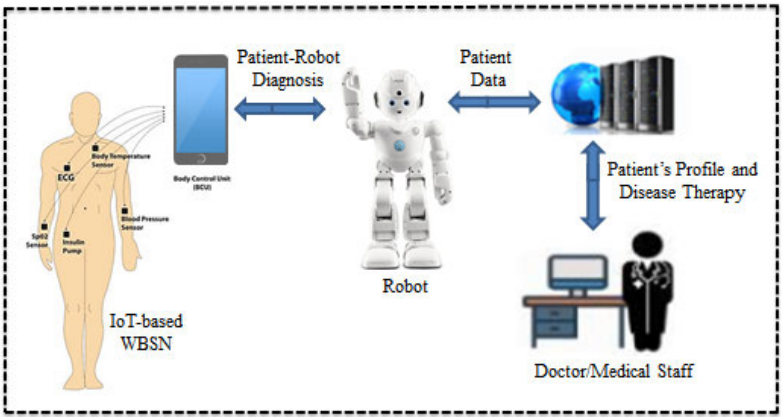

FIGURE 7. Model of the IoRT.

(ESFCM) method to provide a competent attack detection system in IoT. The ELM algorithm provides a faster detection rate, while the semi-supervised fuzzy c-means algorithm handles the labelled data issue. A Soft Hesitant Fuzzy Rough Set (SHFRS) theory is presented by Rathore et al. [171] to resolve the multi-criteria decision creation issues. Referring to their investigations, the inverse hesitant fuzzy soft set is defined by inverse hesitant fuzzy relation to define the lower and upper limits within a specified set of parameters. Further, Singh et al. [172] proposed a Blockchain-enabled Intelligent IoT Architecture (BlockIoTIntelligence) with AI to obtain secure and decentralized big data analysis for IoT. AI intelligence consists of edge, Fog, cloud, and device intelligence. The proposed architecture is based on qualitative and quantitative analysis phases. The qualitative analysis phase analyzes blockchain-driven AI and AI-driven blockchain applications. While in the quantitative analysis phase, an evaluation test is conducted in terms of latency, accuracy, computational complexity, privacy, and security.

Robotic is a famous and endless technology that deals with physically programmable machines/robots. In our daily life, several robots perform various tasks in different applications such as education, transportation, industries, manufacturing, home automation, hospitals, offices, hotels, etc. Furthermore, AI plays a major role in the robotics research zone, providing any semi or complete automation. The fusion of AI and robotics is named artificially intelligent robots.

However, the integration of IoT and robotics is named the IoRT [61], [173], [174], [175], [176], [177], and IoRT is an advanced version of IoT promoting data analysis, sensing, monitoring, decision-making, guidance, safety, security, perception, localization, mapping, navigation, and human-robot interaction via a variety of autonomous robots. The application type of IoRT is categorized into two main groups: service and field robotics [178], [179]. Service robots provide various services to human beings. In contrast, field robots operate in complicated environments such as agriculture, forestry, construction sites, etc., and are further categorized into air, underwater, space, and ground. The architecture of IoRT is categorized into three main layers, i.e., physical/hardware, service and application, and network and control layer. The hardware layer consists of robots and things, i.e., sensors, smartphones, vehicles, etc. The network layer provides various connectivity options such as cellular (3G and 4G), short-range (Bluetooth Low Energy (BLE), Broadband Global Area Network (BGAN), WiFi, Near Field Communication (NFC)) and medium-long range (Z-Wave, Worldwide Interoperability for Microwave Access (WiMAX), ZigBee, and Low Power Wide Area Network (LoRA)). However, the service and application layer executes and supports the application programs under the intentions of the assimilated IoRT. Figure 7 demonstrates an example diagram of the IoRT model. This diagram connects patients, medical sensors, and doctors/caregivers via a robot (master Bluetooth device). The Internet is the crucial communication medium for IoRT to connect with the cloud. IoRT monitors transmit the sensed data (diabetes, blood pressure, etc.) to the doctor and provide feedback regarding the patient's disease [180].

Recently, robotic behaviour was analyzed by imitation and deep reinforcement learning techniques [178]. The deep reinforcement learning technique assists the robots in real-time environments via automatic mapping. In contrast, the imitation learning technique assists the robots in learning and modifying new behaviours via cognitive sciences and perspective of behaviour. Further, a semantic-based platform is presented to deliver the interaction services for IoRT [181]. The proposed platform presents a module that permits the developers to create services accordingly and access the semantically inferred data from robots, sensors, and databases, defining suitable time and contents of the robot and human interaction by reasoning on semantically developed IoT-based data. However, a protection technique has been introduced for the Web of Robotic Things (WoRT) to provide privacy and security to visual data using a deep neural network-based semantic segmentation approach [182].

D. INTEGRATION OF IOT AND WIRELESS BODY SENSOR NETWORKS

The WBSN is a network of restricted, low-cost, and tiny heterogeneous sensor (biosensors, relays/forwarders, and sink)

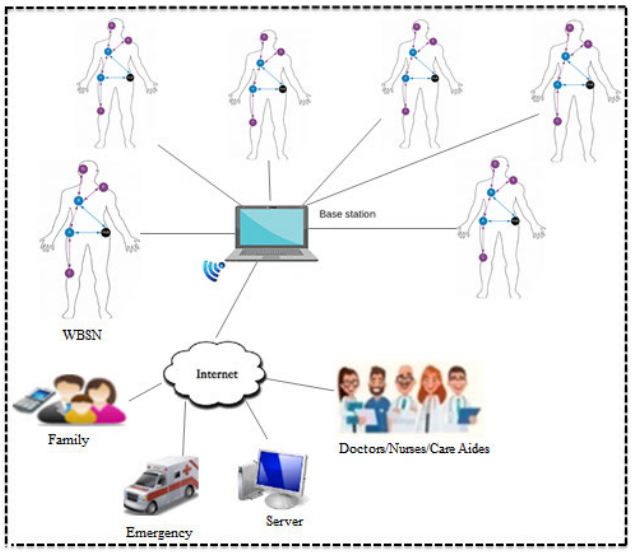

FIGURE 8. Infrastructure of the IoMT.

nodes that monitor patients' health status through their day-to-day activities. WBSN is restricted in size (i.e., number of nodes) and resources (i.e., processing power, communication range, memory, etc.). In WBSN, a variety of biosensors are either implanted or attached to the human body to sense high sensitive patients' data such as Electro-encephalograph (EEG), temperature, Electrocardiogram (ECG), blood sugar, Electromyography (EMG), pacemaker, endoscopic capsule, etc. [183], [184], [185]. The entire architecture of a WBSN is based on three layers: layer 1: intra-Body Area Network, layer 2: inter-Body Area Network, and layer 3: extra-Body Area Network. In layer 1, various biosensors sense, collect and transmit the physical data to a sink node in single and multiple manners. In layer 2, the sink node transmits the obtained data to the base station or gateway for further investigations, and the obtained data is available worldwide via the Internet from layer 3.

QoS, heterogeneous data traffic load, transmission link quality, end-to-end delay, energy consumption, path loss, and network lifetime are the most common issues and challenges of a WBSN. To solve these issues, a wide variety of routing protocols have been proposed in past literature, such as thermal-aware, cluster-based, postured-based, QoS-aware, security-aware, cross-layered, etc. In addition, IoT grows with the WBSN(s) as an IoMT that supports caregivers and patients to improve their quality of life and understand human beings' health possibilities (Figure 8). IoMT is based on a network of WBSNs that deliver global healthcare in terms of telemedicine, spurious drug identification, personal/remote monitoring or transmission of patients' data, assisted living, etc. In healthcare applications, if IoT is associated with the medical system, the fitness/health industry will be more transformed, and the medical system will progress faster than usual. This will benefit the specialists/doctors, medical staff, and patients having less awareness of basic health education/precautions.

Nowadays, IoMT plays a major role in remote patient monitoring and tracking for various chronic diseases [186], [187], [188], [189]. An effective deep neural training model (ETS-DNN) is proposed for edge computing-enabled IoMT [190]. At first, the patient data is transmitted to edge computing that executes the ETS-DNN based on a Hybrid Modified Water Wave Optimization (HMWWO) technique. The HMWWO technique integrates the Limited Memory Broyden–Fletcher-Goldfarb-Shannon (L-BFGS) and Modified Water Wave Optimization (MWWO) algorithms. In contrast, SoftMax (SM) classification is performed at the end of the deep neural network. Afterwards, the generated report is transmitted from edge computing to healthcare professionals via a cloud server. Furthermore, A supervised learning-based system i.e., Modified Deep Belief Network (M-DBN), is proposed for multi-sensor WBSN to predict heart disease [191] where the squirrel search algorithm selects various features.

However, IoMT still faces challenges such as reliability, safety, and security due to the restricted memory space and computational capability, energy consumption, and privacy concern (shown in Table 7) [64]. Researchers have discussed various solutions for secure IoMT [63], [192], [193], [194], [195], [196], [197], [198], [199]. Encryption is the basic solution that encrypts plain text by converting the original message into ciphertext. Then cipher-text is transmitted to the receiver, where the message is decrypted. There are many encryption mechanisms have been proposed in past literature, such as Asymmetric Key Encryption (AKE), Symmetric Key Encryption (SKE), and attribute-based encryption (ABE) [200]. An end-to-end key management scheme is proposed to exchange the keys with the least resource utilization [201].

Moreover, secure authentication key agreement schemes are proposed for a cloud-assisted WBAN [202]. The proposed schemes created secure channels to exchange keys based on the Diffie-Hellman method and Cipher-text Policy Attribute-Based Encryption. A distributed framework is proposed for secure IoMT [193]. The proposed framework uses five modules: handshaking/entry, listener/validation, security, conversion, and publisher. Initially, a connection request is sent to develop a link between sender and receiver tokens. Then this request is validated based on encryption techniques and updated on all adjacent devices.

Moreover, various cryptographic techniques /encryption algorithms are applied to data. Finally, data is directed to the requesting device, and a digital signature technique is applied to validate the user's authenticity. In contrast to cryptographic methods, a friendly-jamming scheme is used for IoMT to defend confidential patient-related data and minimize the eavesdropping risk [195]. Further, the friendly-jamming scheme integrates various communication technologies such as Simultaneous Wireless Information and Power Transfer (SWIPT), beamforming, and full duplexity. In [196], an Identification Security Attribute (ISA) framework is proposed for IoMT to calculate the security features.

TABLE 7. Most common challenges of the IoMT.

Cost	New technologies, techniques, and medications increase healthcare costs and make them unaffordable. The efficient strategies can minimize the use of equipment, operational time, and cost.
Device authentication	Some devices do not support authentication protocols due to inadequate energy and processing power. Optimized authentication schemes with a faster and low-power processor can support device authentication issues.
Data accuracy	Inaccurate data misleads and could be harmful to the patients. The decision-support systems analyze the entire depiction of the diverse types of medical records, resulting in faster and more precise treatments.
Energy consumption/ Energy-efficiency	Nonstop wireless devices consume a substantial amount of energy. Many schemes and protocols were proposed in past literature to minimize energy consumption. Still, minimizing transmission energy and optimizing the quantity of generated data is needed. Energy harvesting methods and energy-efficient devices can solve this issue by converting various energy sources into electrical energy i.e. sunlight, vibration, and heat.
Usability	Considering this factor, patients' safety and excellence can be enhanced based on their feedback. Smart devices predict and socialize, which rises well-defined user involvement standards.
Electrical safety	Improper usage and maintenance of electrical devices i.e. IoMT ecosystems, could be potentially dangerous in terms of burning injuries, severe pain, and fatalities. Therefore, safety measures should be taken before practices to ensure hazardous free devices.
Data storage, security and privacy	The quantity of data increases with the number of connecting devices and various significant issues that should be addressed, like storage, integrity, confidentiality, and data availability. Moreover, communication, access mechanism, and authentication are the major security issues and challenges. Blockchain and software-defined networks solve these problems to some extent.
Network and Communication Technologies	Different mechanisms, protocols, and standards are proposed to associate with the existing technologies, so there is a need for greener, faster communication technologies.

ISA framework is based on two approaches: Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) and Analytical Hierarchical Process (AHP). At first, the AHP approach derives the weights of features then the TOPSIS approach performs the security assessment of substitutes.

E. INTEGRATION OF IOT AND NANOTECHNOLOGY

The concept of "Nanotechnology as mixing, separating and warping of materials at the atomic or molecular level" was originally introduced by Taniguchi [203]. Eventually, nanotechnology becomes one of the most demanding technologies that modify the entire health services framework by introducing nanoscale devices ranging from 1 to 100 nanometers [204]. Further, nanotechnology is the study of extremely small things that can be used across all the other science fields, such as chemistry, molecular physics, computer science, biology, and mechanical and electrical engineering. It is widely used in many applications such as medicine, electronics, food, space, solar and fuel cells, fossil fuel, batteries, water and air quality check, chemical sensors, fabric, and sports [205], [206], [207], [208], [209], [210], [211], [212], [213]. Scientists and engineers are discovering various techniques to deliberately restructure the materials at the nanoscale to precede the advantage of their enriched properties, such as improved control of the light spectrum, lighter weight, higher strength, and better chemical reactivity than their larger-scale counterparts. Nanotechnology comprises two construction techniques: bottom-up and top-down [214], [215]. The bottom-up technique, also known as molecular manufacturing/ nanotechnology, constructs the materials from atoms or molecular components through a self-assembly process. The top-down technique reduces the size of larger structures into the nanoscale while keeping their original properties without atomic-level control. The bottom-up technique, known as molecular manufacturing/ nanotechnology, develops materials from atoms or molecular components through self-assembly. The top-down technique reduces the size of larger structures into the nanoscale while keeping their original properties without atomic-level control.

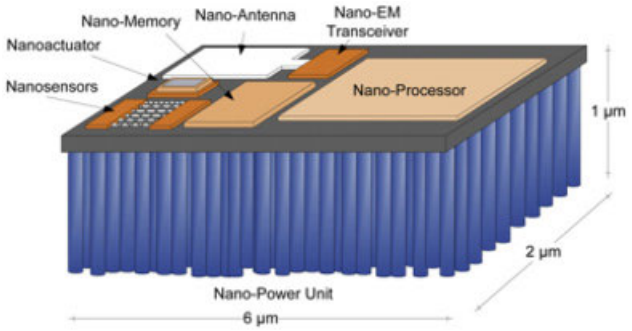

FIGURE 9. Nano-scale device [216].

Nevertheless, integrating nanoscale devices with the IoT-based network states an innovative networking paradigm named the Internet of Nano Things (IoNT) [216]. IoNT is a small-scale IoT, an ideal solution for medical applications and remote environmental monitoring, and is the most ongoing nano-scale network of interconnected physical objects with nano communication [27, 66, 68, 218-222]. Furthermore, IoNT is the interconnection of nano-scale devices (shown in Figure 9), existing communication technologies (for instance, sensors networks, big data analytics, cloud, and Fog computing), and the Internet to execute various operations such as sensing, computation, processing, etc. [222]. The infrastructure of IoNT is based on the bandwidth and the area of operation required by a specific application. Referring to Figure 9, the entire structure of a nano-scale device is based on processing, sensing (chemical, physical and biological nanosensors), actuation (chemical, physical, and biological nanoactuators), storage

(nano-memory), communication (nano-antenna and nano-electromagnetic transceiver), and power unit (nano-power). From the communication viewpoint, nano-scale devices face major challenges such as antenna design, channel modeling, bandwidth, noise, path loss, and channel capacity [27]. The network architecture of IoNT is based on four basic components: nano-routers, nanosensors, gateways, and nano-micro interface devices. Nanosensors are the smallest components of the IoNT network. Due to their small internal memory and size, the calculation and processing capabilities (operations) that they can perform are insufficient. The energy they store is also very restricted, as is the distance from which they can transmit data [223]. Nanosensors are made-up of nanoparticles/ nano-materials (graphene, copper, and carbon nanotube) and are classified as physical, chemical, and biological nanosensors [216].

In addition, nanotechnology offers an advanced method to carry out non-invasive diagnosis and identifies the abnormalities in the tissues, chemical compounds, physical features of structures, and biological agents i.e., bacteria, viruses, etc., is named the Internet of Bio-NanoThings (IoBNT) [69], [224], [225]. However, IoNT plays a very significant role in a variety of applications such as biomedicine (for instance, drug delivery and health monitoring system, bio-hybrid implant, immune system support, and genetic engineering), military (for instance, non-functionalized equipment, damaged detection system, and Nuclear Biological and Chemical (NBC) defences), industry (for instance, food and water quality control, office setup, and functionalized fabrics, and materials) and environment (for instance, air pollution control, animals and biodiversity control, and biogradation) [27], [73], [74], [216], [226], [227], [228], [229]. Figure 10 shows the network architecture of IoNT in a healthcare network scenario. Several nano-nodes are deployed in the targeted area to ensure enough data can be acquired to fulfil the defined task i.e., monitoring, broadcasting, therapy, diagnosis, supervising the patient's health condition, etc.

The communication among various nanosensors in the nano-scale is categorized into two main categories; electromagnetic and molecular communication. Electromagnetic communication occurs between nano-devices ranging from 2 to 6 micrometres based on the novel nano-materials. The nano-materials select the time interval and bandwidth for the emission of electromagnetic radiation. In molecular communication, sender nano-devices encode information into molecules (for instance, protein and Deoxyribo-Nucleic Acid (DNA)) and transmit within a DNA component. Due to the large size and high computational power of the nano-router(s), many nanosensors are associated with them to handle a cluster of nanosensors to accumulate, combine and forward the data to the nano-micro interface device. However, a function of nanomaterials at the non-ionized and safe Tera-Hertz (THz) gap or frequency band that is considered as the sensing and communication paradigm of nano-antennas within a range of 0.1 to 10 THz or 10^{12} Hz (shown in Figure 11) [72], [222], [224], [225], [226], [230],

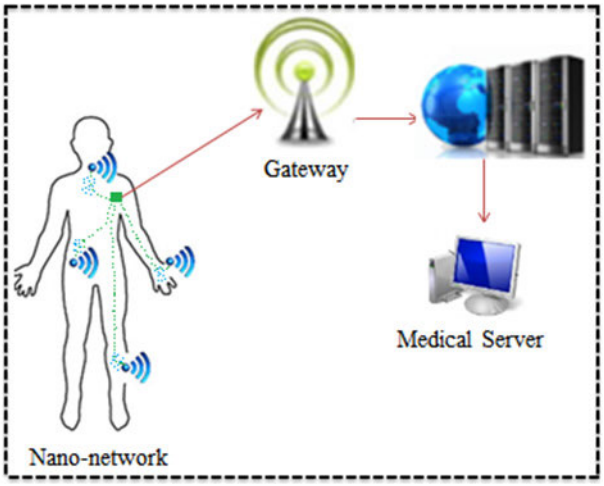

FIGURE 10. Standard network architectures of IoNT in the healthcare application scenario.

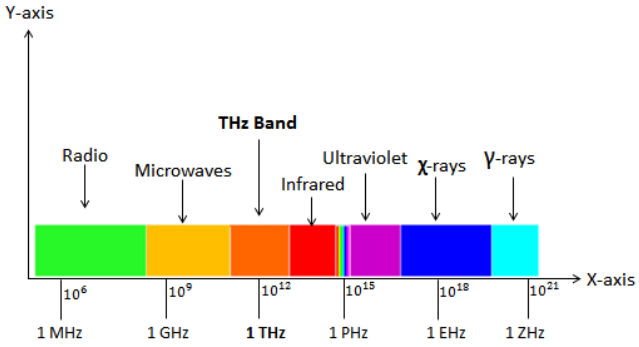

FIGURE 11. THz band in the electromagnetic scale.

[231], [232], [233], [234], [235]. Moreover, it supports very high transmission rates (Tbit/s), bandwidth, and throughput, and low latency in a short range (up to a few terabits per second and below one-meter distance) [70], [236]. The THz communication overwhelmed the capacity restriction of the existing wireless networks supporting new applications in the nano-scale communication and networking field [237], [238], [239], [240].

In the context of the wireless NanoSensor Networks (WNSNs) communication paradigm, various routing protocols, such as flooding, proximity, and energy harvesting protocols, are gaining more attention. The flooding routing protocols are simple, consistent, and have restricted computational power and energy, consequently increasing the retransmission and energy consumption [239]. In addition, the proximity routing protocols are proposed to enhance the flooding routing protocols by handling the number of adjacent nodes [241], [242]. The energy harvesting-based routing protocols are introduced to stable energy harvesting and consumption to maximize the network lifetime [243], [244], [245]. Though Wang et al. [246] proposed an energy harvesting Slot Self-Allocation based Medium Access Control protocol (SSA-MAC) for distributed and centralized

TABLE 8. Most common features of all integrated technologies.

Features	IoT	Cloud	Fog	Blockchain	AI	WBSN	Nanotechnology
Architecture	Distributed and dense(Pervasive)	Centralized	Decentralized and distributed			Limited with single and multihop topology	
Target user	Static and mobile devices	Wide-range Internet users	Mobile users	Static and mobile users		Static and mobile sensors	
No.server/sensor nodes	Large	Few	Large	Large	Few	Few	
Working environment	Indoor and outdoor	Indoor	Indoor and outdoor	Indoor and outdoor	Indoor	Indoor	
Service type	Device's information specific	Globally information specific	Localization information specific	Transactions specific	Data specific	Sensor's information specific	
Location awareness	Yes	No	Yes	Yes	Yes	Depends on the application requirements	
Mobility	Yes	No	Yes	Yes	No	Yes	
Big data	Source	Aims to manage			Aims to detect/Diagnose	Depends on the application requirements	

nano-networks to increase energy efficiency and prevent retransmission. In SSA-MAC, a time frame is categorized into many time slots. Nano-nodes allocate a self-allocated slot via their own identification while the remaining slots are named as sleep slots. By using a self-allocated slot, the nano-node receives packets from other nano-nodes and sends packets to the nano-controller in the distributed and centralized nano-networks, respectively.

Moreover, Xu et al. [223], [247] proposed the Centralized Energy Harvesting-based Time Division Multiple Access (CEH-TDMA) and Energy Balance Clustering Routing (EBCR) protocols to observe the data transmission procedure and minimize the communication overhead, energy consumption, transmission distance, and nano-nodes in a cluster respectively. In CEH-TDMA, time slots are assigned based on the urgency of the data transmission [247]. Nano-controller creates a Markov Decision Process (MDP) based on all nano-nodes' obtained packets and energy-related information. In EBCR, a novel hierarchical clustering technique is used by selecting the next-hop node based on the tradeoff between channel capacity and transmission distance [223]. In addition, one-hop communication occurs between the nano-nodes and cluster head, whereas multi-hop communication occurs between the cluster head and controller.

However, an energy-neutral event monitoring architecture is proposed for IoNT to transmit the event and location information [220]. In the proposed architecture, two main options are designed and analyzed: a single pulse and two pulses. In the first option, a single pulse consists of the entire event harvested energy that interconnects both event type and location information, while in the two pulses option, event harvested energy is categorized into two pulses by which the location information is conveyed before the event type information. Furthermore, in cluster-based nano-networks, several nano-devices, i.e., nano-actuators and nanosensors, are deployed with THz communication along with the proposed energy-efficient and fuzzy logic-based routing protocols for the Body Area Nano-Networks (BANN) [219], [222], [223], [227], [238], [248], [249]. In their proposed architectures, the nano-devices are clustered inside the human body i.e., leg, hand, back, and chest area, along with each independent nano-router to monitor and process the acquired data to the gateway; at this point, the data is remotely accessed via the Internet for further investigation and medicinal purposes.

IV. DISCUSSION

IoT has emerged as a significant research area offering the integration of various sensors/things with other networks/technologies without human interventions. This section summarizes all integrations of IoT technology. Table 8 compares the various features of all considered technologies. The most significant components and platforms of the integrated IoT network are shown in Figure 12, while Tables 9 and 10 summarize the computational part and other aspects.

Cloud computing provides low-cost services and high versatility, power, and performance. Moreover, IoT adopts a distributed computing paradigm with huge processing, storage capacity, computation, and on-demand resources due to resource constraints and short communication ranges to process large amounts of data from different devices. However, this technology experiences many security threats and vulnerabilities, i.e., deployment variations, identity management, user authentication, etc. To prevent these issues to some extent, edge/fog computing is used to provide low-latency computational services at the edge network for delay-sensitive IoT-based applications. Apart from this, blockchain technology provides a decentralized cloud-based network infrastructure. Conventionally, the financial transactions are settled via an authoritative financial institution

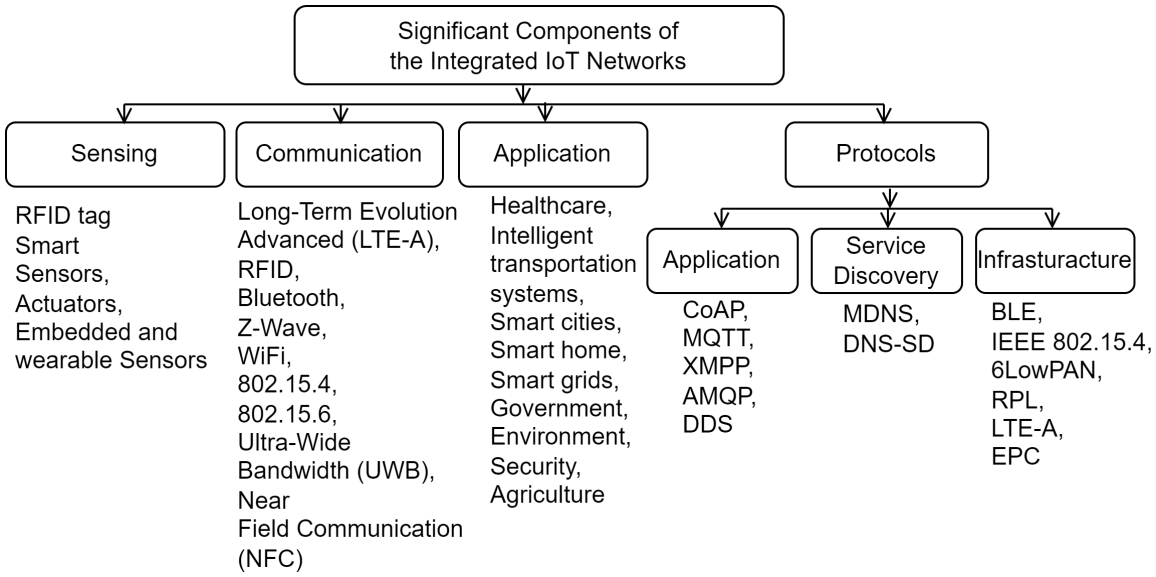

FIGURE 12. Significant component of the integrated IoT networks.

TABLE 9. Computational part of significant components of the integrated IoT networks.

		Operating System	Supporting Language	Event-based programming	Minimum memory (KB)	Dynamic memory	Multithreading
Computation	Software	Contiki	C	Yes	2	Yes	Yes
		Riot OS	C/C++	No	1.5	Yes	Yes
		TinyOS	nesC	Yes	1	Yes	Partial
		LiteOS	C	Yes	4	Yes	Yes
		Android	Java	Yes	-	Yes	Yes
	Hardware	FriendlyARM, Z1, Raspberry PI, Arduino, Gadgeteer, Cubieboard, Mulle, WiSense, and T-Mote Sky					

entity for verification, ensuring the execution of these transactions. However, blockchain technology digitizes and verifies these transactions and ensures the correct execution of these financial transactions with several technical properties i.e., transparency, privacy, traceability, and immutability, without the involvement of third-party authorities.

Furthermore, with the evolvement of AI technology, intelligent machines automatically execute various functions such as learning, perceiving, reasoning, and resolving complex problems using their well-designed learning techniques. In addition, IoMT supports remote healthcare in terms of self/timely care and identification of various diseases. Nevertheless, various machine/deep learning techniques are being utilized to provide security by identifying new attacks via learning skills. In the context of IoNT, nano-scale devices are interconnected to the existing communication technologies and the Internet to execute a variety of operations (i.e., sensing, computation, processing, etc.) in healthcare, agriculture, remote environmental monitoring, i.e., traffic and atmosphere monitoring, war field monitoring systems and many more. Consequently, many benefits are achieved by the integration of IoT with existing technologies such as smart cities, grid, homes, healthcare, transportation, and manufacturing in terms of (a) improving the telecommunication service management/cost-effective services, (b) improving the transparency and traceability, (c) letting the users to securely share their data, (d) reducing the operational/transactional/human errors, (e) automatic decision-making abilities, (f) supporting e-learning facilities, (g) remote consulting, (h) physical-location-independence, and many more.

V. FUTURE RESEARCH DIRECTION

The most significant research challenges and issues in integrated IoT-based networks are still open for future research.

A. AN INTELLIGENT CIoT SECURITY ARCHITECTURE

A reliable and secure network has always been a space for improvement. Adversaries make consistent attempts to hack IoT devices, for instance, injecting malware in the sensors or tampering with the data in the CIoT context, especially financial or health-related data. As such, how to enable smart things to choose between cloud, fog, and mist computing would be an interesting security research direction in CIoT.

TABLE 10. Most common platform used for the integrated IoT networks.

Platform	Open Source	Public Cloud	Private Cloud	Free	Application API	Ready to Use	Proprietary Things	Aim
IoTCloud [250]	✔			✔	✔	✔	✔	To integrate and manage various smart objects with API provision.
Temboo [251]	✔			✔	✔	✔	✔	To incorporate Raspberry Pi, Arduino, and other platforms with different internet services, i.e., SMS, Email, etc.
OpenIoT [252]	✔	✔	✔	✔	✔	✔	✔	To provide a middleware to deploy and configure algorithms for message collection, filtration, and event generation.
IoT Toolkit [253]	✔			✔			✔	Provides several protocols for things, the cloud, and applications.
Arduino IoT Cloud [254]	✔				✔	✔	✔	To create a cloud-based IoT network for real-time data monitoring.
Zetta [255]	✔			✔	✔	✔	✔	To assemble several devices into real-time and data-intensive applications by incorporating WebSockets, REST APIs, and reactive programs.
Nimbits [256]	✔		✔	✔		✔	✔	To create a PaaS that assembles data and triggers alerts when particular circumstances are verified.
OpenPicus [257]					✔		✔	To construct things with TCP/IP stack, HTTP server on-board, and RESTful APIs.
Xively [258]			✔	✔	✔	✔	✔	To collect and store data on the Cloud offered by the service provider.
Open.Sen.se [259]			✔	✔	✔	✔	✔	
ThingSpeak [260]			✔	✔	✔	✔	✔	
CloudPlugs [261]			✔	✔	✔	✔	✔	
Carriots [262]			✔	✔	✔	✔	✔	
NetLab [263]	✔		✔	✔		✔	✔	To interconnect with several CloudIoT services for periodically sending and retrieving data.
Cloudera [264]	✔	✔	✔		✔	✔	✔	To provide self-service access anywhere, manage and secure business data.
Block-Sim [265]	✔			✔	✔	✔	✔	To design blockchain networks.
Nano-Sim [266]	✔			✔		✔	✔	To implement the nanonetworks.
Dynatrace [267]	✔		✔		✔	✔	✔	To create SaaS that automates the dynamic multi-cloud.

Secondly, dealing with a large amount of data with heterogeneity, scalability, and accurate data aggregation in IoT-based networks and various wireless sensor devices with constrained capabilities. Effective data sampling and traffic forecasting schemes are also required to provide high accuracy and adaptability. This would also be a great potential future research direction.

B. BLOCKCHAIN IoT

Considering the challenges identified in this paper, the integration of IoT and Blockchain technologies should be addressed. Integrating deep/machine learning and blockchain should be considered to provide decision-making and data prediction abilities would be an interesting research future direction

C. OPTIMIZE ROUTING FOR WBAN- IoT

The wearable IoT devices in WBAN generate different types of data with various QoS demands. Energy depletion, device mobility, and node/link congestion are among the issues affecting WBAN IoT routing. It would be interesting to devise a multi-routing metrics intelligent-based routing scheme.

D. INTERNET OF NANO THINGS

The emergence of the Internet of Nano Things has made significant contributions to clinical medicine and many other

ground-breaking heights, particularly new technologies with the integration of IoT. Nanostructure-based biosensors are highly appealing candidates for rapid sensing in critical diseases such as cancer detection. This has not been sufficiently covered. It would be an interesting research to devise intelligent cancer detection using deep learning techniques.

VI. CONCLUSION

This paper presents an in-depth review of IoT with its immediate advancement involving existing emerging technologies domain. IoT is the most prominent technology in industry 4.0, with a vision of an interconnected world of unlimited things that can actively connect, identify, perceive, participate in decision-making, and report on a global scale via the Internet. As such, we have extensively discussed the background challenges of IoT. The growth of IoT has also been discussed to highlight its impact on various emerging technologies. Several examples from the literature have also been referenced to provide the applications of such emerging technologies. We touched on integrating IoT and cloud, where several solutions have been proposed over the years. Their weakness has been highlighted. Integrating IoT and Blockchain is also among the emerging technologies. How Artificial intelligence is applied to IoT for different research design objectives was discussed. We also discussed the integration of IoT and WBAN. It is also another hot research topic that is currently receiving attention. Integrating Nanotechnology and IoT has also been discussed. We present the weakness and research issues currently affecting each technology, and finally, we suggest some future research directions.

ACKNOWLEDGMENT

The authors are thankful to Universiti Teknologi Malaysia for the support to carry out this research under grants No Q.J130000.21A2.06E03 and Q.J130000.2409.08G77.

REFERENCES

[1] L. Li, "China's manufacturing locus in 2025: With a comparison of 'Made-in-China 202,' and 'Industry 4,'" *Technol. Forecasting Social Change*, vol. 135, pp. 66–74, Oct. 2018.
[2] I. H. Khan and M. Javaid, "Role of Internet of Things (IoT) in adoption of Industry 4.0," *J. Ind. Integr. Manage.*, vol. 7, no. 4, pp. 515–533, Dec. 2022.
[3] C. Zhang and Y. Chen, "A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics," *J. Ind. Integr. Manage.*, vol. 5, no. 1, pp. 165–180, Mar. 2020.
[4] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018.
[5] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 54–61, Jan. 2017.
[6] T. S. J. Darwish and K. A. Bakar, "Fog based intelligent transportation big data analytics in the internet of vehicles environment: Motivations, architecture, challenges, and critical issues," *IEEE Access*, vol. 6, pp. 15679–15701, 2018.
[7] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, Apr. 2019.
[8] F. Al-Turjman and M. Abujubbeh, "IoT-enabled smart grid via SM: An overview," *Future Gener. Comput. Syst.*, vol. 96, pp. 579–590, Jul. 2019.
[9] S. Dey, A. Roy, and S. Das, "Home automation using Internet of Things," in *Proc. IEEE 7th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2016, pp. 1–6.
[10] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar, and M. S. Obaidat, "An advanced Internet of Things based security alert system for smart home," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2017, pp. 25–29.
[11] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, Jun. 2019.
[12] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.
[13] A. Ouaddah, I. Bouij-Pasquier, A. Abou Elkalam, and A. Ait Ouahman, "Security analysis and proposal of new access control model in the Internet of Things," in *Proc. Int. Conf. Electr. Inf. Technol. (ICEIT)*, Mar. 2015, pp. 30–35.
[14] R. K. Saini, A. K. Dahiya, and P. Dahiya, "A survey on Internet of Things (IoT) applications and challenges for smart healthcare and farming," *Biosci. Biotechnol. Res. Commun.*, vol. 12, no. 4, pp. 1194–1200, 2019.
[15] L. Li, "Application of the Internet of Things in green agricultural products supply chain management," in *Proc. 4th Int. Conf. Intell. Comput. Technol. Autom.*, Mar. 2011, pp. 1022–1025.
[16] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, Mar. 2016, pp. 1–4.
[17] S.-P. Tseng, B.-R. Li, J.-L. Pan, and C.-J. Lin, "An application of Internet of Things with motion sensing on smart house," in *Proc. Int. Conf. Orange Technol.*, Sep. 2014, pp. 65–68.
[18] I. Ganchev, Z. Ji, and M. O'Droma, "A generic IoT architecture for smart cities," in *Proc. 25th IET Irish Signals & Syst. Conf., China-Ireland Int. Conf. Inf. Commun. Technol. (ISSC/CIICT)*, Limerick, Ireland, 2014, pp. 196–199
[19] S. Li, L. Xu, and S. Zhao, "The Internet of Things: A survey," *Inf. Syst. Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.
[20] C. Zhang and R. Green, "Communication security in Internet of Things: Preventive measure and avoid DDoS attack over IoT network," in *Proc. 18th Symp. Commun. Netw.*, 2015, pp. 8–15.
[21] D. Zhang, L. T. Yang, and H. Huang, "Searching in Internet of Things: Vision and challenges," in *Proc. IEEE 9th Int. Symp. Parallel Distrib. Process. With Appl.*, May 2011, pp. 201–206.
[22] R. H. Weber, "Internet of Things-new security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, 2010.
[23] 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.
[24] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[25] J. H. Kim, "6G and Internet of Things: A survey," *J. Manage. Anal.*, vol. 8, no. 2, pp. 316–332, Apr. 2021.
[26] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, Jul. 2020, Art. no. 102630.
[27] E. Almazrouei, R. M. Shubair, and F. Saffre, "Internet of NanoThings: Concepts and applications," 2018, *arXiv:1809.08914*.
[28] E. Ahmed, "The role of big data analytics in Internet of Things," *Comput. Netw.*, vol. 129, pp. 459–471, Dec. 2017.
[29] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Dec. 2017.
[30] C. W. Tsai, C. F. Lai, and A. V. Vasilakos, "Future Internet of Things: Open issues and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2201–2217, 2014.
[31] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Secur.*, Dec. 2013, pp. 663–667.
[32] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Frontiers Inf. Technol.*, Dec. 2012, pp. 257–260.
[33] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. V5-484–V5-487.
[34] I. A. Halepoto, U. A. Khan, and A. A. Arain, "Retransmission policies for efficient communication in IoT applications," in *Proc. IEEE 6th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2018, pp. 197–202.
[35] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[36] S. Severi, F. Sottile, G. Abreu, C. Pastrone, M. Spirito, and F. Berens, "M2M technologies: Enablers for a pervasive Internet of Things," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2014, pp. 1–5.

[37] Q. M. Quadir, 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.

[38] A. O. Barznji, T. A. Rashid, and N. K. Al-Salihi, "Computer network simulation of firewall and VoIP performance monitoring," *Int. J. Online Eng. (iJOE)*, vol. 14, no. 9, p. 4, Sep. 2018.

[39] T. A. Rashid and A. O. Barznji, "A virtualized computer network for salahaddin university new campus of HTTP services using OPNET simulator," in *Online Engineering & Internet of Things*, vol. 22. Cham, Switzerland: Springer, 2018, pp. 731–740, doi: 10.1007/978-3-319-64352-6_69.

[40] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha, "Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10474–10498, Jul. 2021.

[41] A. Shilpa, V. Muneeswaran, D. D. K. Rathinam, G. A. Santhiya, and J. Sherin, "Exploring the benefits of sensors in internet of everything (IoE)," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2019, pp. 510–514.

[42] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of Nano Things (IoNT)," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2015, pp. 219–224.

[43] X. Li and L. D. Xu, "A review of Internet of Things—Resource allocation," *IEEE Internet Things J.*, vol. 8, no. 11, pp. 8657–8666, Jun. 2021.

[44] M. H. Miraz, S. Khan, M. Bhuiyan, and P. S. Excell, "Mobile academy: A ubiquitous mobile learning (mLearning) platform," in *Proc. Int. Conf. eBus., eCommerce, eManage., eLearn. eGovernance (IC5E)*. London, U.K.: Held Univ. Greenwich, 2014, pp. 89–95.

[45] S. Khan, M. Al Shayokh, M. H. Miraz, and M. Bhuiyan, "A framework for Android based shopping mall applications," in *Proc. Int. Conf. eBus., eCommerce, eManage., eLearn. eGovernance*, vol. 1, 2014, Art. no. 12181.

[46] D. Laney, "3D data management: Controlling data, volume, velocity and variety," *META Group Res. Note*, vol. 6, no. 70, p. 1, 2001.

[47] A. Gandomi and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics," *Int. J. Inf. Manage.*, vol. 35, no. 2, pp. 137–144, 2015.

[48] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 171–209, Apr. 2014.

[49] A. Gani, A. Siddiqa, S. Shamshirband, and F. Hanum, "A survey on indexing techniques for big data: Taxonomy and performance evaluation," *Knowl. Inf. Syst.*, vol. 46, no. 2, pp. 241–284, 2016.

[50] M. Aazam, I. Khan, A. A. Alsaffar, and E.-N. Huh, "Cloud of things: Integrating Internet of Things and cloud computing and the issues involved," in *Proc. 11th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*. Islamabad, Pakistan, Jan. 2014, pp. 414–419.

[51] M. Aazam, P. P. Hung, and E.-N. Huh, "Smart gateway based communication for cloud of things," in *Proc. IEEE 9th Int. Conf. Intell. Sensors, Sensor Netw. Inf. Process. (ISSNIP)*, Apr. 2014, pp. 1–6.

[52] M. Aazam, E.-N. Huh, M. St-Hilaire, C.-H. Lung, and I. Lambadaris, "Cloud of things: Integration of IoT with cloud computing," in *Robots Sensor Clouds*. Cham, Switzerland: Springer, 2016, pp. 77–94.

[53] A. Botta, W. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generat. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.

[54] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[55] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. Choo, and M. Dlodlo, "From cloud to fog computing: A review and a conceptual live VM migration framework," *IEEE Access*, vol. 5, pp. 8284–8300, 2017.

[56] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[57] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on Internet of Things and cloud computing for healthcare," *Electronics*, vol. 8, p. 768, Jul. 2019.

[58] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the Internet of Things: A survey," *ACM Trans. Internet Technol.*, vol. 19, pp. 1–41, Apr. 2019.

[59] 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.

[60] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019.

[61] O. Vermesan, "Internet of robotic things: Converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT platforms," in *Cognitive Hyperconnected Digital Transformation*. U.K.: Taylor & Francis 2017.

[62] G. Manogaran, N. Chilamkurti, and C.-H. Hsu, "Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks," *Pers. Ubiquitous Comput.*, vol. 22, nos. 5–6, pp. 879–882, Oct. 2018.

[63] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[64] F. Al-Turjman, M. H. Nawaz, and U. D. Ulusar, "Intelligence in the Internet of Medical Things era: A systematic review of current and future trends," *Comput. Commun.*, vol. 150, pp. 644–660, Jan. 2020.

[65] F. Qureshi and S. Krishnan, "Wearable hardware design for the Internet of Medical Things (IoMT)," *Sensors*, vol. 18, no. 11, pp. 1–21, 2018.

[66] F. Al-Turjman, "Intelligence and security in big 5G-oriented IoNT: An overview," *Future Gener. Comput. Syst.*, vol. 102, pp. 357–368, Jan. 2019.

[67] M. Miraz, M. Ali, P. Excell, and R. Picking, "Internet of nano-things, things and everything: Future growth trends," *Future Internet*, vol. 10, no. 8, p. 68, Jul. 2018.

[68] A. Nayyar, V. Puri, and D.-N. Le, "Internet of Nano Things (IoNT): Next evolutionary step in nanotechnology," *Nanosci. Nanotechnol.*, vol. 7, no. 1, pp. 4–8, 2017.

[69] A. Rizwan, "A review on the role of nano-communication in future healthcare systems: A big data analytics perspective," *IEEE Access*, vol. 6, pp. 41903–41920, 2018.

[70] S. Ghafoor, N. Boujnah, M. Husain Rehmani, and A. Davy, "MAC protocols for terahertz communication: A comprehensive survey," 2019, *arXiv:1904.11441*.

[71] S. Ghafoor, N. Boujnah, M. H. Rehmani, and A. Davy, "MAC protocols for terahertz communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2236–2282, 4th Quart., 2020.

[72] K. Tekbıyık, A. R. Ekti, G. K. Kurt, and A. Görçin, "Terahertz band communication systems: Challenges, novelties and standardization efforts," *Phys. Commun.*, vol. 35, Aug. 2019, Art. no. 100700.

[73] H. Mohammad and R. M. Shubair, "Nanoscale communication: State-of-art and recent advances," 2019, *arXiv:1905.07722*.

[74] K. Yang, D. Bi, Y. Deng, R. Zhang, M. M. Ur Rahman, N. A. Ali, M. A. Imran, J. M. Jornet, Q. H. Abbasi, and A. Alomainy, "A comprehensive survey on hybrid communication for Internet of Nano-Things in context of body-centric communications," 2019, *arXiv:1912.09424*.

[75] K. P. Saharan and A. Kumar, "Fog in comparison to cloud: A survey," *Int. J. Comput. Appl.*, vol. 122, no. 3, pp. 10–12, Jul. 2015.

[76] A. Ghazizadeh, "Cloud computing benefits and architecture in E-learning," in *Proc. IEEE 7th Int. Conf. Wireless, Mobile Ubiquitous Technol. Educ.*, Mar. 2012, pp. 199–201.

[77] S. Ashraf, T. Kehkashan, M. Gull, and S. Moin u Din, "Transparency service model for data security in cloud computing," in *Proc. Int. Conf. Comput., Math. Eng. Technol. (iCoMET)*, Mar. 2018, pp. 1–6.

[78] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog computing: A taxonomy, survey and future directions," in *Internet Everything*. Cham, Switzerland: Springer, 2018, pp. 103–130.

[79] G. Fortino, D. Parisi, V. Pirrone, and G. Di Fatta, "BodyCloud: A SaaS approach for community body sensor networks," *Future Gener. Comput. Syst.*, vol. 35, pp. 62–79, Jun. 2014.

[80] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," *Int. J. Eng. Res. Appl.*, vol. 3, no. 4, pp. 1922–1926, 2013.

[81] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing-the business perspective," *Decis. Support Syst.*, vol. 51, no. 1, pp. 176–189, 2011.

[82] J. Yang, "Cloud computing for storing and analyzing petabytes of genomic data," *J. Ind. Inf. Integr.*, vol. 15, pp. 50–57, Sep. 2019.

[83] F. Y. Okay and S. Ozdemir, "A fog computing based smart grid model," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2016, pp. 1–6.

[84] O. Diallo, J. J. P. C. Rodrigues, M. Sene, and J. Niu, "Real-time query processing optimization for cloud-based wireless body area networks," *Inf. Sci.*, vol. 284, pp. 84–94, Nov. 2014.

[85] A. Ibaida, D. Al-Shammary, and I. Khalil, "Cloud enabled fractal based ECG compression in wireless body sensor networks," *Future Gener. Comput. Syst.*, vol. 35, pp. 91–101, Jun. 2014.

[86] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "Iot-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, Jan. 2017.

[87] R. Ranjan, D. Thakker, A. Haller, and R. Buyya, *A Note on Exploration of IoT Generated Big Data Using Semantics*. Amsterdam, The Netherlands: Elsevier, 2017.

[88] Y. Ma, L. Wang, A. Y. Zomaya, D. Chen, and R. Ranjan, "Task-tree based large-scale mosaicking for massive remote sensed imageries with dynamic DAG scheduling," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2126–2137, Aug. 2014.

[89] S. Horrow and A. Sardana, "Identity management framework for cloud based Internet of Things," in *Proc. 1st Int. Conf. Secur. Internet Things*, Aug. 2012, pp. 200–203.

[90] S. Horrow, S. Gupta, A. Sardana, and A. Abraham, "Secure private cloud architecture for mobile infrastructure as a service," in *Proc. IEEE 8th World Congr. Services*, Jun. 2012, pp. 149–154.

[91] B. D. Deebak and F. AL-Turjman, "Lightweight authentication for IoT/Cloud-based forensics in intelligent data computing," *Future Gener. Comput. Syst.*, vol. 116, pp. 406–425, Mar. 2021.

[92] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 1, pp. 420–438, Jan. 2021.

[93] N. Xie, W. Tan, X. Zheng, L. Zhao, L. Huang, and Y. Sun, "An efficient two-phase approach for reliable collaboration-aware service composition in cloud manufacturing," *J. Ind. Inf. Integr.*, vol. 23, Sep. 2021, Art. no. 100211.

[94] V. W. Wong, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[95] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, and D. S. Nikolopoulos, "Challenges and opportunities in edge computing," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Nov. 2016, pp. 20–26.

[96] P. G. Lopez, *Edge-Centric Computing: Vision and Challenges*. New York, NY, USA: ACM, 2015.

[97] K. Kaur and M. Sachdeva, "Fog computing in IoT: An overview of new opportunities," in *Proc. ICETIT*. Cham, Switzerland: Springer, 2020, pp. 59–68.

[98] S. Dustdar, C. Avasalcai, and I. Murturi, "Invited paper: Edge and fog computing: Vision and research challenges," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, pp. 96–9609.

[99] S. Rani, A. Kataria, and M. Chauhan, "Fog computing in industry 4.0: Applications and challenges—A research roadmap," in *Energy Conservation Solutions for Fog-Edge Computing Paradigms*. Cham, Switzerland: Springer, 2022, pp. 173–190.

[100] C. Liu, F. Xiang, P. Wang, and Z. Sun, "A review of issues and challenges in fog computing environment," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber. Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 232–237.

[101] T. Wang, "Edge-computing-based trustworthy data collection model in the Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4218–4227, May 2020.

[102] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2054–2062, Mar. 2020.

[103] X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, and L. Qi, "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Gener. Comput. Syst.*, vol. 95, pp. 522–533, Jun. 2019.

[104] H. Shah-Mansouri and V. W. S. Wong, "Hierarchical fog-cloud computing for IoT systems: A computation offloading game," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3246–3257, Aug. 2018.

[105] H. Tan, Z. Han, X.-Y. Li, and F. C. M. Lau, "Online job dispatching and scheduling in edge-clouds," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[106] Y. Xiao and M. Krunz, "QoE and power efficiency tradeoff for fog computing networks with fog node cooperation," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2017, pp. 1–9.

[107] M. S. Elbamby, M. Bennis, and W. Saad, "Proactive edge computing in latency-constrained fog networks," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2017, pp. 1–6.

[108] G. Lee, W. Saad, and M. Bennis, "An online secretary framework for fog network formation with minimal latency," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[109] X. Chen and J. Zhang, "When D2D meets cloud: Hybrid mobile task offloadings in fog computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[110] X. Meng, W. Wang, and Z. Zhang, "Delay-constrained hybrid computation offloading with cloud and fog computing," *IEEE Access*, vol. 5, pp. 21355–21367, 2017.

[111] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, "Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1171–1181, Dec. 2016.

[112] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[113] A. Gorkhali, L. Li, and A. Shrestha, "Blockchain: A literature review," *J. Manag. Anal.*, vol. 7, no. 3, pp. 321–343, 2020.

[114] S. Nakamoto and A. Bitcoin. (2008). *A Peer-to-Peer Electronic Cash System*. Bitcoin. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[115] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[116] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[117] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[118] B. Chase and E. MacBrough, "Analysis of the XRP ledger consensus protocol," 2018, *arXiv:1802.07242*.

[119] F. R. Yu, J. Liu, Y. He, P. Si, and Y. Zhang, "Virtualization for distributed ledger technology (vDLT)," *IEEE Access*, vol. 6, pp. 25019–25028, 2018.

[120] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, Oct. 2017, pp. 51–68.

[121] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "BlockBench: A framework for analyzing private blockchains," in *Proc. ACM Int. Conf. Manage. Data*, 2017, pp. 1085–1100.

[122] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[123] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: A survey," *Comput. Electr. Eng.*, vol. 81, Jan. 2020, Art. no. 106526.

[124] K. Fan, S. Sun, Z. Yan, Q. Pan, H. Li, and Y. Yang, "A blockchain-based clock synchronization scheme in IoT," *Future Gener. Comput. Syst.*, vol. 101, pp. 524–533, Dec. 2019.

[125] J. D. C. Silva, J. J. Rodrigues, J. Al-Muhtadi, R. A. Rabêlo, and V. Furtado, "Management platforms and protocols for Internet of Things: A survey," *Sensors*, vol. 19, no. 3, p. 676, 2019.

[126] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[127] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks Money*. Cham, Switzerland: Springer, 2016, pp. 239–278.

[128] G. Foroglou and A.-L. Tsilidou, "Further applications of the blockchain," in *Proc. 12th Student Conf. Managerial Sci. Technol.*, 2015, pp. 1–8.

[129] G. W. Peters, E. Panayi, and A. Chapelle, "Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective," *SSRN Electron. J.*, pp. 1–25, Aug. 2015.

[130] W. Viriyasitavat, L. D. Xu, Z. Bi, and V. Pungpapong, "Blockchain and Internet of Things for modern business process in digital Economy—The state of the art," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1420–1432, Dec. 2019.

[131] L. D. Xu and W. Viriyasitavat, "Application of blockchain in collaborative Internet-of-Things services," *IEEE Trans. Computat. Social Syst.*, vol. 6, no. 6, pp. 1295–1305, Dec. 2019.

[132] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[133] J. Wang, K. Han, A. Alexandridis, Z. Chen, Z. Zilic, Y. Pang, G. Jeon, and F. Piccialli, "A blockchain-based eHealthcare system interoperating with WBANs," *Future Gener. Comput. Syst.*, vol. 110, pp. 675–685, Sep. 2020.

[134] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4671–4679, Jun. 2019.

[135] P. Danzi, A. E. Kalor, C. Stefanovic, and P. Popovski, "Analysis of the communication traffic for blockchain synchronization of IoT devices," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7.

[136] W. Dong and X. Liu, "Robust and secure time-synchronization against Sybil attacks for sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1482–1491, Dec. 2015.

[137] J. He, J. Chen, P. Cheng, and X. Cao, "Secure time synchronization in wirelesssensor networks: A maximumconsensus-based approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 4, pp. 1055–1065, Apr. 2014.

[138] M. Akhlaq and T. R. Sheltami, "RTSP: An accurate and energy-efficient protocol for clock synchronization in WSNs," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 3, pp. 578–589, Mar. 2013.

[139] L. Schenato and F. Fiorentin, "Average TimeSynch: A consensus-based protocol for clock synchronization in wireless sensor networks," *Automatica*, vol. 47, no. 9, pp. 1878–1886, Sep. 2011.

[140] S. Hong, "P2P networking based Internet of Things (IoT) sensor node authentication by blockchain," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 579–589, Mar. 2020.

[141] S. Nanayakkara, M. N. N. Rodrigo, S. Perera, G. T. Weerasuriya, and A. A. Hijazi, "A methodology for selection of a blockchain platform to develop an enterprise system," *J. Ind. Inf. Integr.*, vol. 23, Sep. 2021, Art. no. 100215.

[142] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 464–467.

[143] C. Machado and A. A. Medeiros Frohlich, "IoT data integrity verification for cyber-physical systems using blockchain," in *Proc. IEEE 21st Int. Symp. Real-Time Distrib. Comput. (ISORC)*, May 2018, pp. 83–90.

[144] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.

[145] L. D. Nguyen, I. Leyva-Mayorga, A. N. Lewis, and P. Popovski, "Modeling and analysis of data trading on blockchain-based market in IoT networks," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6487–6497, Apr. 2021.

[146] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for Internet of Things," *Sensors*, vol. 21, no. 3, p. 772, Jan. 2021.

[147] Y. Lu, "Artificial intelligence: A survey on evolution, models, applications and future trends," *J. Manage. Analytics*, vol. 6, no. 1, pp. 1–29, Jan. 2019.

[148] 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.

[149] F. Alam, R. Mehmood, I. Katib, and A. Albeshri, "Analysis of eight data mining algorithms for smarter Internet of Things (IoT)," *Proc. Comput. Sci.*, vol. 98, pp. 437–442, Jan. 2016.

[150] S. Naveen and M. R. Kounte, "In search of the future technologies: Fusion of machine learning, fog and edge computing in the Internet of Things," in *Proc. Int. Conf. Comput. Netw., Big Data IoT*. Cham, Switzerland: Springer, 2018, pp. 278–285.

[151] K. Guo, Y. Lu, H. Gao, and R. Cao, "Artificial intelligence-based semantic Internet of Things in a user-centric smart city," *Sensors*, vol. 18, no. 5, p. 1341, Apr. 2018.

[152] X. Wang, X. Wang, S. Mao, J. Zhang, S. C. G. Periaswamy, and J. Patton, "Indoor radio map construction and localization with deep Gaussian processes," *IEEE Internet Things J.*, vol. 7, no. 11, pp. 11238–11249, Nov. 2020.

[153] J. Lin, W.-M. Chen, Y. Lin, J. Cohn, C. Gan, and S. Han, "MCUNet: Tiny deep learning on IoT devices," 2020, *arXiv:2007.10319*.

[154] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102252.

[155] D. D. A. Rodrigues, R. F. Ivo, S. C. Satapathy, S. Wang, J. Hemanth, and P. P. R. Filho, "A new approach for classification skin lesion based on transfer learning, deep learning, and IoT system," *Pattern Recognit. Lett.*, vol. 136, pp. 8–15, Aug. 2020.

[156] X. Liu, H. Li, G. Xu, S. Liu, Z. Liu, and R. Lu, "PADL: Privacy-aware and asynchronous deep learning for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6955–6969, Aug. 2020.

[157] M. Elhoseny, M. M. Selim, and K. Shankar, "Optimal deep learning based convolution neural network for digital forensics face sketch synthesis in Internet of Things (IoT)," *Int. J. Mach. Learn. Cybern.*, vol. 12, pp. 3249–3260, Nov. 2020.

[158] M. Price, J. Glass, and A. P. Chandrakasan, "14.4 A scalable speech recognizer with deep-neural-network acoustic models and voice-activated power gating," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 244–245.

[159] X. Wang, L. Gao, S. Mao, and S. Pandey, "DeepFi: Deep learning for indoor fingerprinting using channel state information," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2015, pp. 1666–1671.

[160] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.

[161] 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.

[162] P. S. Pandey, "Machine learning and IoT for prediction and detection of stress," in *Proc. 17th Int. Conf. Comput. Sci. Its Appl. (ICCSA)*, Jul. 2017, pp. 1–5.

[163] A. L. Diedrichs, F. Bromberg, D. Dujovne, K. Brun-Laguna, and T. Watteyne, "Prediction of frost events using machine learning and IoT sensing devices," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4589–4597, Dec. 2018.

[164] N. Baracaldo, B. Chen, H. Ludwig, A. Safavi, and R. Zhang, "Detecting poisoning attacks on machine learning in IoT environments," in *Proc. IEEE Int. Congr. Internet Things (ICIOT)*, Jul. 2018, pp. 57–64.

[165] X. Huang, K. Xie, S. Leng, T. Yuan, and M. Ma, "Improving quality of experience in multimedia Internet of Things leveraging machine learning on big data," *Future Gener. Comput. Syst.*, vol. 86, pp. 1413–1423, Sep. 2018.

[166] M. Azeem, A. Haleem, and M. Javaid, "Symbiotic relationship between machine learning and Industry 4.0: A review," *J. Ind. Integr. Manage.*, vol. 7, no. 3, pp. 401–433, 2021.

[167] H. Chen, L. Li, and Y. Chen, "Explore success factors that impact artificial intelligence adoption on telecom industry in China," *J. Manage. Anal.*, vol. 8, no. 1, pp. 36–68, Jan. 2021.

[168] S. Rathore, Y. Pan, and J. H. Park, "BlockDeepNet: A blockchain-based secure deep learning for IoT network," *Sustainability*, vol. 11, no. 14, p. 3974, Jul. 2019.

[169] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, Oct. 2019.

[170] S. Rathore and J. H. Park, "Semi-supervised learning based distributed attack detection framework for IoT," *Appl. Soft Comput.*, vol. 72, pp. 79–89, Nov. 2018.

[171] S. Rathore, P. K. Sharma, A. K. Sangaiah, and J. J. Park, "A hesitant fuzzy based security approach for fog and mobile-edge computing," *IEEE Access*, vol. 6, pp. 688–701, 2018.

[172] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.

[173] I. Afanasyev, M. Mazzara, S. Chakraborty, N. Zhuchkov, A. Maksatbek, A. Yesildirek, M. Kassab, and S. Distefano, "Towards the internet of robotic things: Analysis, architecture, components and challenges," in *Proc. 12th Int. Conf. Develop. eSyst. Eng. (DeSE)*, Oct. 2019, pp. 3–8.

[174] P. Simoens, M. Dragone, and A. Saffiotti, "The internet of robotic things: A review of concept, added value and applications," *Int. J. Adv. Robotic Syst.*, vol. 15, no. 1, 2018, Art. no. 1729881418759424.

[175] R. S. Batth, A. Nayyar, and A. Nagpal, "Internet of robotic things: Driving intelligent robotics of future–concept, architecture, applications and technologies," in *Proc. 4th Int. Conf. Comput. Sci. (ICCS)*, Aug. 2018, pp. 151–160.

[176] P. P. Ray, "Internet of robotic things: Concept, technologies, and challenges," *IEEE Access*, vol. 4, pp. 9489–9500, 2016.

[177] W. M. Lafta, A. A. Alkadhmawee, and M. A. Altaha, "Best strategy to control data on internet-of-robotic-things in heterogeneous networks," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 2, pp. 1830–1838, 2021.
[178] Y. Liu, W. Zhang, S. Pan, Y. Li, and Y. Chen, "Analyzing the robotic behavior in a smart city with deep enforcement and imitation learning using IoRT," *Comput. Commun.*, vol. 150, pp. 346–356, Jan. 2020.
[179] B. Siciliano and O. Khatib, *Springer Handbook of Robotics*. Cham, Switzerland: Springer, 2016.
[180] M. A. Al-Taee, W. Al-Nuaimy, Z. J. Muhsin, and A. Al-Ataby, "Robot assistant in management of diabetes in children based on the Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 437–445, Apr. 2017.
[181] C. Mahieu, F. Ongenae, F. De Backere, P. Bonte, F. D. Turck, and P. Simoens, "Semantics-based platform for context-aware and personalized robot interaction in the internet of robotic things," *J. Syst. Softw.*, vol. 149, pp. 138–157, Mar. 2019.
[182] M. H. Abbasi, B. Majidi, M. Eshghi, and E. H. Abbasi, "Deep visual privacy preserving for Internet of robotic things," in *Proc. 5th Conf. Knowl. Based Eng. Innov. (KBEI)*, Feb. 2019, pp. 292–296.
[183] F. T. Zuhra, K. A. Bakar, A. Ahmed, and M. A. Tunio, "Routing protocols in wireless body sensor networks: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 99, pp. 73–97, Dec. 2017.
[184] F. T. Zuhra, K. B. A. Bakar, A. A. Arain, K. M. Almustafa, T. Saba, K. Haseeb, and N. Islam, "LLTP-QoS: Low latency traffic prioritization and QoS-aware routing in wireless body sensor networks," *IEEE Access*, vol. 7, pp. 152777–152787, 2019.
[185] F. T. Zuhra, K. B. A. Bakar, A. A. Arain, U. A. Khan, and A. R. Bhangwar, "MIQoS-RP: Multi-constraint intra-BAN, QoS-aware routing protocol for wireless body sensor networks," *IEEE Access*, vol. 8, pp. 99880–99888, 2020.
[186] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of Medical Things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.
[187] R. Basatneh, B. Najafi, and D. G. Armstrong, "Health sensors, smart home devices, and the Internet of Medical Things: An opportunity for dramatic improvement in care for the lower extremity complications of diabetes," *J. Diabetes Sci. Technol.*, vol. 12, no. 3, pp. 577–586, May 2018.
[188] A. Onasanya and M. Elshakankiri, "Smart integrated IoT healthcare system for cancer care," *Wireless Netw.*, vol. 27, pp. 4297–4312, Jan. 2019.
[189] R. P. Singh, M. Javaid, A. Haleem, R. Vaishya, and S. R. Ali, "Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," *J. Clin. Orthopaedics Trauma*, vol. 11, no. 4, pp. 713–717, 2020.
[190] I. V. Pustokhina, D. A. Pustokhin, D. Gupta, A. Khanna, K. Shankar, and G. N. Nguyen, "An effective training scheme for deep neural network in edge computing enabled Internet of Medical Things (IoMT) systems," *IEEE Access*, vol. 8, pp. 107112–107123, 2020.
[191] J. J. Jijesh, "A supervised learning based decision support system for multi-sensor healthcare data from wireless body sensor networks," *Wireless Pers. Commun.*, vol. 116, pp. 1795–1813, Feb. 2020.
[192] J. Cecil, A. Gupta, M. Pirela-Cruz, and P. Ramanathan, "An IoMT based cyber training framework for orthopedic surgery using next generation internet technologies," *Informat. Med. Unlocked*, vol. 12, pp. 128–137, 2018.
[193] M. A. Bilal and M. A. Hassan, "A distributed secure framework for sharing patient's data among IoMT devices," *Pakistan J. Eng. Appl. Sci.*, vol. 24, no. 1, pp. 89–100, 2019.
[194] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, Jul. 2020.
[195] X. Li, H.-N. Dai, Q. Wang, M. Imran, D. Li, and M. A. Imran, "Securing Internet of Medical Things with friendly-jamming schemes," *Comput. Commun.*, vol. 160, pp. 431–442, Jul. 2020.
[196] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of Internet of Health Things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.
[197] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. 7th Int. Symp. Parallel Archit., Algorithms Program. (PAAP)*, Dec. 2015, pp. 217–222.
[198] J.-X. Hu, C.-L. Chen, C.-L. Fan, and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," *J. Sensors*, vol. 2017, pp. 1–11, 2017.
[199] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: Securing Internet of Medical Things (IoMT)," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 82–89, 2019.
[200] A. Lounis, A. Hadjidj, A. Bouabdallah, and Y. Challal, "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks," *Future Gener. Comput. Syst.*, vol. 55, pp. 266–277, Feb. 2016.
[201] M. R. Abdmeziem and D. Tandjaoui, "A cooperative end to end key management scheme for e-health applications in the context of Internet of Things," *Ad-Hoc Netw. Wireless*. Cham, Switzerland: Springer, 2014, pp. 35–46.
[202] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *J. Med. Syst.*, vol. 40, no. 5, pp. 1–15, May 2016.
[203] N. Taniguchi, "On the basic concept of nanotechnology," in *Proc. Int. Conf. Prod. Eng.*, Tokyo, Japan, Aug. 1974
[204] C. P. Poole and F. J. Owens, *Introduction to Nanotechnology*. Hoboken, NJ, USA: Wiley, 2003.
[205] J. P. Giraldo, H. Wu, G. M. Newkirk, and S. Kruss, "Nanobiotechnology approaches for engineering smart plant sensors," *Nature Nanotechnol.*, vol. 14, no. 6, pp. 541–553, Jun. 2019.
[206] X. Qu, P. J. J. Alvarez, and Q. Li, "Applications of nanotechnology in water and wastewater treatment," *Water Res.*, vol. 47, no. 12, pp. 3931–3946, Aug. 2013.
[207] D. M. Smith, J. K. Simon, and J. R. Baker Jr., "Applications of nanotechnology for immunology," *Nature Rev. Immunol.*, vol. 13, no. 8, pp. 592–605, Aug. 2013.
[208] T. J. Webster and I. Seil, "Antimicrobial applications of nanotechnology: Methods and literature," *Int. J. Nanomed.*, vol. 7, p. 2767, Jun. 2012.
[209] T. V. Duncan, "Applications of nanotechnology in food packaging and food safety: Barrier materials, antimicrobials and sensors," *J. Colloid Interface Sci.*, vol. 363, no. 1, pp. 1–24, Nov. 2011.
[210] P. J. Bartos, "Nanotechnology in construction: A roadmap for development," in *Nanotechnology in Construction*. Cham, Switzerland: Springer, 2009, pp. 15–26.
[211] Z. Bittnar, P. J. Bartos, J. Nemecek, V. Smilauer, and J. Zeman, *Nanotechnology in Construction: Proceedings of the NICOM3*. Cham, Switzerland: Springer, 2009.
[212] K. L. Scrivener and R. J. Kirkpatrick, "Innovation in use and research on cementitious material," *Cement Concrete Res.*, vol. 38, no. 2, pp. 128–136, Feb. 2008.
[213] M. P. Hughes, "AC electrokinetics: Applications for nanotechnology," *Nanotechnology*, vol. 11, no. 2, pp. 124–132, Jun. 2000.
[214] F. Sanchez and K. Sobolev, "Nanotechnology in concrete—A review," *Construct. Building Mater.*, vol. 24, no. 11, pp. 2060–2071, 2010.
[215] K. Sobolev and M. F. Gutierrez, "How nanotechnology can change the concrete world: Part two of a two-part series," *Amer. Ceram. Soc. Bull.*, vol. 84, no. 11, pp. 16–19, 2005.
[216] I. F. Akyildiz and J. M. Jornet, "The Internet of Nano-Things," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 58–63, Dec. 2010.
[217] F. Al-Turjman, "A rational data delivery framework for disaster-inspired Internet of Nano-Things (IoNT) in practice," *Cluster Comput.*, vol. 22, no. S1, pp. 1751–1763, Jan. 2019.
[218] S. Canovas-Carrasco, R. M. Sandoval, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "Optimal transmission policy derivation for IoNT flow-guided nano-sensor networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2288–2298, Apr. 2019.
[219] S. Canovas-Carrasco, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "A nanoscale communication network scheme and energy model for a human hand scenario," *Nano Commun. Netw.*, vol. 15, pp. 17–27, Mar. 2018.
[220] N. Hassan, C. T. Chou, and M. Hassan, "ENEUTRAL IoNT: Energy-neutral event monitoring for Internet of Nano Things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2379–2389, Apr. 2019.
[221] S. J. Lee, C. Jung, K. Choi, and S. Kim, "Design of wireless nanosensor networks for intrabody application," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 7, Jul. 2015, Art. no. 176761.
[222] S. Javaid, Z. Wu, H. Fahim, M. M. S. Fareed, and F. Javed, "Exploiting temporal correlation mechanism for designing temperature-aware energy-efficient routing protocol for intrabody nanonetworks," *IEEE Access*, vol. 8, pp. 75906–75924, 2020.

[223] J. Xu, Y. Zhang, J. Jiang, and J. Kan, "An energy balance clustering routing protocol for intra-body wireless nanosensor networks," *Sensors*, vol. 19, no. 22, p. 4875, Nov. 2019.
[224] A. Vavouris, F. Dervisi, V. Papanikolaou, P. Diamantoulakis, G. Karagiannidis, and S. Goudos, "An energy efficient modulation scheme for body-centric terahertz (THz) nanonetworks," *Technologies*, vol. 7, no. 1, p. 14, Jan. 2019.
[225] V. K. Papanikolaou and G. K. Karagiannidis, "Channel modeling of in-vivo THz nanonetworks: State-of-the-art and research challenges," in *Proc. Int. Conf. Wireless Mobile Commun. Healthcare*. Cham, Switzerland: Springer, 2017, pp. 50–57.
[226] H. Elayan, R. M. Shubair, J. M. Jornet, and R. Mittra, "Multi-layer intrabody terahertz wave propagation model for nanobiosensing applications," *Nano Commun. Netw.*, vol. 14, pp. 9–15, Dec. 2017.
[227] J. Jarmakiewicz, K. Parobczak, and K. Maslanka, "On the Internet of Nano Things in healthcare network," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2016, pp. 1–6.
[228] B. E. Usibe, A. Menkiti, M. U. Onuu, and J. C. Ogbulezie, "Development and analysis of a potential nanosensor communication network using carbon nanotubes," *Int. J.*, vol. 3, no. 1, pp. 4–10, 2013.
[229] V. Upadhayay, "Application of wireless nano sensor networks for wild lives," *Int. J. Distrib. Parallel Syst.*, vol. 3, no. 4, pp. 173–181, Jul. 2012.
[230] K. Tsujimura, K. Umebayashi, J. Kokkoniemi, and J. Lehtomaki, "Time domain channel model for the THz band," in *Proc. 16th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2019, pp. 446–449.
[231] Q. Xia, Z. Hossain, M. Medley, and J. M. Jornet, "A link-layer synchronization and medium access control protocol for terahertz-band communication networks," *IEEE Trans. Mobile Comput.*, vol. 20, no. 1, pp. 2–18, Jan. 2021.
[232] N. Nurain, B. M. S. B. Talukder, T. Choudhury, S. Tairin, M. Ferdousi, M. Naznin, and A. B. M. A. Al Islam, "Exploring network-level performances of wireless nanonetworks utilizing gains of different types of nano-antennas with different materials," *Wireless Netw.*, vol. 25, no. 5, pp. 2651–2664, Jul. 2019.
[233] H. Elayan, R. M. Shubair, A. Alomainy, and K. Yang, "In-vivo terahertz EM channel characterization for nano-communications in WBANs," in *Proc. IEEE Int. Symp. Antennas Propag. (APSURSI)*, Jun. 2016, pp. 979–980.
[234] S. Mumtaz, J. M. Jornet, J. Aulin, W. H. Gerstacker, X. Dong, and B. Ai, "Terahertz communication for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 5617–5625, Jul. 2017.
[235] T. Yasui, "Terahertz frequency metrology based on frequency comb techniques," in *Handbook of Terahertz Technology for Imaging, Sensing and Communications*. Amsterdam, The Netherlands: Elsevier, 2013, pp. 436–463.
[236] E. Lallas, "Key roles of plasmonics in wireless THz nanocommunications—A survey," *Appl. Sci.*, vol. 9, no. 24, p. 5488, Dec. 2019.
[237] H. Ferjani and H. Touati, "Efficient data dissemination in electromagnetic wireless nano-sensor networks," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 531–536.
[238] G. Piro, G. Boggia, and L. A. Grieco, "On the design of an energy-harvesting protocol stack for body area nano-NETworks," *Nano Commun. Netw.*, vol. 6, no. 2, pp. 74–84, Jun. 2015.
[239] O. Yalgashev, M. Bakhouya, J. Gaber, and M.-A. Manier, "Adaptive transmission range control for electromagnetic-based broadcasting in nanonetworks," *Proc. Comput. Sci.*, vol. 52, pp. 1077–1082, Jan. 2015.
[240] O. Yalgashev, *Towards Nanoscale Interconnect for System-on-Chip*. Meroux-Moval, France: Belfort-Montbéliard, 2015.
[241] A. Tsioliaridou, C. Liaskos, S. Ioannidis, and A. Pitsillides, "CORONA: A coordinate and routing system for nanonetworks," in *Proc. 2nd Annu. Int. Conf. Nanosc. Comput. Commun.*, Sep. 2015, pp. 1–6.
[242] J. Xu, R. Zhang, and Z. Wang, "An energy efficient multi-hop routing protocol for terahertz wireless nanosensor networks," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.* Cham, Switzerland: Springer, 2016, pp. 367–376.
[243] J. Xu, J. Jiang, Z. Wang, and Y. Zhao, "Energy harvesting multi-path routing for wireless multimedia nanosensor networks in terahertz band," in *Proc. 14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2018, pp. 1011–1017.
[244] M. Pierobon, J. M. Jornet, N. Akkari, S. Almasri, and I. F. Akyildiz, "A routing framework for energy harvesting wireless nanosensor networks in the terahertz band," *Wireless Netw.*, vol. 20, no. 5, pp. 1169–1183, Jul. 2014.
[245] S. Mohrehkesh and M. C. Weigle, "Optimizing energy consumption in terahertz band nanonetworks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 12, pp. 2432–2441, Dec. 2014.
[246] W.-L. Wang, C.-C. Wang, and X.-W. Yao, "Slot self-allocation based MAC protocol for energy harvesting nano-networks," *Sensors*, vol. 19, no. 21, p. 4646, Oct. 2019.
[247] J. Xu, J. Kan, and Y. Zhang, "Centralized energy harvesting-based TDMA protocol for terahertz NanoSensor networks," *Sensors*, vol. 19, no. 20, p. 4508, Oct. 2019.
[248] H. Fahim, W. Li, S. Javaid, M. M. S. Fareed, G. Ahmed, and M. K. Khattak, "Fuzzy logic and bio-inspired firefly algorithm based routing scheme in intrabody nanonetworks," *Sensors*, vol. 19, no. 24, p. 5526, Dec. 2019.
[249] F. Afsana, M. Asif-Ur-Rahman, M. R. Ahmed, M. Mahmud, and M. S. Kaiser, "An energy conserving routing scheme for wireless body sensor nanonetwork communication," *IEEE Access*, vol. 6, pp. 9186–9200, 2018.
[250] *IoTCloud*. Accessed: Sep. 7, 2022. [Online]. Available: https://sites.google.com/site/opensourceiotcloud/
[251] *Temboo*. Accessed: Sep. 8, 2022. [Online]. Available: https://temboo.com/
[252] *OpenIoT*. Accessed: Sep. 8, 2022. [Online]. Available: http://www.openiot.eu/
[253] *IoT Toolkit*. Accessed: Aug. 19, 2022. [Online]. Available: http://iot-toolkit.com/
[254] *Arduino IoT Cloud*. Accessed: Dec. 10, 2021. [Online]. Available: https://www.arduino.cc/en/IoT/HomePage
[255] *Zetta*. Accessed: Jul. 8, 2022. [Online]. Available: https://www.zettajs.org/
[256] *Nimbits*. Accessed: Mar. 10, 2022. [Online]. Available: http://www.nimbits.com/
[257] *OpenPicus*. Accessed: Aug. 12, 2022. [Online]. Available: http://www.iot-a.eu/
[258] *Xively*. Accessed: Jan. 4, 2023. [Online]. Available: https://xively.com/
[259] *Open.Sen.se*. Accessed: Feb. 10, 2022. [Online]. Available: http://open.sen.se/
[260] *ThingSpeak*. Accessed: Apr. 18, 2022. [Online]. Available: https://thingspeak.com/
[261] *CloudPlugs*. Accessed: Jun. 19, 2022. [Online]. Available: http://cloudplugs.com/
[262] *Carriots*. Accessed: Nov. 2022. [Online]. Available: https://www.carriots.com
[263] *NetLab*. Accessed: Apr. 16, 2022. [Online]. Available: http://www.netlabtoolkit.org/learning/tutorials/iot-cloud-services/
[264] *Cloudera*. Accessed: Dec. 19, 2021. [Online]. Available: https://www.cloudera.com/products/cloudera-data-platform.html?tab=1
[265] *Block-Sim*. Accessed: Sep. 5, 2022. [Online]. Available: https://github.com/maher243/BlockSim#:~:text=BlockSim%20is%20an%20open%20source,incentives%20layers%20of%20blockchain%20systems
[266] *Nano-Sim*. Accessed: Mar. 15, 2022. [Online]. Available: http://www.bcgsc.ca/platform/bioinfo/software/nanosim
[267] *Dynatrace*. Accessed: May 20, 2022. [Online]. Available: https://www.dynatrace.com/platform/

KAMALRULNIZAM BIN ABU BAKAR received the B.Sc. degree in computer science from Universiti Teknologi Malaysia (UTM), Malaysia, in 1996, the M.Sc. degree in computer communications and networks from Leeds Metropolitan University, U.K., in 1998, and the Ph.D. degree in computer science from Aston University, U.K., in 2004. He is currently a Professor with the Department of Computer Science, UTM, and a member of the Pervasive Computing Research Group. He is involved in many research projects and a referee of several scientific journals and conferences. His research interests include mobile and wireless computing, ad hoc and sensor networks, information security, and grid computing. He is also a member of ACM, the Internet Society, and the International Association of Engineering.

FATIMA TUL ZUHRA received the bachelor's degree in computer science from the Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan, in 2009, the master's degree in computer science from the University of Malaya (UM), Malaysia, in 2016, and the Ph.D. degree in computer science from Universiti Teknologi Malaysia (UTM), Malaysia, in 2020. She worked as a Researcher with the School of Computing, UTM, under the high impact research and postdoctoral fellowship projects. Currently, she is working as an Assistant Professor, the Head of the Department of Information Technology, and the Manager of the Office of Research, Innovation and Commercialization (ORIC), Shaheed Benazir Bhutto University, Shaheed Benazirabad, Pakistan. She has 13 different research publications in various journals with 29.33 cumulative impact factor.

BABANGIDA ISYAKU received the B.Sc. degree in computer science and information system from Oxford Brookes University, in 2012, and the M.Sc. and Ph.D. degrees in computer science from Universiti Teknologi Malaysia (UTM), in 2017 and 2022, respectively. He works with Sule Lamido University, Kafin Hausa, Jigawa, Nigeria. He is currently a Researcher with Universiti Teknologi Malaysia, under the postdoctoral fellowship scheme. His research interests include software defined networks, routing, failure recovery, and flowtable management. He was a recipient of the Best Paper Award at the IEEE Symposium on Computer Applications and Industrial Electronics, in 2020, and the Best Postgraduate Student Award from the Faculty of Computing, UTM.

SAPIAH BINTI SULAIMAN received the Diploma degree in computer science, in 2001, the B.Sc. degree in information system engineering from Universiti Teknologi MARA, Malaysia, in 2004, and the M.Sc. degree in computer science from Universiti Teknologi Malaysia (UTM), Malaysia, in 2008. She is currently a Research Officer with UTM. She involves in and manages many research projects. Her research interests include information retrieval and information management.