IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 12 May 2024, accepted 12 June 2024, date of publication 24 June 2024, date of current version 9 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3418995

RESEARCH ARTICLE

Internet of Things (IoT): Origins, Embedded Technologies, Smart Applications, and Its Growth in the Last Decade

JAMEEL SHEHU YALLI[1], (Member, IEEE), MOHD HILMI HASAN[1], (Member, IEEE), AND AISHA ABUBAKAR BADAWI[2]

[1]Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, Perak 32610, Malaysia
[2]School for Computer Science and Informatics, De Montfort University, LE1 9BH Leicester, U.K.

Corresponding author: Jameel Shehu Yalli (jameel_20001035@utp.edu.my)

This work was supported by Yayasan Universiti Teknologi PETRONAS through Universiti Teknologi PETRONAS (UTP) under Grant 015PBC-027.

ABSTRACT The idea of the IoT began back in 1982 when a vending machine was connected to the internet, then to the concept of Mark Weiser in 1992, then RFID, and so on. A detailed evolution of the IoT and how it was transforming is given. Due to the wide embracement of IoT by industries and home users, it has become the cornerstone of the Information and Communication Technology (ICT) market. The market value of the IoT was worth $1.90 billion in 2018; $25 billion in 2020; $925.2 billion as of 2023; while it is forecasted to hit $6 trillion in 2025 at 15.12% growth rate. This work presented some major technologies integrated with the IoT to achieve a certain goal and improve an existing system. IoT's capability to create smart applications is demonstrated and some major distinctions between IoT & the Internet were highlighted.

INDEX TERMS IoT, embedded technologies, smart applications, cloud, AI in IoT, ML in IoT, blockchain.

I. INTRODUCTION

IoT Internet of things can be considered as the third wave of the internet. The IoT aims to allow objects to get connected to the wider internet. IoT is deployed on a larger scale in industries, manufacturing plants, and smart homes, while the number of connected IoT devices has surpassed the number of people on Earth. IoT's nature and capability have changed many production processes and living experiences. With IoT's deployment in the environment, energy consumption is minimized, farming is modernized, other objects are made to perform certain tasks, etc [2].

When IoT devices are deployed in the field, they can configure themselves, identify neighboring objects, and start sharing information about the surroundings, information reading about light, motion, orientation, sound, temperature, pressure, humidity, etc. IoT devices are made to be intelligent by sensing and transmitting sensitive data that could influence a decision. To gain this intelligence, IoT objects must fully measure and report readings correctly, such as observation, monitoring, record human user motions, locations, context, environment, etc.

IoT's applicability enters many domains such as home automation, factory production, assembly line, etc. Users can monitor and supervise home activities such as turning on/off appliances, opening and closing doors, adjust the temperature. For example, when the occupant sleeps, a light goes off automatically, an item contacts its vendor if the stock is decreasing, a traffic light manages jams intelligently, senses environmental pollution, and controls a normal distribution of cars on the road in a smart city. In France, glass containers equipped with ultra-sonic sensors were used to send information when it was filled up. In the US, garbage cans attached with sensors send alerts to the municipality to request for emptying [3].

IoT paradigms are systems that embed the brain in an item to let it learn about behavior, think about processes, and understand its surroundings. Every day new IoT smart applications are being developed and used. Physical devices like the IoT have numerous limits in terms of computational

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

capacity, energy usage, and storage space, making it difficult to build a solid security solution on its own [4]. IoT inherits the attributes of Wireless Sensor Networks (WSN) and the internet such as limited battery constraint, multi-hop communication, scalability, and global accessibility [5].

This paper begins with an introduction and highlights the motivation for conducting this research, and then an overview of the evolution of IoT is given in section II. Section III presents some embedded technologies with the IoT. Smart IoT applications were explained in section IV and some major distinctions between IoT and the internet were highlighted in section V. Finally, this paper concludes with IoT future vision in section VI.

A. MOTIVATION

This study aims to assess the evolution, adoption, technologies, and growth of IoT and report all the findings in a single document to give readers the full awareness of IoT and its application. Because of its immense benefits, IoT is gradually being embraced by the day and it's gaining more attention by both researchers and industries to solve the problems associated with it. The figure below shows how research in IoT is gaining momentum, this has indicated that more awareness, more applicability, and more benefits would be derived from the IoT. If this trend continues, and if the integration of IoT into other technologies continues, one out of every ten publications will feature IoT.

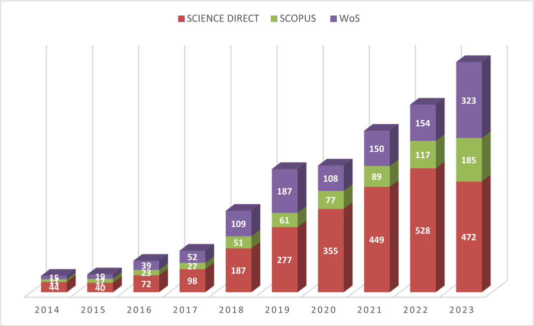

FIGURE 1. IoT research trend in the last decade.

B. RESEARCH QUESTIONS

The following research questions were listed to help researchers especially those that develop interest and want to delve into IoT research. In the method of thoroughly analyzing the developments in IoT growth over the last decade the following research questions need to be addressed:

1) **RQ1**: What does the literature on IoT in the last decade entail?
2) **RQ2**: What attributes of a collaborative network in the realm of IoT research are defined?
3) **RQ3**: What are the key theme trends responsible for IoT development?
4) **RQ4**: What are the main problems associated with IoT security and effective countermeasures for the IoT?
5) **RQ5**: What communication protocols are more compatible with implementing smart things for the IoT?
6) **RQ6**: What are the characteristics, performance, and effectiveness of the messaging protocols used in the IoT?
7) **RQ7**: What electronic devices and electronic platforms are used to implement the scenarios in the IoT environment?

Studying the above seven fundamental issues, researchers can identify theme trends and state-of-the-art issues in the IoT domain, entrepreneurs strategically compete in the IoT industry, and governments can exploit these insights to design more informed and professional action plans based on the development trends of IoT [6].

II. OVERVIEW OF IOT

The history of IoT started way back in 1982 when a vending machine of Coke mineral was connected to the internet and set to display the number of bottles in the machine with its temperature. In 1991, Mark Weiser introduced the concept of ubiquitous computing, a concept that aligns with that of IoT [5]. However, the first known and accepted technology used in the IoT was Radio Frequency Identification (RFID) in 1998. It was initially used in logistics and pharmaceutical retail. RFID was widely used before it later became the main component in IoT due to its affordability and availability. Bill Joy in 1999 demonstrated in a taxonomy a working clue of inter-connected devices which is termed as the IoT [7].

The most famous name who is the founder of IoT, Kevin Ashton, 1999, was an executive director of the Auto-ID center at the Massachusetts Institute of Technology (MIT), and was however, the first to coin the term IoT. The Auto-ID center as a collaboration between industries and private sectors has 7 research laboratories across 4 continents, holding 60 researchers and 15 professional leading research networks in IoT. This idea started in the same year the Auto-ID lab at MIT, 2001 presented its vision of IoT, in 2003 a closed-door meeting, and in 2005 is the year the International Telecommunication Union first mentioned the term IoT in its annual reports [8].

The first conference on IoT was organized and held in 2008, and from there many countries embraced it and drafted action plans on the IoT. Countries such as Belgium released their IoT – Action Plan in Brussels in 2009. China published a 12-year development plan in 2010. In 2013, the Kantara initiative was founded which solves open issues and questions such as identity, ownership, object identifier, authorization, authentication, data management, and privacy. Auto–ID released a state-of-the-art report on IoT in 2014 [9].

In the last decade, there has been skepticism about embracing IoT until when tech giants such as Google, Samsung, Gear Net Labs, and Apple IOS made IoT big business opportunities. Cisco revealed that IoT has a potential financial value worth $14 trillion [10]. They reported that 25 billion devices were connected before 2020 with 50 billion permanent connections and over 200 billion intermittent connections [11].

In [12], reports a projection of 29.4 billion in 2023. Intel projected that the market value for the IoT could hit 6.2 trillion dollars by 2025, and a big percentage of it is in manufacturing and healthcare [13]. Strategy Analytics predicted 38 billion connections by the end of 2025 and 50 billion by 2030 [13]. The production of sensors will expand worldwide specifically in areas of energy and mining to 33%, power and utilities to 32%, automotive to 31%, industrial use 25%, health 22% and retail 20% [14]. Another projection reported that the IoT sector is worth \$25 billion as of 2020, with a forecast of \$6 trillion in 2025 [1]. According to a market research estimate, the global IoT industry was worth \$1.90 billion in 2018 and is predicted to grow to \$11.03 billion by 2026 [5]. The European Union (EU), the United States (USA), China, and other governments have all developed IoT-related action plans [5]. Forbes in August 2014 reported that IoT had overtaken big data as a topic of discussion, with 15,000 references in 2013 and 45,000 in 2014. And IoT will be the main application area that will benefit from 5G & 6G [15].

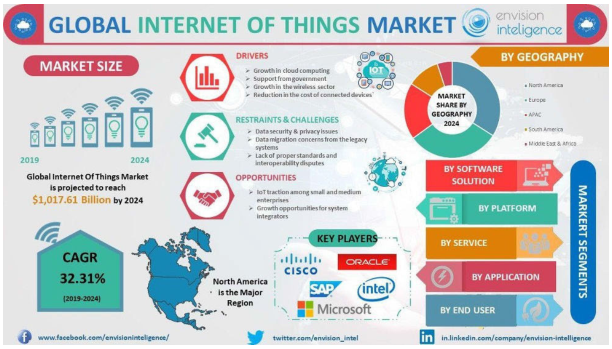
GLOBAL INTERNET OF THINGS MARKET
envision inteligence
MARKET SIZE
2019
2024
Global Internet Of Things Market is projected to reach $1,017.61 Billion by 2024
DRIVERS
Growth in cloud computing
Support from government
Growth in the wireless sector
Reduction in the cost of connected devices
IOT
RESTRAINTS & CHALLENGES
Data security & privacy issues
Data migration concerns from the legacy systems
Lack of proper standards and interoperability disputes
OPPORTUNITIES
IoT traction among small and medium enterprises
Growth opportunities for system integrators
BY GEOGRAPHY
MARKET SHARE BY GEOGRAPHY 2024
North America
Europe
APAC
South America
Middle East & Africa
CAGR
32.31%
(2019-2024)
North America is the Major Region
KEY PLAYERS
CISCO
ORACLE
SAP
intel
Microsoft
BY SOFTWARE SOLUTION
BY PLATFORM
BY SERVICE
BY APPLICATION
BY END USER
MARKERT SEGMENTS
www.facebook.com/envisioninteligence/
twitter.com/envision_intel
in.linkedin.com/company/envision-intelligence

FIGURE 2. IoT global market statistics.

In the last decade (IoT) has been gaining acceptance gradually and the initial wireless communications systems, RFID, IEEE 802.11.x, 3G, 4G, ZigBee, Bluetooth are appreciated [16]. The first literature on IoT was published in 2002 when Schulenberg pioneered the use of IoT in stores, claiming that a tiny wireless chip can store an eye. With over two decades of development, many government officials, businesses, and researchers believe that IoT is a critical technology for improving the quality of life and the environment [17].

The first technology used by the IoT is Radio Frequency Identification (RFID). RFID is used for many purposes including tracking, location authentication, etc [18]. Wireless sensor networks (WSNs) are the second technology embraced by IoT. Table 1 lists some early and current technologies embedded with the IoT by researchers to come up with a more promising IoT security solution and usage.

TABLE 1. The evolution of IoT embedded technologies.

TECHNOLOGY	YEAR	DESCRIPTION
IDS	1986 - date	Specialized in cyber security strategies. Specialized in cyber security strategies. Design to detect and respond to unauthorized activities
Wi-Fi	1997 - date	Automation and general-purpose use
RFID	1998 - date	Uses radio signal to provide wireless communication between devices
Quantum computing	1998 - date	A science of quantum mechanics extended to IoT
ZWave	1999 – date	Smart home automation
Zigbee	2003 - date	Low power, low data rate, short range wireless communication
WSN/ 6LoWPAN/IPV6	2005 – date	Uses AES-128 link layer security that is defined in IEEE 802.15.4
CPS	2006 - date	Integrates computational procedures on IoT technology
Blockchain	2008 - date	Combines with IoT to provide immutability, transparency, and decentralization
Cloud computing	2010 - date	Stores and analyze vast amount of data in the cloud generated by IoT devices
Bluetooth 4.0LE	2010 - date	Energy efficient communication
NFC	2011 - date	Contactless communication within close proximity
SDN	2011 - date	Communication in networks with flexibility, programmability and centralized management
Bluetooth	2016 - date	Wireless communication solution within range

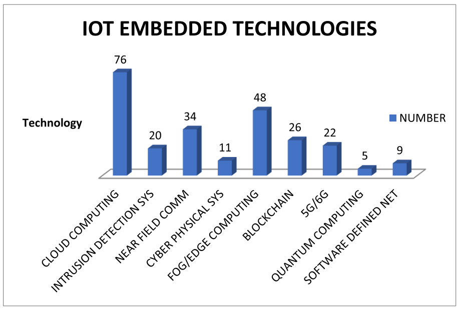

FIGURE 3. Research schemes integrating other technologies with IoT.

III. IOT EMBEDDED TECHNOLOGIES

IoT enhances convenience and automation, but security and user privacy remain the major challenges. Researchers are embedding other technologies to address these issues, resulting in promising solutions.

A. WIRELESS SENSOR NETWORKS

The Wireless Sensor Network (WSN) can be seen as the originator of IoT. It has played a key role in propagating the notion of IoT where every physical or virtual object can be identified, sensed, accessed, and interconnected via the internet. The WSN were sensor chips used for many purposes such as surveillance, battlefield, monitoring, awareness, medical purposes, etc. When such chips are thrown to the field or mounted on any surface, the security of the data it generates or reads is highly sensitive since any change or alteration of the data could cause severe damage [19]. The IoT works similarly to the WSN, but its network, devices, and technology are bigger and higher than that of the WSN.

In the WSN, there is a gateway node which is usually higher in capability than the sensor node. All the data being transferred is stored in the gateway node and requests for any data will go to the gateway node. In real-time demand of the data such as in the battlefield, a specific authentication algorithm is designed to verify the request to the data and give access to the requesting node [20], [21]. WSNs are deployed in a self-organized manner. Requests and responses to and from the sensor nodes are of two methods. The first is the access to perceptual data, the user sends a request to a node or gateway and then gets perceptual data from the node. The second is the real-time data where the user gets the data generated instantly and continuously. However, in real-time, devices need to be authenticated to join the network and communicate [22].

The IoT application scenario has numerous constraints and requirements. The implementation of test beds is critical for assessing the functionality of these systems, but it is much more important. It is extremely difficult to create and debug software for these networks. To design a susceptible protocol, like the use of Contiki's simulator environment (Cooja). Cooja may use real-world commercial radio transmitters (TI CC2420, CC2538) to simulate real hardware devices like TMote Sky, Zolertia Z1 Mote, WiSMote, and so on. Cooja may provide an identical network topology environment as a genuine test bed [23].

Consider the Survivable Path Routing (SPR) protocol, which uses many paths rather than the Contiki RPL protocol. RPL is a single-path routing system that selects just the best nodes for parent nodes. The package is passed to the parent node, which is the next hop node from the root. However, the authors in [24] alter the RPL functionality so that each node retains information about all possible routes to the root. If a DIO packet is received from an upstream node, the current receiving node saves the parent rank value in its routing table. When another package is received, the rank is likewise saved based on the individual node, as seen in [25].

Again, consider GE's US factory that deployed 10,000 sensors across 180,000 square feet [26]. The sensors are connected via a high-speed Ethernet and sense and transmit information. Wi-Fi nodes are deployed as gateway nodes. Employers send requests via the gateway nodes using a secure key agreement protocol to guarantee the integrity of the messages being exchanged [27].

B. CLOUD COMPUTING

Cloud computing is a concept that could allow the sharing of network resources, enable convenience, and ubiquitous, configuration among computing devices such as servers, networks, applications, and services, and above all bring those services from the cloud nearer to the application layer for utilization by the user [28].

Cloud computing is a storage system that operates on the Internet and employs centralized or distributed computing technology. Parallel and distributed computing can be coupled or integrated individually and deployed in a data center, either physically or conceptually [29]. It is important to all IoT systems. IoT devices are meaningful when they are connected to the cloud. When linked to other related sensors, data obtained from individual IoT sensors becomes valuable. Cloud services offer large-scale storage by linking huge virtual computers to accomplish certain operations. Cloud computing skills and resources can help IoT users overcome limits such as storage, processing, and connectivity [30].

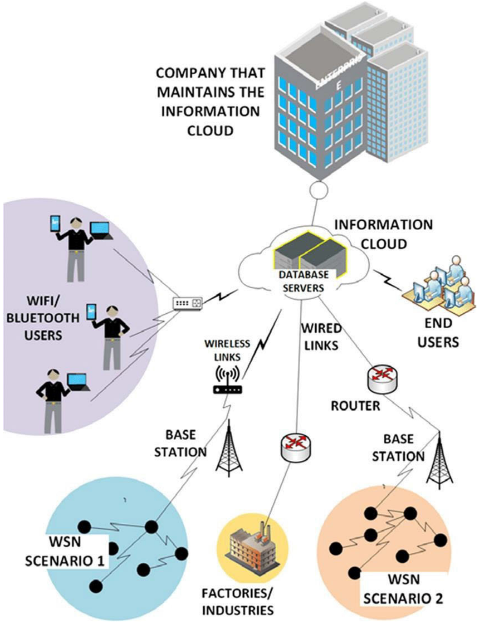

FIGURE 4. Wireless sensor nodes at the field.

In another definition, cloud computing can be defined as a concept that collects and processes big data generated by humans, IoT, and other objects at a low-cost service in the cloud, providing high performance, openness, accessibility, and versatility [31]. Cloud computing mainly provides storage capabilities with lots of servers and is considered a rapid on-demand network according to the National Institute of Standards and Technology (NIST). Big companies such as Google, Amazon, Facebook, and eBay have already embraced cloud computing and are benefiting from it. Cloud computing is a migration from classical computing to the cloud where resources are shared flexibly at a reduced cost [32].

The primary goal of data processing is to collect and analyze the obtained information, such as monitoring agricultural production on greenhouse farms is done in real-time, dynamically, and using a wide range of production data. The adoption of IoT technology allows for some storage and analysis of this industrial data, allowing the identification of key data patterns. Cloud computing technology is primarily used to process data and offers an efficient option for storing, calculating, and processing large-scale agricultural output data. Various data services, including cloud computing, fog/edge computing, and artificial intelligence (AI), are integrated with IoT technology and supported at the application level. This allows greenhouse farming applications to implement a variety of intelligent management operations, including automatic irrigation, autonomous environmental control systems, remote monitoring, fertilization, and ice prevention [33].

Three categories of cloud services are defined in the literature, these include private cloud, public cloud, and hybrid cloud. A study by [34] demonstrated a three-layer architecture for cloud computing. The end user layer, the fog layer, and the cloud layer. The end user layer is the nearest to the user, it has become an interface between the user and the fog devices (i.e. gateway nodes) where all requests of the user are serviced at the end user layer. Whereas the fog layer interfaces between the user layer and the cloud layer. All the fog devices and the data they hold reside in this layer. While the cloud layer handles all the requests and devices virtually.

The security of cloud computing is of course important for its being and continuous adoption by many. With robust architecture and operational security, the needed security can be achieved. However, the challenge will arise when each individual or firm requires storage allocation and computing capabilities according to its need [35]. The integration of cloud computing with IoT has brought so many benefits.

First, IoT devices being resource-constrained have gained additional storage and computing capability with effectiveness supported by cloud servers. Second, a more stable middle layer in the IoT (between IoT devices and applications) can be offered by the cloud by aggregating service implementation. Therefore, cloud computing is an ideal component of an IoT system [36], [37]. The convenience and cost-effectiveness of cloud computing have made individuals and enterprises subscribe to cloud-assisted IoT services where they can keep their data generated by IoT devices. However, users need to be aware of any risks associated with storing data in the cloud. What private information can be kept securely? What if cloud computing providers obey privacy requirements or not? What if the data in the cloud is breached by intruders?

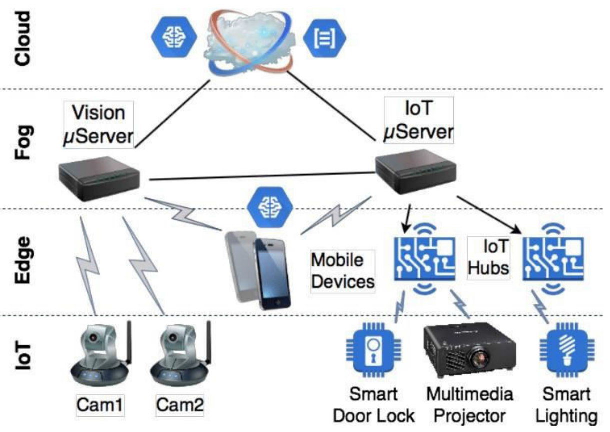

FIGURE 5. The concept of cloud computing.

1) CLOUD EDGE

A Cloud-Edge (CE) is a concept that divides the task of processing power, communication capabilities, and part of the intelligence between the edge devices, while heavy computations are carried out in the cloud. In the network setting, the devices are closer to the user while the cloud is in the sky, so all requests and processes handled by the devices are closer to the user, so the user gets services easily and accessibly. When IoT devices are tailored to the CE paradigm, they fit into the 3 architectural stacks, i.e. the upper layer which represents the cloud services for processing heavy data and providing IoT system management control functionalities to end users [38]. The lower layer contains heterogeneous (edge) IoT devices. Then the middle layer which contains nodes, and gateways acting as logical intermediaries between terminal nodes and cloud services in a logic sub-network [39].

The cloud layer is incredibly strong and has a wealth of resources at its disposal to handle demanding activities like extracting insight from massive amounts of data and executing extremely difficult assignments such as distributed intrusion detection. In addition, there are numerous potent instruments and sophisticated algorithms that can be used to create strong applications [40]. The sky and the items are related, they are typically situated far apart from direct lines of communication with one another. It's really expensive to use many hops to transport all data from items to the cloud arranging. However, cloud computing is not the best option to enable IoT. Applications with characteristics like intense real-time demands, great mobility or wide Geodistribution [41].

While heavy computation tasks are performed in cloud data centers, the Cloud-Edges (CE) paradigm distributes some intelligence, processing power, and communication capabilities among the so-called Edge devices, which are represented by highly heterogeneous appliances (from PCs to smartphones, from smart devices to automation controllers, etc.). These appliances are placed as close as possible to the component, device, application, or human that produces the data being processed. Such an architecture's features present serious security and privacy issues, primarily because there is no centralized control and user-sensitive data is exposed [42].

IoT systems built using the CE paradigm are generally divided into three architectural layers: (i) the cloud services that handle large amounts of data and give end users access to IoT system management and control functionalities are represented by the upper layer; (ii) a variety of heterogeneous (edge) IoT devices, which are referred to as terminal nodes are found in the lower layer; these devices generate the data needed to process and potentially interact with the physical environment; and (iii) a collection of (possibly heterogeneous) devices, known as gateway nodes, operate as logic intermediaries between the terminal nodes in a logic subnetwork and the cloud services [43].

Data tampering and spoofing attacks that target gateways and terminal nodes in an attempt to steal sensitive information are especially common with CE systems. In this case, authentication is essential to building confidence between participating nodes and preventing illegal devices from joining the network [44]. Many different types of IoT applications have needs that the current cloud architecture is unable to fully meet.

First, there is a significant access latency and data transmission cost between IoT devices and Cloud Data Centers (CDCs) since CDCs are situated several hops away from IoT devices. As a result, it presents a significant obstacle to the effective service delivery of IoT applications that depend on real-time and latency. Besides, the longer transmission time needed to convey commands to remote Cloud Servers (CSs) can have a negative impact on the service initiation time of IoT applications [45]. Additionally, for IoT devices with limited battery life, the longer transmission period and increased latency result in higher energy usage.

Second, a multitude of IoT devices might cause significant network loads and perhaps catastrophic congestion when they start data-driven interactions with applications that are installed on distant CSs. Thirdly, it may lower the computing efficiency of CDCs by adding to their computational burden. Fourth, due to privacy and security issues, some IoT applications cannot transmit sensitive raw data over the Internet [46]. The Edge and Fog computing paradigms have arisen in response to these limitations, bringing Cloud-like services closer to IoT devices.

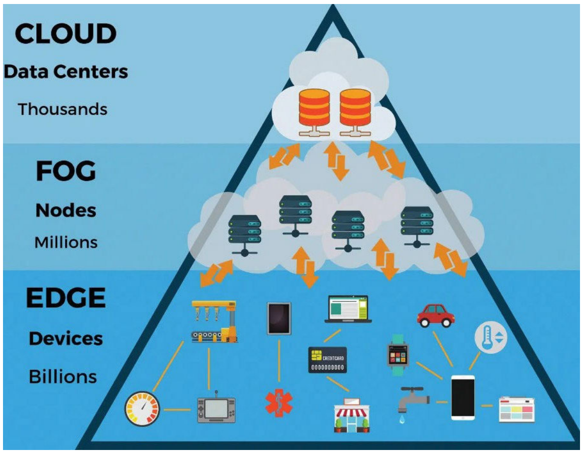

FIGURE 6. Cloud edge computing paradigm.

2) FOG COMPUTING

Recently, fog computing has gained popularity as an adjunct to cloud computing, offering some unique features including reduced latency, Geo-distribution, position awareness, enhanced data security, and real-time processing [47]. Furthermore, its goal is to bring network, storage, and computing capabilities closer to the end users. Fog computing is almost similar to cloud computing, it facilitates communication and collaboration among universal and prevalent things [48]. Fog can be deployed alongside cloud fog things.

An architecture known as fog or edge computing was created to offer computing services to consumers and applications that are situated between end users and central networks. Large volumes of data produced by various IoT device types can be handled on the edge of the network instead of being sent to a central cloud infrastructure in fog computing, as a result of bandwidth and energy consumption problems [49].

With its many benefits, fog computing should be properly integrated into IoT and taken into consideration for future IoT infrastructure. It can handle large volumes of data (better than the cloud due to energy consumption), process data quickly, and produce high-quality results. The features and concept of IoT should be studied to develop and implement fog IoT infrastructure. For example, IoT can link ubiquitous devices from many networks to offer integrated, effective, and secure services at anytime, anywhere [50].

The two characteristics of the IoT are as follows: (1) The IoT is an extension of the net or internet, and interconnection is a crucial architectural issue. These networks must be compatible to transport information. (2) Things connected in the IoT can encompass more than just objects; they can also include information itself, behaviors, etc., so a more comprehensive mechanism to manage this is required. The study of IoT challenges, enabling technologies, and architectures helps novices comprehend the current status of IoT development [51].

For example, when fog computing is implemented, a request from a user may go to a specific node but if the node is busy servicing another request, it may forward the request to a free neighboring node. If for instance, all nodes are busy due to high demand the request will then go directly to the cloud where the cloud will process the request and send back the response or service requested traditionally. Traditional computing cannot handle the big data generated on the internet; thus, cloud computing continues to be an option [52]. Cloud computing has proved to be a promising technology for solving big data problems.

A vast number of geographically dispersed and heterogeneous Fog Servers (FSs) are situated in an intermediary layer between CSs and IoT devices according to the Fog computing paradigm [44]. For IoT devices running a variety of applications, distributed file systems (FSs) such as Raspberry, Nvidia Jetson platform, small-cell base stations, nano servers, and core routers, provide heterogeneous computing and storage capabilities.

Fog is a high-virtualization service that connects end devices to cloud computing data centers, which are often positioned at the network's edge [53]. This means that cloud computing comprises infrastructure-level services that may be scaled to satisfy the storage and processing requirements of IoT. However, certain applications, such as sensor monitoring, control, and analytical response, necessitate minimal latency. As a result, delays induced by data transmission to cloud servers and subsequent return to applications might have a major impact on their performance. Fog and edge computing frameworks are intended to overcome these restrictions.

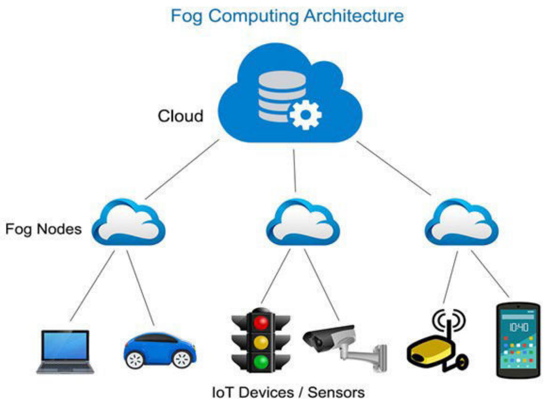

FIGURE 7. Fog computing architecture.

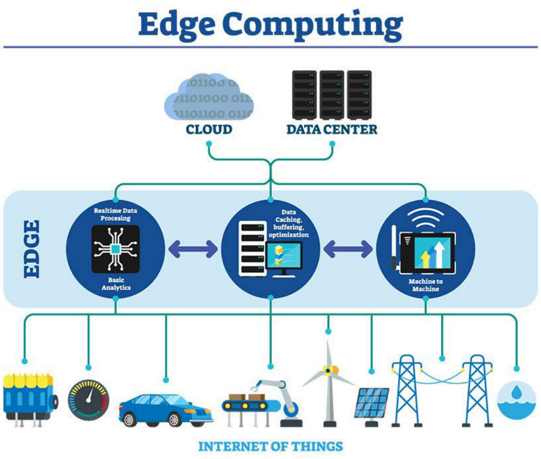

FIGURE 8. Edge computing architecture.

3) EDGE COMPUTING

The idea of the edge layer, also known as the fog layer or the gateway layer, is to bridge the gap between the cloud layer, which has abundant resources, and the objects layer, which has limited resources. The boundary layer has developed into an essential layer in the IoT architecture. Typically, edge gadgets are either close to the items or a short distance away from them. In general, edge devices have greater resources than items comprising storage capacity, processing speed, and power supply. With their numerous interfaces for communication, they can aid in hiding the things' diversity and offer additional services to things like transferring heavy tasks [40].

Edge computing involves directing computer power to the device's sensors and delivering processing capacity using low-power microcontrollers integrated in the devices. Despite their limited processing capabilities, they can nevertheless be used for image processing applications [54]. Cloud services are being extended to the network's edge [55] to reduce latency and congestion. Edge computing devices include wireless communication-capable sensors with microcontrollers. An IoT system based on fog computing can make decisions rapidly at the edge, reduce the volume of data transported between the fog and the cloud, and reduce the amount of data the cloud processes [56].

Edge computing is the placement of networked computing units near end devices on the internet. Decentralizing computing resources to the edge addresses two significant challenges in the cloud architecture. Distributing edge servers across different locations prevents bottlenecks at certain hot spots and allows for better application response times due to their closeness to data sources [57].

Edge computing deployments often use networked compute nodes scattered throughout an environment, as largescale edge data centers may not be possible in certain contexts, such as urban areas. Edge IT operations have significant technological hurdles due to the physical dispersion of servers, which are only a few hops from end devices. Edge servers are put outdoors in small buildings. Once that is done, small facilities have hardware challenges such as rapid aging, power outages, and physical damage, as well as security threats including network attacks and tampering, etc. Maintenance policies are essential for maximizing the benefits of edge infrastructure's closeness to data sources by addressing performance and security concerns [58].

C. INTRUSION DETECTION SYSTEM

Intrusion Detection System (IDS) is a data protection concept similar to cryptography. But IDS is enriched with capabilities to detect and prevent attacks in a computing system [59]. The attacks to be detected can be passive, that is when attackers impersonate a genuine node and tap communication or remain in the network. Or active attacks, that is when malicious acts are carried out on the data.

Several techniques for improving the security of IoT networks have been investigated, with deep learning (DL) intrusion detection being the most commonly employed. Deep learning systems can learn patterns from existing data sets and forecast invisible data. This feature allows an IDS to detect harmful activities in network traffic based on mode learning history from the training stage [60]. Furthermore, the DL approach can give generalization to defend IDS against unknown/unknown anomalies. However, the dataset has a significant impact on the DL algorithm's performance. As a result, good DL models necessitate careful selection and specialized data sets for training and testing.

To improve the security of IoT networks, DL algorithms are employed to train IoT-specific data sets. It suggested and trained a long short-term memory (LSTM) model using the planned BoT-IoT data set [61]. The input dimension is set to 10, which corresponds to the top ten features in the BoT-IoT data collection. Other DL methods are proposed that use fewer features from the same set [62]. Continuous neural

networks (CNN), LSTM, and gate repeat units (GRU) are suggested and trained on the BoT-IoT data set. Their input dimensions are limited to four functions, which are smaller than the LSTM suggested in [61].

For instance, a model by [63] proposed Deep Learning based IDS is made up of three components: the data mirror module, the anomaly detection module, and the counter measurement deployment module. Our IDS is assumed to be built into the SDN environment controller. This approach is similar to the one proposed in [64], however, our Data Mirroring module just pulls data from Open Flow messages and transmits it to the error detection module. The last module is a deep learning binary classification model that makes predictions based on the data from the previous module. If the prediction is incorrect, the Counter Measurement deployment module will add a new flow input to avoid anomalous data. To reduce interference in the SDN network, Ryu apps use data mirroring and countermeasure deployment modules. Meanwhile, anomaly detection.

IDS is categorized into two distinct technologies. The first is the Network Intrusion Detection System (NIDS) where the system of the IDS have capabilities to intercept and analyze the packet for abnormalities. Because all the communication is in the cloud, a node can notice the activity of another node, so this concept can allow the traffic to be listened to and examined. The second is the Host Intrusion Detection (HIDS) where an IDS is installed and used to analyze the data in the node. The information is obtained from the activity log files [65].

The IDS architecture is in three types. The Standalone IDS is the architecture that operates independently and has detecting capabilities against attacks. No information is shared in this architecture but rather each node executes IDS. Another type of architecture is the Distributed and Cooperative IDS which is an architecture where the nodes have agents and can decide by themselves, and the nodes can cooperate to have a global detection. This architecture is considered more fit for a flat network configuration than a cluster-based multilayer [22], [66]. The third is the Hierarchical IDS which is sub-divided into clusters while having the cluster head as the leader of it cluster. The cluster head is responsible for routing all messages shared, exchanged, or transferred [67].

D. FUZZY LOGIC

Fuzzy logic uses the notion of trust as an ambiguous component. Trust contains uncertainties, vague and hazy relationships and therefore cannot be applied with probability. Trust situations cannot be generalized. But in networks, a more representative component is needed to visualize exactly how an entity behaves or what it entails [68]. Thus, fuzzy logic is a multi-valued logic derived from fuzzy set theory to solve problems, it becomes a good choice for actual representation. The rules of fuzzy are used in control techniques to make decisions and recognize patterns. Fuzzy logic contains a series of IF-THEN rules to solve control problems [69].

The model addresses unstable behaviors such as contradictory behavior and ON/OFF behavior. In contrary behaviors, malicious nodes j and neighboring nodes k and l usually send packets, malicious nodes h drop packets, and malicious nodes j behave similarly maliciously ON & OFF. Fuzzy systems and inferences are the main categories of machine learning methods that prove the ability to handle ambiguities and unpredictable conditions and accurately simulate human brain decision-making behaviors [70]. This has shown the robustness of fuzzy against changes in malicious behavior and signatures during the test time.

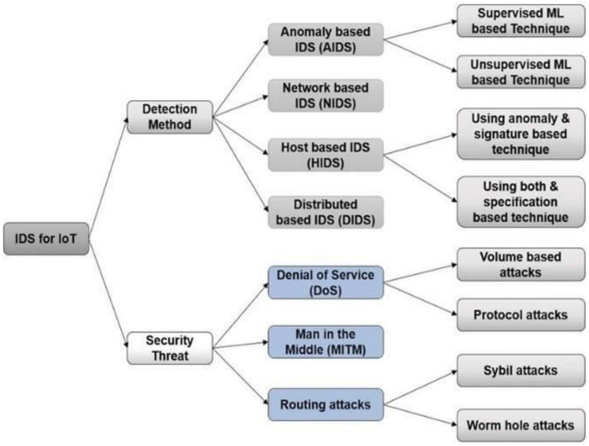

FIGURE 9. Description of IDS topology.

A model by [71] is proposed to improve safety at two levels: intra and inter-cluster. In the intra-cluster phase, the cluster head employs fuzzy logic to assess the trust level of the nodes, if the node is trusted, data is received and transmitted. Reference [72] proposed a fuzzy logic-based cross-layer optimization model (FL-CLOM) for WSN, they combined fuzzy control and congestion control to dynamically regulate queue sizes in dense nodes while mitigating the effects of external uncertainty. Another model uses hybrid characteristics, demographic information, and fuzzy logic principles to enhance recommendation accuracy, capturing uncertainty and inconsistency in user preferences for more precise results [73].

E. NEAR FIELD COMMUNICATION

Near Field Communication (NFC) is a new technology that was built on RFID standard, it engages in radio communication and provides short-range communication when touched or brought to proximity just like the RFID, both have Unique Identification (UID). But also, is similar to WSN for being a bidirectional communication. NFC can be used in smart networks which encompass decipherable NFC tags that if data is transferred to the smartphone, it can be read from the tag [74]. One of the core technologies of IoT is the NFC which is being more widely used in mobile devices.

NFC is a high-frequency, non-contact, short-range automated identification wireless technology that operates at a distance of less than 10 cm and uses the 13.56MHz frequency band. It is the evolution and innovation of RFID technology. It is frequently utilized in a variety of sectors, including product security and electronic tickets [75]. It reads merchandise information and allows for mobile payments. Certain NFC authentication systems enhance functionality and performance without taking security and privacy into account, while other systems are very complex.

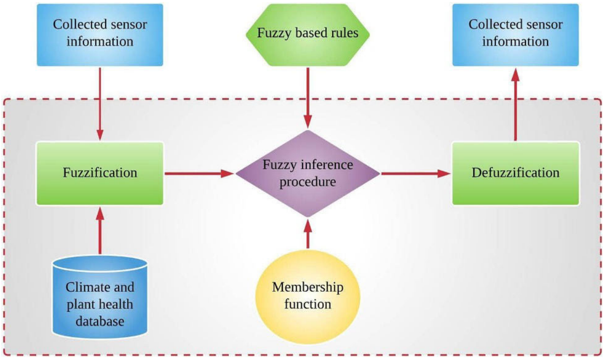
Collected sensor information
Fuzzy based rules
Collected sensor information
Fuzzification
Fuzzy inference procedure
Defuzzification
Climate and plant health database
Membership function

FIGURE 10. Fuzzy logic technique.

Additionally, there is a security risk involving authentication between the tag's validity and the reader. NFC communication is vulnerable to numerous malicious attacks, including packet loss attacks, man-in-the-middle attacks, and clone attacks because it is fully exposed to the wireless environment. The NFC system has several limitations, including processing speed, storage capacity, and power supply. Developing a reliable and effective NFC authentication mechanism is a difficult undertaking. There isn't a general applicability system for NFC authentication, despite all the research and proposed techniques [75].

The NFC comprises three components, the hardware, the software, and the middleware. Hardware is sensors, actuators, fog devices, smartphones, smart objects, PDAs etc. Whereas the software is the applications, algorithms, and protocols that rely on the hardware to work effectively and provide the services a user needs. An abstraction layer that sits between the hardware and the programs that control it is known as middleware. Apart from the programmer who finds and fixes a specific problem, it conceals the specifics of many technologies. Semantic middleware and service-oriented architecture (SOA) are the most often used middleware layers. While SOA and REST (Representational State Transfer) based systems are more common in enterprise environments due to their advantage of addressing both semantic and technical interoperable issues, the semantic is dependent on Extensible Markup Language (XML) meta exchange for interoperability [76].

According to [77] NFC is utilized in mobile IoT for identity identification and electronic payments. Few studies address identity identification in NFC, but a large number concentrate on electronic payments. Like readers and point-of-sale (POS) systems, NFC devices are used to retrieve data from tags, just like cards. Tags, readers, and even stored data retrieved from NFC devices are authenticated by the cloud server [78]. A cloud server and several NFC devices, including NFC tags, phones, watches, special NFC readers, and numerous more NFC smart devices, are part of the system for the NFC mobile IoT network. It is important to note that NFC smartphones are extremely unique in this regard. The NFC mobile phone can function in three different ways: as a tag on a card, as a reader, or can facilitate peer-to-peer file sharing between phones.

One popular test-bed is the re-configurable intelligent surface (RIS) that supports near-field communications in the recent 6G wireless networks presented by [79]. Power scaling laws and EDOFs are analyzed, and beam training and beamforming design are discussed. A two-stage hierarchical approach is proposed for cost reduction. Reference [80] highlighted how various novel antennas have arisen to meet the need for its integration in NFC. Antennas have gone beyond their basic role as signal conduits, becoming dynamic, flexible, and intelligent components. Modern antennae actively shape, control, and manage data flows to satisfy the complex demands of modern wireless communications.

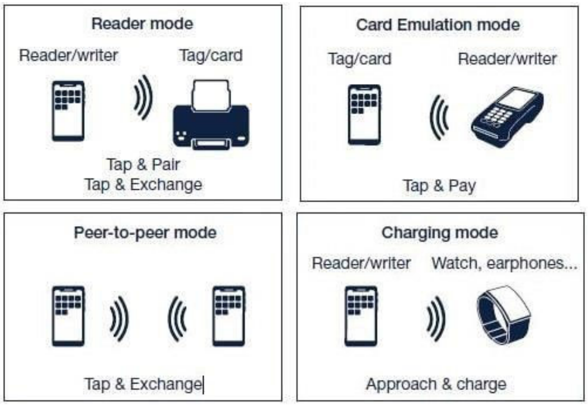

FIGURE 11. Application of NFC.

F. CYBER PHYSICAL SYSTEMS

Cyber-physical systems (CPSs) are built on the seamless integration of computation algorithms and physical components [81]. These CPSs operate often in larger and more complex environments, and the concept of system (SoS) plays an important role [82]. The CPS is an effective system that integrates computers and physical components by integrating modern computing and communications technologies to change the methods of interaction between the human, cybernetic, and physical worlds.

In other words, CPS are contemporary computer and communications technologies that integrate cyber and physical components. In CPS, cyber means modern communication while physical refers to actual physical things in the network, system refers to integration, diversity, and complexity, and cyber refers to contemporary communication technology with sensing and monitoring computing ability with the physical components. The primary goal of the IoT is to link different networks together so that heterogeneous networks can be used for data collecting, resource sharing, analysis, and administration [83].

As a result, to establish interconnection, the IoT is a horizontal design that needs to combine all CPS applications' communication layers. The primary distinction between the IoT and the CPS is that the CPS is regarded as a system, but the IoT is regarded as the ''Internet''. Additionally, the following are the particular criteria for CPS and IoT: The

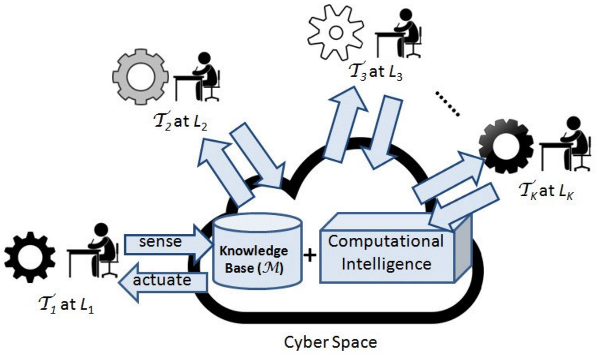

FIGURE 12. Working Concept of CPS.

primary objective of CPS is efficient, dependable, accurate, real-time control of the IoT, key services include high quality of service (QoS) network, resource and management sharing, data and management, interconnections between various networks, large data collection and storage, data extraction, data aggregation, and information extraction [84].

Real-time, dependable, and secure are the common needs for both CPS and IoT. In smart cities where many CPS applications run concurrently are among the most exemplary applications that combine CPS and IoT.

Part of the fourth industrial revolution (Industry 4.0), cyber-physical systems (CPSs) are integrated technologies like big data, healthcare IoT, industrial IoT (IIoT), smart cities IoT, and AI that are used for innovation in smart industries to promote data transmission between networks. Several researchers have created CPS based on different AI techniques to address the security vulnerabilities endangering the IoT. To enhance edge computing, presented a distributed service framework that facilitates the growth of privacy protection and trustworthiness for multi-directional data aggregation [85].

Part of the fourth industrial revolution (Industry 4.0), CPS are integrated technologies like big data, healthcare IoT, industrial IoT (IIoT), smart cities IoT, AI, and big data that are used for innovation in smart industries to promote data transmission between networks. Several researchers have created IDSs based on different AI techniques to address the security vulnerabilities endangering the Internet of Things. To enhance edge computing, presented a distributed service framework that facilitates the growth of privacy protection and trustworthiness for multi-directional data aggregation [85].

Existing IoT test beds and platforms, as well as comparisons with UMBRELLA, include wireless experimentation, AI/ML test beds, robotic test beds, wireless sensor networks, and smart cities. An IoT application, such as a city-wide air quality monitoring use-case, uses sensors installed on street furniture and building facades to collect data. The collected data is transmitted wirelessly, post-processed, and stored on local servers or a cloud system. The data can be visualized and used to make recommendations to optimize system behavior, either holistically or from a research perspective [86].

G. ARTIFICIAL INTELLIGENCE IN IoT

Today advances in radio technology, network protocols, artificial intelligence (AI) and machine learning (ML) make it easier to design efficient IoT systems with appropriate device selection, network architecture, and data processing capabilities. Existing IoT test beds can be classified into three main categories depending on their characteristics, support for use cases, and main objectives: wireless experiments, robotics research, and AI-related activities. Here are examples of three AI in the IoT testbed applications.

1. AI Application for Monitoring Streetlight: This use case entails monitoring the operation of lighting to promptly detect abnormalities or problems. Any unforeseen operation will alert the Council's streetlight maintenance crew. Except for those with a unique schedule, most lights are configured to turn out 15 minutes after sunrise and 15 minutes before nightfall. The municipal street lighting crew performs manual checks for appropriate functionality every four weeks. Normally, the team uses public reports to discover light fixture issues. If several fixtures exhibit unexpected behaviors, such as being triggered or being triggered outside of the specified time, the team addresses these issues by performing a batch correction throughout the road to reduce expenses. Our implementation automates the process and offers a more cost-effective method of managing fixed street assets [87].
2. AI System for Large-scale Federated Learning: Federated Learning (FL) is a decentralized machine learning framework that parallelizes training across interconnected devices. In edge, nodes collect raw data. However, network quality and energy constraints can hinder model parameter sharing. This use case aims to develop an FL system that minimizes model parameter transmission, reduces bandwidth requirements, improves service quality, and lowers energy consumption [88].
3. AI Model for Intrusion Detection: The AI's flexibility to model systems, which allows end-users to deploy containerized experiments, raises security concerns about the system's operation. Attacks such as privilege escalation can compromise both the host and the IoT infrastructure. A semi-supervised FL solution to detect edge issues and guarantee the platform runs smoothly can be created. This use case can train and deploy a real-time anomaly detection system across the IoT infrastructure [89].

H. MACHINE LEARNING FOR IoT

Implementing ML capabilities can be used to improve the reliability and performance of IoT systems in certain circumstances, such as predictive maintenance of IIoT devices, energy optimization of intelligent buildings, traffic prediction in intelligent transportation, and intrusion detection. By using machine learning algorithms to evaluate sensor data, predict events, optimize operations, and discover

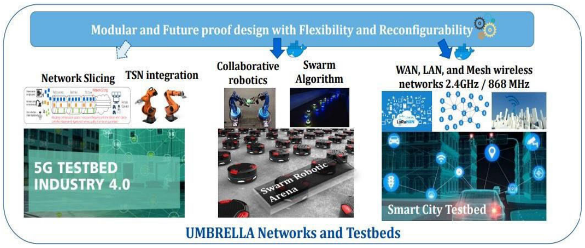
Modular and Future proof design with Flexibility and Reconfigurability
Network Slicing
TSN integration
Collaborative robotics
Swarm Algorithm
WAN, LAN, and Mesh wireless networks 2.4GHz / 868 MHz
5G TESTBED INDUSTRY 4.0
Swarm Robotic Arena
Smart City Testbed
UMBRELLA Networks and Testbeds

FIGURE 13. **AI Applications Test-bed in IoT.**

anomalies, IoT systems may become more efficient, resilient, and dependable [90].

The integration of machine learning algorithms into IoT applications is becoming increasingly significant. The testing platform creates useful data that may be utilized to apply these algorithms in new contexts. Recent research, such as that conducted by the researchers in [91], has investigated the application of neural networks in radio frequency fingerprinting data on the POWDER test bed. Similarly, supervised learning algorithms [92] are trained on limited Wi-Fi performance indicators derived from City-Lab data observations. In addition, another study [93] examined and identified interference using data from 11 city-Lab entries. Researchers have created a neural network model that can accurately forecast interference using received signal strength indicator (RSSI) readings. Finally, in [94], the authors developed a deep-learning method to detect junctions using data from the COSMOS test-bed. There are three main classes of ML algorithms:

1) SUPERVISED LEARNING

In the realm of IoT integration, supervised learning algorithms are used for a variety of tasks, including spectrum recognition, channel estimation, adaptive filtering, and positioning. These algorithms rely on labeled datasets for training. There are two sorts of procedures in this field: regression and classification. Polynomial and logistic regression are two common regression algorithms used in prediction tasks. These algorithms, often known as ''Instance-Based'' algorithms, predict outputs for fresh observations using learned models. Furthermore, classification algorithms such as decision trees, random forests, Naive Bayes, and Support Vector Machines (SVMs) are often utilized to categorize tasks. And in IoT security, these algorithms have seen widespread [95]. Consider integrating machine learning techniques into IoT systems. Nonlinear constraints, for example, are included in solution models using support vector machines (SVMs). SVMs are useful, however, they have limits with huge data sets. Random forest approaches, on the other hand, are simple and scalable, making them perfect for managing large datasets. This leads to higher accuracy and faster predictions, but training takes longer than SVM and Naive Bayes (NB). Logistic regression and similar algorithms need significant computer resources, particularly for processing feature-rich datasets and memory use [96]. In IoT networks, supervised learning algorithms are used on the cloud and communication layers to detect attackers and prevent distributed denial of service (DDoS) assaults.

2) UNSUPERVISED LEARNING

Unsupervised learning algorithms play an important role in IoT integration because they use heuristics to discover patterns in input data without labeling. These algorithms excel in detecting abnormalities, identifying trends, and classifying data. Unsupervised learning uses classification algorithms to classify data. One of the primary benefits of IoT without supervision solutions is their ability to operate without the desired outcome being known. Common clustering techniques, such as K-means and hierarchical clustering, use unsupervised machine learning algorithms to organize data effectively [97].

The most commonly used clustering approach in IoT integration is K-means clustering. The method uses simple algorithms to create clusters based on data point observations, such as recognizing typical and anomalous traffic. Unsupervised learning techniques, such as K-means, are frequently employed in the IoT system's communication layer to detect anomalies and potential attacks [98].

3) REINFORCEMENT LEARNING

Reinforcement learning (RL) techniques are used in IoT integration to discover the ideal combinations of actions that maximize revenues. Through experimentation with various actions in a specific situation, RL effectively addresses numerous IoT security issues. Unlike other approaches, RL interacts with the environment and learns via experience rather than depending on prior knowledge. Despite their efficiency, RL approaches may require time to establish the optimal line of action. In the dynamic network environment of the IoT, the primary concerns are the progressive convergence of RL and the design of ideal transition functions or policies [99].

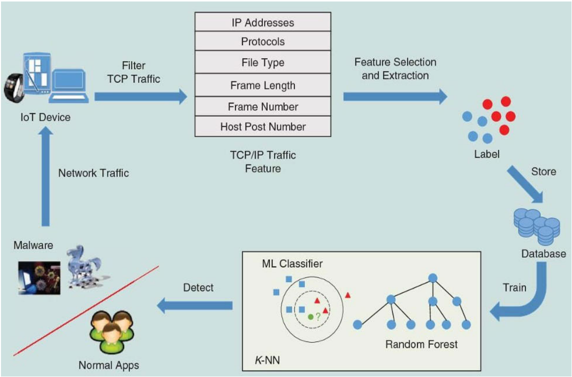

FIGURE 14. **An illustration of ML-based malware detection using IoT.**

I. BLOCKCHAIN

The term ''blockchain'' refers to the process of turning a data chain into a block that is connected to the one before it [100]. The blocks that follow each other reinforce each block even more. This is because the blocks that follow the preceding one will include information about the last block. Due to the use of blockchain technology in cryptocurrencies like Ethereum and Bitcoin, it has recently attracted a lot of interest and recognition. In essence, blockchain is a data recording technology that makes data much harder to alter or hack [101]. A distributed networking system of machines is used by blockchain to duplicate and build a chain of data. Each of these data points becomes a block in what may be thought of as a ledger.

Furthermore, every block spreads throughout the network, enabling any machine to access the complete chain and all its contents and enabling several verifications. This guarantees the integrity of the block and the authenticity of the data. Blockchain's distributed architecture makes it possible for it to function as a transparent, safe, decentralized transaction system. Blockchain technology has grown in promise as a foundation for the future development of the internet and data processing since it is not dependent on a centralized network. The world will eventually depend on data processing and storage as its network grows smartly [102].

This highlights the requirement for a quicker and more effective way to provide a reliable system and secure data. These intelligent and networked systems can take advantage of blockchain technology, thanks to its distributed and unchangeable structure which can offer data security. Blockchain integration with IoT is a suggested solution for IoT's problem. Blockchain's decentralized and distributed architecture makes it extremely impervious to manipulation. It is also appropriate for a minimal processing device commonly found in the IoT, as it requires less computing power from each node or device [103].

This highlights the requirement for a quicker and more effective way to provide a reliable system and secure data. These intelligent and networked systems can take advantage of blockchain technology, which thanks to its distributed and unchangeable structure, can offer data security. Blockchain integration with IoT is one suggested remedy for this. Blockchain's decentralized and distributed architecture makes it extremely impervious to manipulation. It is also appropriate for a minimal processing device commonly found in the IoT, as it requires less computing power from each node or device [103].

Smart homes [104], smart cities [105], smart agriculture [106], smart power grids [107], smart transportation and automobiles [75], smart healthcare [32], and smart manufacturing are just a few of the IoT applications [108] domains that have effectively leveraged blockchains, as figures 19 to 25 illustrate. Future applications, such as a cloud constellation of nanosatellites creating an orbital data center where businesses may upload their data and forego the terrestrial network, are also aided by this technology. Nevertheless, with the advantages of blockchain technology, the advancement of IoT devices has just lately allowed for its usage [109].

For instance, the use of blockchain in satellites would improve the value chain's efficiency, trust, and transparency for logistical reasons. Using blockchain over satellite reduces the risk of a data breach or compromise by doing away with the need for terrestrial infrastructure for data transport, storage, or calculation. Blockchain can facilitate record keeping, enhance transparency, stop fraud, and protect data privacy [110].

Industry researchers predict that blockchain technology will be a game-changer in the management, control, and security of IoT devices. A peer-to-peer P2P network of miners timestamped and validated transactions (chained blocks of data) register assets and transactions in the blockchain, a decentralized, distributed, shared, and un-changeable database ledger. Strong cryptography is provided by ECC and SHA-256. The blockchain offers a cross-border global distributed trust and contains a complete history of all transactions [111].

1) BLOCKCHAIN AND IoT TESTBEDS

A model proposed by [112] is a combination of symmetric and asymmetric encryption that is designed to be as light as possible and able to provide security with minimum energy consumption and computation. Fogify [113] is a simulation framework for designing and deploying IoT services in fog computing infrastructures. The framework makes it easier to model, experiment with, and evaluate IoT services by leveraging use case and failure simulation factors. Similarly, MockFog [114] offers a framework for emulating cloud edge resources, allowing them to be deployed simultaneously.

Kaala [115] is a scalable end-to-end IoT simulator that integrates virtual cloud providers. The simulator can replicate a large number of devices and accompanying events, allowing you to compare IoT to cloud systems. However, it does not consider any advanced aspects in the evaluation, instead focusing solely on CPU and latency, and it does not use a blockchain evaluation mechanism. The IoT NetSim architecture [116] includes simulation-based IoT frameworks. Unlike Kaala, each device requires a new virtual machine, which might cause resource exhaustion issues, particularly with light deployment schemes.

Only the simulation framework FobSim [113] supports blockchain technology from the literature. However, their blockchain implementation is quite limited and does not take into account the most recent technology contained in modern blockchains, such as digital signature systems and block Merkle trees. This considerably reduces the feasibility of building a system for evaluating such integration. Furthermore, the solution is a full simulation-based platform that includes an emulation element.

In [117], sensors are used as transducers. A transducer is a device that transforms one form of energy into another. Physical events are turned into electrical impulses that can be read by sensors or transducers. There are various methods for measuring the same thing. Actuators are the second sort of transducer. The actuators operate in the opposite direction as the sensors. It engages in physical action through electrical impulses. Temperature sensors, for example, are capable of detecting heat. Sensors are classified into several sorts, including temperature sensors, distance sensors, optical sensors, light sensors, and environmental sensors.

Reference [118] identified the inability of many works to provide an evaluation of this integration in practical terms of full complexity and idiosyncrasies of real-world system interactions. Therefore, a hybrid simulation/emulation test platform for the deployment and evaluation of blockchain and DLT technologies in the IIoT environment. Implementation and deployment of the solution on a bespoke IoT test-bed comes with three distinct development areas: software, hardware, and orchestration.

2) COMPONENTS OF BLOCKCHAIN AND IoT

The applications of blockchain solutions for IoT are as such:

i) Address: IPV6 provides a 128-bit address space for IoT, whereas blockchain has a 160-bit address space.

ii) A blockchain address is a 20-byte hash of the public key produced by the Elliptic Curve Digital Signature Algorithm (ECDSA), or a 160-bit hash. Blockchain may therefore generate and allocate addresses offline for about 1.46 × 1048 IoT devices using this 160-bit address. Thus, the likelihood of an address collision is roughly 1048, which is secure enough to offer a global unique identifier (GUI).

ii) c. Blockchain technology can also resolve open research concerns in the areas of supply chain management, data privacy, and safe and reliable governance of IoT device ownership [119].

On the other hand, scalability, efficiency, arbitration/regulations, and key collision present problems for blockchain technology itself. Even if they include intri-

cate calculations, the traditional procedures need to be redesigned to be lightweight and energy-efficient, and energycollecting techniques need to be improved [120]. Furthermore, blockchain has gained attention for its potential to address several authentication-related problems with IoT authentication protocols. The methods have made use of various sophisticated encryption algorithms that meet mutual authentication and access control requirements. Additionally, these methods can merely prevent the Sybil attack from being exploited. In addition, blockchain-based approaches applied Lagrange interpolation mechanisms and pre-image sample entryway techniques for mitigating the vulnerabilities of chosen plain text message attack [121].

3) BLOCKCHAIN FEATURES INTEGRATED WITH IoT

As mentioned before, the name "blockchain" comes from the way blocks in blockchain technology are arranged into chains. But blockchain technology is far more intricate than a simple arrangement of links and blocks. To genuinely assemble the block and ensure that it won't be tampered with or compromised, numerous additional parts are needed. Asymmetric-key cryptography, ledgers, and cryptographic hash functions are a few of these crucial technologies [122].

a.) Blockchain technology's cryptographic hash algorithms are its primary constituent. A technique called hashing can be used to determine a unique output for any size input. If the recipient does not have the keys, the material is encrypted into a safe format that cannot be read. This demonstrates that the data has not changed [123]. An output with a length of 256 bits is produced by the SHA256 algorithm from inputs with a length of less than 264 bits. There are sixteen 32-bit words that make up its 512-bit block size. Through a message scheduler, this 512-byte block is fed into a message compression mechanism in 32-bit words. The 512-bit message block is then expanded into sixty-four 32-bit by the message scheduler.

b.) Asymmetric-key cryptography, sometimes referred to as public-key cryptography, is a second crucial element of blockchain [124]. Two keys are used in asymmetric key cryptography: a public key and a private key. This component's primary function is to be employed in cryptocurrency-related transactions. The public key is used to safeguard blockchain activities and provide open access to data stored in the block, including the address of a single cryptocurrency across the network. An individual uses the far more limited private key to digitally sign transactions.

c.) The ledger is the third key component of blockchain. All that would be a ledger would be a list of transactions. Traditionally, one entity operated and consolidated these ledgers. In the case of blockchain, however, the distributed ledger is far more prevalent [125]. Digital ledgers known as distributed ledgers are dispersed among nodes in a network so that each node has an identical copy of the ledger. All nodes or holders on the network will receive simultaneous updates from this ledger. Distributed ledgers employ cryptography signatures for information authentication as well. Distributed ledgers apply to blockchain technology.

To raise the total security level of IoT, the right technologies and procedures must be used. The blockchain's security features have come to light because of its quick development, and these could now be used as viable IoT security strategies. Building distributed IoT systems using the blockchain's features of decentralization, consensus mechanisms, data encryption, and smart contracts is a good way to prevent possible threats and save transaction costs [126]. Blockchain, being a decentralized and transparent database platform, can improve IoT security performance to a greater extent.

4) BENEFITS OF BLOCKCHAIN IN IoT

IoT and blockchain are two cutting-edge technologies that are getting a lot of attention. However, security is the most crucial component that influences how well blockchain integrates with IoT and how well IoT security performs. Some of the major advantages of the blockchain integrated in IoT are as follows:

I) Blockchain uses consensus techniques to guarantee IoT security. The absence of trust mechanisms amongst IoT devices is the cause of the security problems. Blockchain offers a method that eliminates the need for nodes to trust one another.

II) Blockchain addresses IoT reliability. Blockchain's distributed network architecture ensures that the system's data remains safe and dependable even in the event of a node or nodes being attacked. The consensus process can be used to identify a participant through the agreement of 51% nodes when the system needs to ban them from acting inappropriately. This can be done without compromising the system's overall performance.

III) Blockchain has the potential to greatly lower equipment costs and improve the overall efficiency of the IoT. Blockchain processes hundreds of billions of IoT transactions by fully utilizing P2P computing. Blockchain technology has the potential to lower setup and maintenance costs for centralized databases. In the meanwhile, the blockchain may fully utilize the internet, computational power, and storage capacity of idle IoT devices, which lowers computation and storage expenses [127].

IV) Products and services can have a longer life cycle thanks to blockchain. According to the blockchain concept, IoT assigns equipment maintenance duties to a community that takes care of itself. Regardless of whether a device is nearing the end of its life cycle or not, this fact keeps IoT relevant and will reduce infrastructure costs [128].

Blockchain is designed as 1) a private network with permissions that can be limited to a specific number of users.

2) A public, permission-less network that anybody can join [129]. One of the earliest and most popular apps to rely on blockchain technology is Bitcoin. Most well-known cryptocurrencies have utilized the technology and/or platform of the Bitcoin network. Digital currency transactions use Bitcoin. In July 2015, the Ethereum blockchain became live and became accessible to the public. The Ethereum blockchain can run smart contracts like Hyper ledger, Eris Stellar, Ripple, and Tender Mint in addition to storing records. Ethereum facilitates the use of its own virtual money, ether. User-written programs known as "smart contracts" can be uploaded to blockchains and run [130]. Data that is immutable cannot be deleted or changed. Blockchain increases access control and privacy.

J. PHYSICAL UNCLONABLE FUNCTION

Physical Unclonable Function (PUF) is a circuit chip. Every chip has a unique fingerprint that is formed during production, just like human fingerprints [131]. By incorporating a particular circuit architecture referred to as a PUF circuit into the chip, this inherent feature can be extracted. PUF circuits take an input consisting of a series of bits (so-called challenges) and output a response sequence of bits (so-called replies). No two chips ever produce the same results for a given stimulus. A challenge and the matching response that goes with it are referred to as a challenge-response pair (CRP) [132].

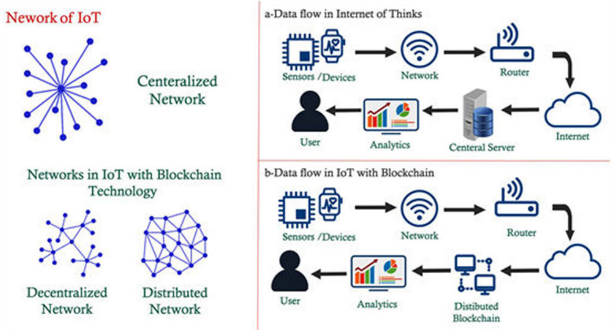

FIGURE 15. Blockchain in IoT.

PUFs are one potential hardware solution for identity and authentication in IoT applications. PUFs have the potential to be an inexpensive and useful solution for secret key generation since they extract distinctive hardware properties. Nonetheless, several obstacles restrict the PUFs' use in key generation. -based key generation approaches [133].

One strong and portable way to secure IoT devices is to use PUFs. PUF interoperability with IoT devices with constrained processing resources is its primary benefit over existing conventional cryptography methods. PUFs have been suggested as a scalable low-cost alternative. PUFs hold significant value for IoT developers as they guarantee completely secure authentication without requiring any cryptography assets on the device, making them particularly appealing for IoT devices with limited resources [134].

By including a unique PUF circuit, an IoT product can incorporate a PUF, for example, as a stand-alone ASIC or as a component of a system on a chip. Implementing a PUF circuit on reconfigurable hardware, such as a Field Programmable Gate Array (FPGA) is the alternative. With this second method, IoT developers have more control over the PUF architecture they employ and may more closely customize the system to meet their unique application requirements [135].

The authors in [136] mentioned that users must remember and continuously change their complex passwords. Users do not utilize high-entropy passwords, hence password authentication schemes are vulnerable to offline password-guessing attacks. They devised a safe authentication technique that combines password-protected biometrics and physical non-cloning functions.

Another model was developed to create a new lightweight mutual authentication protocol for RFID-based IoT systems using multipurpose digital logic encoder architectures [137]. Model multi-function logic circuits produce various logic outputs for each random selection of control inputs, significantly improving security. The protocol was described in Verilog Hardware, implemented on the Altera DE2 Cyclone II FPGA board (EP2C35F672C6), and synthesized into the technology platform for 180 and 90 nm ASICs. The suggested protocol was tested in real time on Jennic JN5168 test beds running Contiki OS for IoT applications with low resources.

Reference [138] proposed a static random-access memory (SRAM) stack for fingerprinting and an auto-encoding network (AEN) for fingerprinting and verification. They evaluated eleven AVR Harvard architecture probe devices from various vendors in a diverse pool. The fingerprint's independence in the AENs allows for easy distribution and update, and the observed assessment time (approx. 10-4 sec) and data gathering time (approx. 1 sec) make the approach useful in real-world applications.

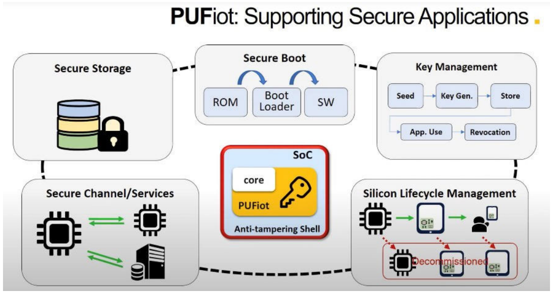

FIGURE 16. A Depiction of PUF.

K. QUANTUM COMPUTING

Peter Shor introduced the idea of quantum computing in 1994. It can calculate the physical properties of matter and energy and can break the RSA crypto-system, whose security depends on integer factorization, in polynomial time. Furthermore, according to the publishing of Shor's algorithm, a strong quantum computer would be able to defeat every contemporary communication security method, including key exchange and digital data authentication. As a result, every conventional public-key crypto-system was made useless [139].

To give one example, the advent of quantum computing will herald the end of conventional cryptography. The publickey crypto-system's security will vanish with the creation of the first quantum-factoring device. For public-key cryptography systems like RSA, the post-quantum transition presents numerous basic difficulties that must be resolved to prevent further intimidation. Quantum computers will be able to crack RSA with 2000 bits by 2030. Additionally, there is a risk to those crypto-systems that give security of 80 bits or fewer that were phased out between 2011 and 2013 [140].

Despite this, the use cases for post-quantum RSA rely on the remote chance of significant advancements in attacks against widely used alternatives, and the same critique is also heavily utilized as covered in On traditional computers, it is challenging to solve several hard crypto-system problems, including the conventional RSA algorithm, confidentiality and integrity, and other cutting-edge threats. Consequently, when quantum mechanics is considered, the idea becomes valid. This means that the traditional pre-quantum RSA methodology needs to be changed to a safe post-quantum cryptography-based RSA method.

Because IoT-based cloud applications require a lot of processing power, there has been a noticeable increase in interest in quantum computing in recent years [141]. Professionals and experts in computers have been working on developing quantum computers. These devices use quantum principles, which enable them to use these phenomena to solve mathematical problems that are too complex and difficult for classical computers, such as logarithmic problems and integer factorization.

Furthermore, these gadgets have the potential to propel advancements in artificial intelligence and effortlessly breach the encryption safeguarding crucial computers for national security. Public-key encryption is seriously threatened by this security scenario because it is unable to withstand quantum attacks by lengthening its keys faster than the rate at which quantum computing is developing. Particularly when considering IoT-based cloud applications, such security risks would jeopardize the secrecy and integrity of digital communications cryptography both online and offline. There is a lot of concern about this security hazard obstacle [142].

1) QUANTUM CYBER SECURITY TEST-BED

Testing platforms focus on quantum capabilities, despite security principles. Simulated systems avoid costs and complexity but are limited due to parallel processing capacity limitations. True quantum processing relies on superposition states in non-quantum devices. The Quantum Cryptography Secure Communication Project (SECOQC) in Vienna built a test platform for encryption communications and video conferences, demonstrating AES encryption and QKD protocol distribution, but limited transmission capacity [143].

Many physical test-bed environments focus on communication, for example, the 2004-2008 SECOQC project in Vienna utilizes AES encrypted communication and QKD protocols, but with limited transmission capacity and security guarantees in controlled networks. The IEQNET test bed (2021) demonstrated 90% fidelity of teleportation over approximately 44 km [144], demonstrating quantum entanglement and quantum teleportation. Oak Ridge National Laboratory groups have also demonstrated full control of frequencybin qubits, promoting frequency encoding potential [145]. Qubitekk and EPB collaborated on a commercial quantum network in Chattanooga, Tennessee, recognizing the maturity of quantum communications [146].

Other test-beds focus on computing capabilities such as the Sandia National Laboratory's QSCOUT research facility aims to build a 32-qubit quantum calculator using trapped ions, while services like AWS, Google, Quantinuum, IBM, and IBM use quantum computing resources. Security considerations are relevant in various areas, but the evaluation of experiments varies [147]. Experts may learn about quantum systems and their "red teaming" for vulnerability assessments and penetration tests. However, domain-specific knowledge and niche hardware resources may limit the need for quantum testbeds. A "user-facility" test bed is needed, similar to largescale research infrastructures.

Quantum computing's rapid development poses a significant threat to current public key encryption standards, including the Shor Algorithm. This algorithm, used in digital applications like email, banks, and defense, could be broken by quantum machines, despite their development taking 30 years [IEEE]. Accelerated quantum computing has significantly impacted public key encryption standards, including Shor Algorithms, making them unsafe. These algorithms are crucial in digital applications like email, banking, and digital currency. It's too risky to ignore quantum machines' potential to break systems [147].

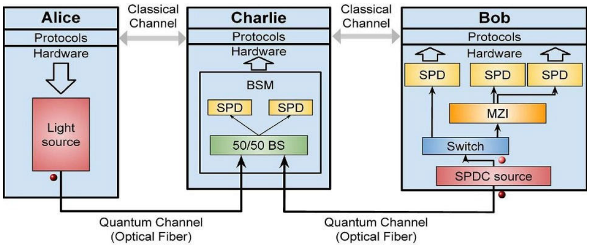

FIGURE 17. Quantum computing concept.

L. GREEN IOT (GIOT)

The GIoT is an energy-efficient IoT that aims to link everything, anywhere, at any time, and with a key characteristic that energy needs must come first. The fact that the components of the GIoT are identifiable, recognizable, intelligent, and autonomous and that they can access and share data and with other objects makes it an amazing technology. A GIoT schematic. GIoT will be necessary in the future since it can save energy and protect the environment for coming generations. As IoT (IoT) connects different objects anywhere, anytime, and with anything, the large number of IoT gadgets and their proximity to people, energy efficiency is a basic need for this technology. In general, focusing on energy efficiency at different IoT levels results in Green IoT (GIoT), which lowers costs while lowering risks to human health [148].

Green IoT is crucial for reducing energy use and promoting environmental sustainability. The GIoT program aims to enhance energy efficiency across IoT systems, involving academic and industrial research on software optimization and hardware improvement. This research covers various challenges and solutions in IoT energy efficiency. The study focuses on energy efficiency in IoT networks and devices, evaluating hardware and software components for improvement. It also investigates ecologically-friendly manufacturing processes and materials, examining the environmental impacts of sound production methods and sustainable materials [149].

The study emphasizes the importance of integrating renewable energy sources like solar and wind power into Green IoT devices, incorporating optimization and data analytics techniques to enhance energy efficiency and sustainability. The study explores the potential of IoT sensors for environmental programs, resource management, and e-waste elimination. It explores strategies to prolong device life, promote upgradeability, and promote ethical disposal practices. Compliance with environmental standards and legislation is closely scrutinized, with recommendations for future policy revisions.

Some literature such as [00] discusses energy consumption and technology concerns, emphasizing green IoT, security, trends, and global carbon footprint, offering solutions for technical advancements and addressing the planet's carbon footprint. Again, authors in [00] explore the trend of IoT development, highlighting its potential for careless use and the need for green IoT. It emphasizes the importance of ecologically responsible technology use, particularly in healthcare and agriculture. The article also discusses sensor cloud integration models.

In [150] studies explore IoT development trends, emphasizing careless use and green IoT, especially in healthcare and agriculture, and discuss sensor cloud integration models. Other authors in [151] emphasize the importance of responsible and efficient use of IoT in daily activities, emphasizing the need for green energy-based technology development. In [152], the aim is to transform IoT networking into an environmentally friendly platform by enhancing network coding's functionality in communication and reliable storage.

We can say that if suitable industrial and scientific solutions are offered to address difficulties like security concerns, lack of standards, and technological limitations, GIoT will prove to be a viable and suitable substitute for IoT. It is believed that as GIoT develops and grows, CO2 emissions from various businesses will be reduced and managed. The four core components of the GIoT are communication, architecture, hardware, and software. On the other hand, there are certain technological difficulties, standards, security concerns, and other unresolved issues with GIoT implementation. However, to speed up the recycling of GIoT equipment, renewable materials need to be created.

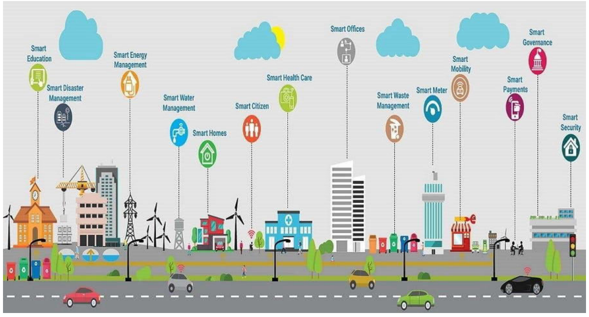

FIGURE 18. A depiction of GIoT environment.

IV. SMART APPLICATION DOMAINS

IoT increased the connectivity of digital objects, called intelligent objects, based on standard interoperability communication protocols, which have their identity, physical characteristics, and virtual characteristics [153]. Intelligent objects are connected to wireless interfaces and integrate the concept of object-oriented interfaces with RFID, which enables objects to communicate through the Internet, receive data, interpret the meaning of data, act intelligently, and react appropriately to the environment. Internet connectivity brings the concept of Internet-oriented. Then it followed semantic oriented, where machine representations, in combination with other intelligent technologies, demonstrated promise in describing objects, sharing, integrating information, and creating new knowledge by inference [154]. The following are some of the major smart areas of IoT in use today.

A. SMART HOME

In recent years, smart homes have become increasingly popular. It is estimated that the average household will contain 500 or more smart devices [107]. Smart homes have the vision to add intelligence to everyday household objects such as appliances, door locks, surveillance cameras, furniture, and storage doors to build them and interact with existing Internet infrastructure. The addition of intelligence to physical objects offers many advantages, including better convenience, safety, and efficient use of natural resources. For example, Smart Home adjusts the blinds according to environmental changes to save energy, automatically opens the garage door when an authorized vehicle approaches, or automatically orders medical services when an emergency occurs.

In smart homes, traditional household appliances are part of existing Internet extensions. If the device is damaged, the consequences may be severe. For example, a successful hack of a smart lock can allow intruders to enter the house; a compromise of a baby monitor can scare a baby from intruders; a hack of a microwave can cause a fire in the house. Smart Homeowners may not want to live in Smart Home if safety is a concern. Instead, they can expect to improve home security through intelligent surveillance services [155]. In addition, the privacy of smart homeowners must be maintained. However, continuous data collection from smart home devices can reveal homeowners' private activities. It poses serious threats to the privacy of homeowners.

An essential component of this urban ecosystem is the home, which is currently a sophisticated structure with several interrelated systems and frameworks, including utilities, security, and lighting [156]. Building complexity increases with building growth, and buildings are susceptible to disturbing disturbances that could jeopardize resources and life safety. The potential for smart buildings should be to lessen the effects of infiltration, enable proactive and intelligent data management to support preventive activities and actions, and enhance the overall quality of life [18]. It is anticipated that effective control and security technology will reduce the number of undesired items in private residences.

For instance, if a theft occurs while the house is unoccupied and locked. Thanks to the IoT, many individuals can now do things that previously seemed like dreams, such as voice-activated heater control. IoT Smart Homes combines technology and smartness. The IoT was first introduced in the early 1980s, whereas the smart house was first offered in 1975. Numerous scholars have expressed interest in this subject since then. Since 2017, in particular, the research on IoT applications in smart homes has advanced quickly.

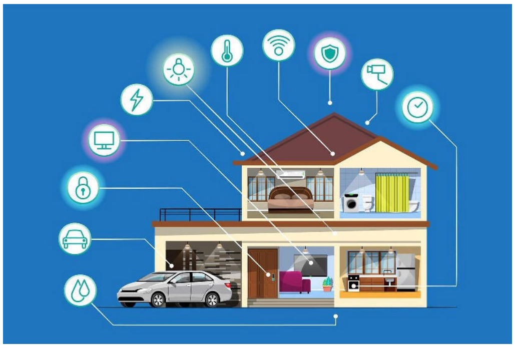

FIGURE 19. A typical smart home.

The development of smart home systems has been made possible by the IoT. Homeowners can operate their appliances both manually and automatically with smart home automation. Previous studies have shown that with the aid of electronic platforms like Arduino, ESP8266, and Raspberry Pi, the majority of IoT implementations on smart homes use a certain kind of messaging/communication protocol, such as the (Message Queuing Telemetry Transport) MQTT protocol [157]. Constructing an IoT-based smart house primarily aims to provide smart home monitoring and control, which can enhance quality of life and bring comfort, effectiveness, and energy efficiency.

B. SMART CITY

IoT is used in the development, implementation, and upkeep of smart cities. Urban expansion has reached a new technological level of user convenience and ease of life. The term "smart city" refers to a broad notion that includes managing and organizing a city using embedded technology. A smart city must be able to use IoT-embedded technology to integrate all of its infrastructures, administration, governance, people and communities, health, education, and natural environment [108]. These IoT technologies include electronics, sensors, and networks that are connected to computer systems that have databases, tracking, and algorithms for making decisions.

Concerns about economic restructuring, environmental challenges, governance issues, and public sector problems that require more intelligent solutions are growing with the increase in urbanization. The enormous rate of development in modern cities is making the problems they face more complex. Thus, wiser growth is promised by the smart city. With smart cities utilizing the most recent technological advancements to seamlessly accelerate urbanization, the globe has truly become a global village where communication, information access, and distant interaction, integration, and cooperation are now conceivable. Smart cities that are

FIGURE 20. A typical smart city.

leading the way include Barcelona, Amsterdam, Singapore, and France [158].

C. SMART GRID

Another typical IoT application is the construction of smart grids. Smart grids are designed and implemented to improve the reliability, cost savings, and performance of traditional power networks. It aims to integrate green and renewable energy, such as wind power, geothermal power, and solar power, and to improve the reliability and management of traditional power networks more efficiently [159]. The intelligent grid data communication network connects many intelligent grid devices and plays an important role in achieving the above objectives. It not only collects energy consumption data but also monitors the status of intelligent network systems [160].

Many new applications can be developed based on smart grid data communication networks. As an example, utilities can better distribute and balance the load based on the collected energy consumption information. It also helps to design a fair but scaled pricing model taking into account insufficient energy consumption in the time and space dimensions. By building intelligent network status monitoring applications, it is possible to detect network system failures as soon as possible and design new failure-tolerant mechanisms to better respond to failures.

Many technologies, including automatic measuring infrastructure [161], have been proposed to build intelligent network communications networks. Intrusion into the intelligent network and cutting off power supplies to a large area may cause enormous physical and economic damage to society. Analyzing energy use data can also reveal the daily private activities of individuals [162]. Moreover, attack data integrity and false data injections can interfere with the smart network charging system, disrupt the network start-up state estimate, disturb the electricity flow, and delay the response to demand. Smart grids replace conventional energy grids because they provide efficient, reliable, intelligent, and interactive features.

Smart grids not only manage power distribution but also guarantee customers' current and future needs. Smart grid is a digital computing and communications technology integrating digital computing and communications to improve the traditional power grid and provide a secure, efficient, reliable power supply and information exchange between power plants, utilities, and consumers [163].

Therefore, the intelligent network is a smart power infrastructure that can maintain power providers, distributors, and consumers' operational needs in real-time. Through smart grids, consumers can use efficient and higher-quality electricity, communicate with smart meters or electricity providers, and manage their consumption. Conventional electricity distributes electricity in one way, so consumers cannot participate and cannot tailor their consumption needs [164].

Smart grids are electrical distribution systems that distribute energy flows from manufacturers to users in two directions and have electrical functions such as intelligent meters, intelligent machines, sustainable energy resources, and efficient energy supplies. Smart grids are the fundamental components of energy management, reliability, cost-effectiveness, and sustainable environment energy independence. IoT has become the largest computing platform. It has been applied in many application areas such as logistics [165], intelligent homes [166], intelligent cities [167], intelligent health [168], intelligent connected vehicles [169], and intelligent networks [170], smart farming [171].

Electricity suppliers have launched campaigns to replace old electricity meters with smart meters that enable two-way communication between the smart meters and the Metering Data Management System (MDMS). Meter readings can be sent directly and automatically to the MDMS to generate bills etc. without the need for human intervention. Each smart meter in the network monitors its neighbors and reports any malfunctioning activity. The compromised node can launch various types of malicious attacks, such as black hole attacks, sinkhole attacks, injecting false information, and jamming the channels [172].

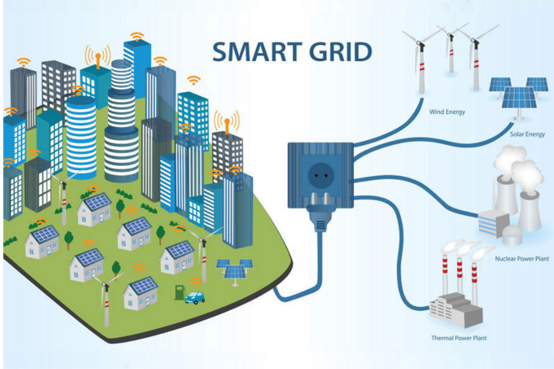

FIGURE 21. A typical smart grid.

D. SMART HEALTHCARE

It is proposed that Smart Health improves the efficiency of health systems and reduces health costs. Market Research analyst predicts that the sector is worth $117 billion as of 2020. By integrating smart health devices into existing health infrastructures, health professionals can monitor patients more effectively and use data collected from these devices to determine who needs the greatest attention. In other words, health professionals can build proactive management systems based on the collected data because prevention is more important and effective than treatment and using a network of devices.

Researchers also study techniques for installing sensors into the human body to monitor their health [168]. Health professionals can discover behavior changes in patients with diseases and medications during treatment. Integrated health and security is also an important concern. Networked medical devices are convenient to collect data and verify the status of devices, but are also dangerous, as instructions can be sent to stop the device's function.

In addition, most of the data collected in the system are very sensitive medical data, privacy is an important issue in intelligent connected health care [164]. Without a doctor present, smart flexible wearable linked with RFID technology in hospitals will be able to monitor patients' blood pressure, heart rate, temperature, and other vital signs. In an emergency, a drone ambulance can fly with a medical kit to administer first aid until an ambulance arrives or until the hospital is reached.

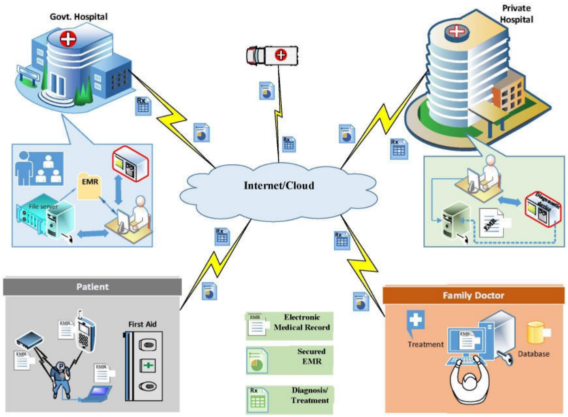

FIGURE 22. A typical smart health.

E. INTELLIGENT TRANSPORTATION SYSTEM

Research has shown the synergy between Intelligent Transportation Systems and IoT as a transformative paradigm in the field of transportation. IoT sensors can be mounted on vehicles to track their location, search for availability of parking space, intelligent traffic management, information about the road ahead, and so on. All this is achieved via the analysis of the data generated and shared from the sensors in the field, on the cars, and in other places and objects. A smart transportation system added to the development of a state. Intelligent traffic management is essential in any populated city, it helps reduce the time people spend on the road, helps reduce accident rates, and gives information that helps the driver make certain decisions. Road signs are again helpful to drivers as they help connect and navigate through the road network [173].

Smart infrastructure can be realized when IoT technology is embedded in modern transportation systems such as traffic lights, and adaptive traffic management systems. Consider for example four-side traffic that allocates an equal amount of time of say one minute to every side of the traffic while in reality, one side is denser than the others, it will create a long traffic queue on that side and leave other less traffic sides empty. But with intelligent traffic, the system will decide on the amount of time to be allocated to each side and permit those that need to pass if there is no one at the moment.

Therefore, IoT technology integration into transportation systems has the potential to produce more effective, Ecofriendly, and user-friendly mobility solutions; nevertheless, security, privacy, and legal issues need to be carefully taken into account [174]. Smart infrastructure can be realized when the IoT technology is embedded in modern transportation systems such as traffic lights, and adaptive traffic management systems. Consider for example four-side traffic that allocates an equal amount of time of say one minute to every side of the traffic while in reality, one side is denser than the others, it will create a long traffic queue on that side and leave other less traffic sides empty.

But with intelligent traffic, the system will decide on the amount of time to be allocated to each side and permit those that need to pass if there is no one at the moment. Therefore, IoT technology integration into transportation systems has the potential to produce more effective, Eco-friendly, and user-friendly mobility solutions; nevertheless, security, privacy, and legal issues need to be carefully taken into account [174].

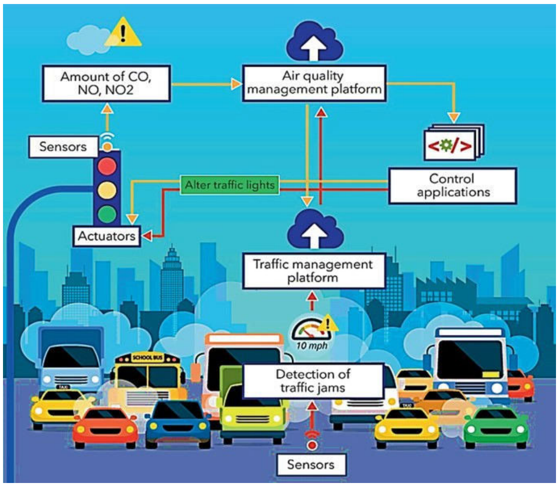

FIGURE 23. An intelligent transport system.

F. SMART EDUCATION

The term ''smart education'' describes the application of cutting-edge ideas and technology to improve the educational process. To make education more interactive, individualized, and accessible, it entails integrating digital tools like artificial intelligence, online learning environments, and interactive whiteboards. The goal of smart education is to use technology to enhance instruction, involve students, and streamline the learning process as a whole. By using cutting-edge technologies to change the classroom, smart education goes beyond conventional teaching techniques [175]. It entails utilizing technologies like artificial intelligence, augmented reality, and virtual reality to produce engaging and dynamic learning environments.

The main goals of smart education are to accommodate different learning styles, encourage teamwork, and give teachers and students immediate feedback. This method seeks to prepare students for the challenges of a quickly changing digital world by making learning more dynamic, interesting, and customized to meet their individual requirements [104]. Smart education takes place in a smart environment that integrates various ICT tools and a whole range of new technologies (e.g. AI, ubiquitous, and cloud computing) into the traditional classroom to enable a high-quality and interactive educational process [176].

Smart school management with solutions for smart management of transportation, energy consumption, school and campus security, access to classrooms and other facilities, monitoring student activity and participation in the learning process, etc. These functions are achieved through specialized applications such as IoT sensors and actuators, cameras, data collectors, cloud computing, artificial intelligence, and machine learning algorithms. Temperature, lighting, humidity, and oxygen levels are a few of the physical aspects of the school environment that have an impact on learning [177].

To provide the best possible learning environment, they are appropriately observed and managed. An enormous amount of data about the classroom environment is gathered and analyzed by several sensors. Through the use of wearable technology, cameras, motion sensors, RFID readers, and other devices, the learning process flow is monitored. They monitor students' participation, keep an eye on their presence, identify inappropriate behavior, and keep tabs on how students communicate within the learning system.

The IoT changes the conventional classroom setting into an intelligent, next-generation setting with improved and more effective learning procedures. To do this, intelligent systems for access control, lighting, heating, air conditioning, air quality monitoring, and other facilities must be integrated with intelligent systems that handle the actual learning process, such as keeping an eye on student behavior, noise levels, in-class fidgeting, etc. These systems are linked to a cloud-based control center that processes and analyses sensor data to control other environmental factors [178].

G. SMART AGRICULTURE

To improve farming methods, smart agriculture makes use of technology such as sensors, data analytics, and the IoT. Precision farming is included, where resource usage is optimized through data-driven decision-making. Farm management software, robots, and automation simplify operations, while remote monitoring allows for fast reactions to shifting circumstances. Enhancing productivity, minimizing the impact on the environment, and advancing sustainable agriculture are the objectives [179].

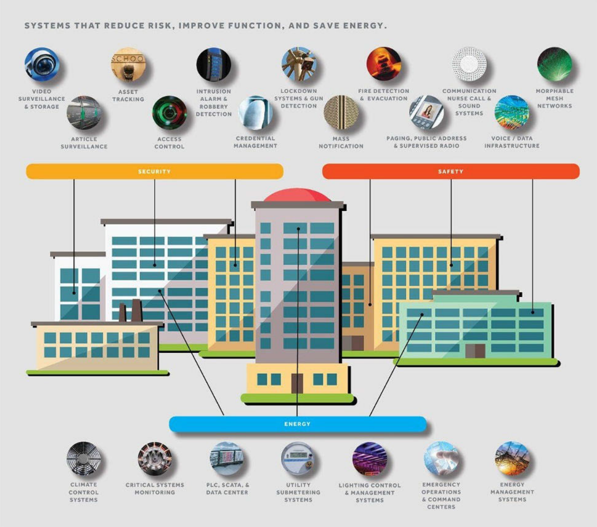
SYSTEMS THAT REDUCE RISK, IMPROVE FUNCTION, AND SAVE ENERGY.
VIDEO SURVEILLANCE & STORAGE
ARTICLE SURVEILLANCE
ASSET TRACKING
ACCESS CONTROL
INTRUSION ALARM & ROBBERY DETECTION
CREDENTIAL MANAGEMENT
LOCKDOWN SYSTEMS & GUN DETECTION
MASS NOTIFICATION
FIRE DETECTION & EVACUATION
PAGING, PUBLIC ADDRESS & SUPERVISED RADIO
COMMUNICATION NURSE CALL & SOUND SYSTEMS
VOICE / DATA INFRASTRUCTURE
MORPHABLE MESH NETWORKS
SECURITY
SAFETY
ENERGY
CLIMATE CONTROL SYSTEMS
CRITICAL SYSTEMS MONITORING
PLC, SCATA, & DATA CENTER
UTILITY SUBMETERING SYSTEMS
LIGHTING CONTROL & MANAGEMENT SYSTEMS
EMERGENCY OPERATIONS & COMMAND CENTERS
ENERGY MANAGEMENT SYSTEMS

FIGURE 24. A typical smart education system.

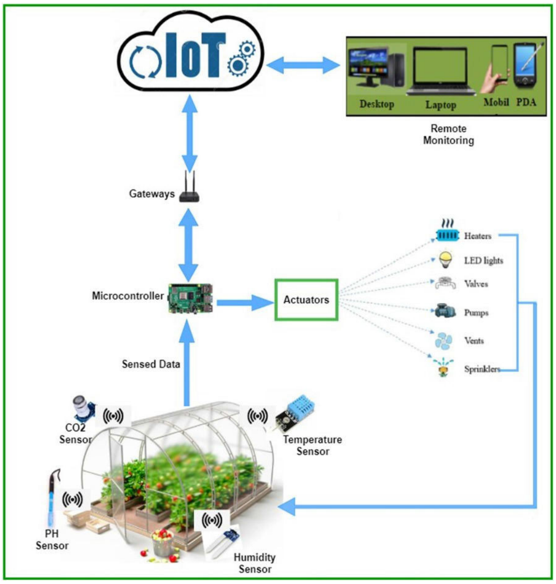

FIGURE 25. A typical smart agriculture

A high-tech farming method known as ''smart agriculture'' uses cutting-edge technologies to provide the best possible agricultural management. It transforms conventional farming methods by fusing sensors, data analytics, and the IoT. Cloud-based IoT design for precise agriculture [180] has been presented and has emerged as a prominent technology with widespread applications in a variety of industries, including agriculture. Farmers can acquire information about greenhouse farms for a minimal cost by using video, pictures, and short message services.

Furthermore, cloud computing is capable of managing large-scale intelligent computing systems [181]. The integration of IoT-based agriculture with cloud computing accelerates monitoring, facilitates maintenance, simplifies understanding, and precisely addresses greenhouse

TABLE 2. Differences between IoT and the Internet.

No	IoT	INTERNET
1	Uses RFID nodes & WSN nodes	Use PCs, servers, etc
2	Can only utilize lightweight algorithms	Can use combination of complex and lightweight algorithms
3	Connection is always through slower, less secure wireless media	Connection is faster through more secure wired or wireless media
4	Very easy node compromise	Can compromise device by skilled attacker
5	Slow acceptance in the society	Wide acceptance and usage in the society
6	IoT network is more vulnerable to attack	Vulnerable also but not as in IoT
7	Can only accommodate its own protocols	Can accommodate all protocols
8	Mostly require our personal information to assist us and makes our life easier	Can run to do other works without supplying our personal information
9	Specific operating system	Generic operating system
10	Limited resources and less network guard	More resources and protection
11	Makes life convenient	Makes life better
12	Directly leads to big data problem	When data increases can become big data
13	Nodes are deployed in more dangerous environment	Devices are placed in homes and offices
14	Security issues should be treated as indivisible entity	Security issues can be addressed from its architecture
15	Customized architecture (no single framework to handle all cases)	The architecture is more standardized and generic
16	Deployment based on LLN	Deployment based on dynamic topologies
17	Characterized by great data loss due to impersonation and attacks	Data loss is minimized, high data loss will affect the whole network performance
18	Supports only lightweight technology such as lightweight cryptographic algorithm	Supports conventional cryptographic algorithms which are complex in nature
19	The architecture is a stack as the most widely accepted and adopted i.e the perception, network, and application layers	The architecture is the conventional 7-layer stack of the OSI model
20	The perception layer nodes have limited power and low computational ability	The data link layer can accommodate more devices
21	The network layer is vulnerable to man in the middle and counterfeit attack	The network layer is vulnerable to modifying the routing table
22	The application layer encounters security problems such as data privacy, access control, and disclosure of information	The application layer is only concerned about the management of apps, their data, and services
23	Physical layer protocol: IPV6 is used over 6LoWPAN in the IoT perception / physical layer	Physical layer protocol: Wi-Fi is used in the physical layer of the internet
24	Network layer protocol: the DTLS is used for transmission over the network	Network layer protocol: the TCP is used for transmission over the network
25	Application layer protocol: the CoAP is used for communication over the network	Application layer protocol: the HTTP is used for communication over the network
26	The security architecture is aimed at integrating seamless communication among objects and people	The conventional security architecture is designed based on the perspective of users and not applicable for communication among machines

cultivation issues [182]. A model in [183] described an IoT-based greenhouse network architecture built on cloud technology. The model allows greenhouse resource managers to manage a large number of requests while also efficiently managing resources.

Their platform consists of three types of cloud services: software as a service (SaaS), platform as a service Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The network can give data for a variety of reasons within the greenhouse, such as pest management information, meteorological conditions, irrigation information, and so forth [184]. Developed cloud integration solutions that evaluate big data quantities and automate agricultural monitoring despite inadequate network information.

The new method also accelerates data processing and aids pest management in smart greenhouse plants [184], [185]. The agricultural system used cloud computing, IoT technology, and sensor data. The primary goal of this system is to successfully control all environmental parameters of intelligent greenhouse farms using fuzzy controllers to reduce complexity [185]. To put it simply, smart agriculture uses technology to build an ecosystem of farming that is efficient, data-driven, and sustainable.

Farmers may increase productivity, lessen their impact on the environment, and support the long-term survival of agriculture by adopting these innovations [164]. Greenhouses will benefit from smart agriculture's ability to regulate temperature, monitor soil nutrition, lighting, humidity, and precise watering and fertilizing. The merchant will be able to keep track of the goods and products that are available, together with their smart supply chain management and retailing. The things themselves can even make orders automatically when they are about to run out.

V. IoT VS INTERNET

RFID, Zigbee, Bluetooth, and other short-range wireless technologies are used to connect the IoT to the internet. The Internet Assigned Numbers Authority (IANA) depleted the IPV4 addressing scheme in February 2011, making the transition to IPV6 necessary as billions of connected devices must be identified online. IEEE standards body is responsible for implementing IoT in terms of privacy, security, and network architecture.

VI. CONCLUSION AND IOT FUTURE VISION

Imagine a situation in which someone wakes up from a nap, imagine a situation where someone resides in a smart city, and a series of events take place after the person wakes up from sleep and ends when he gets back home (i.e. work hours events). He uses the restroom first. The door to the bathroom opens automatically, next, the water faucet is turned on for a variable interval of time. The apartment door opens as he walks in front of it. The elevator's door will open as he approaches it, and it will be adjusted to stop at the person's preferred level. These actions are performed from when he wakes up and go on until he reaches his workplace.

Standardization is a good solution to IoT problems. It will assist in resolving issues with cost, complexity of communication, and compatibility and generally simplify IoT problems. For example, contacting an IoT refrigerator is to contact the owner at home but if the refrigerator is in a hospital who to contact requires multiple parameters, therefore a need for standardization. Three stand-alone IoT applications are marketing, transportation, and healthcare. However, the issue of duplication can be solved if these three applications are combined into one and made into smaller apps.

REFERENCES

[1] J. H. Kim, "A survey of IoT security: Risks, requirements, trends, and key technologies," *J. Ind. Integr. Manage.*, vol. 2, no. 2, Jun. 2017, Art. no. 1750008.

[2] M. Aboubakar, M. Kellil, and P. Roux, "A review of IoT network management: Current status and perspectives," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4163–4176, Jul. 2022.

[3] M. Jung, E. Hajdarevic, W. Kastner, and A. Jara, "Short paper: A scripting-free control logic editor for the Internet of Things," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 193–194.

[4] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for intelligent IoT-enabled WSNs," *Comput. Electr. Eng.*, vol. 105, Jan. 2023, Art. no. 108495.

[5] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Comput. Ind. Eng.*, vol. 155, May 2021, Art. no. 107174.

[6] G. Beniwal and A. Singhrova, "'A systematic literature review on IoT gateways,'" *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9541–9563, Nov. 2022.

[7] D. Misra, G. Das, and D. Das, "Review on Internet of Things (IoT): Making the world smart," in *Advances in Communication, Devices and Networking*, R. Bera, S. K. Sarkar, and S. Chakraborty, Eds., Singapore: Springer, 2018, pp. 827–836.

[8] S. Secgin, "Internet of Things (IoT)," in *Evolution of Wireless Communication Ecosystems (IoT)*, 3rd ed., Hershey, PA, USA: IGI Global, 2023, pp. 177–189.

[9] I. Muhic and M. Hodzic, "Internet of Things: Current technological review," *Periodicals Eng. Natural Sci. (PEN)*, vol. 2, no. 2, pp. 1–8, Dec. 2014.

[10] V. Tuomala, "IoT productivity versus cybersecurity. Is the risk worth it?" South-Eastern Finland Univ. Appl. Sci., Kotka, Finland, Tech. Rep., 2021.

[11] A. Fehske, G. Fettweis, J. Malmodin, and G. Biczok, "The global footprint of mobile communications: The ecological and economic perspective," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 55–62, Aug. 2011.

[12] M. M. Pohan and B. Soewito, "Injection attack detection on Internet of Things device with machine learning method," *Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika)*, vol. 8, no. 1, pp. 204–212, 2023.

[13] M. Chui, M. Collins, and M. Patel, "The Internet of Things: Catching up to an accelerating opportunity," McKinsey Company, New York, NY, USA, 2021.

[14] P. Vijay, "Evolution of Internet of Things go-to-market strategies for semiconductor companies," Ph.D. dissertation, Dept. Syst. Des. Manag. Eng. Syst. Division, Massachusetts Inst. Technol., USA, 2015.

[15] 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.

[16] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[17] S. Zahoor and R. N. Mir, "Resource management in pervasive Internet of Things: A survey," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 33, no. 8, pp. 921–935, Oct. 2021.

[18] A. Yudidharma, N. Nathaniel, T. N. Gimli, S. Achmad, and A. Kurniawan, "A systematic literature review: Messaging protocols and electronic platforms used in the Internet of Things for the purpose of building smart homes," *Proc. Comput. Sci.*, vol. 216, pp. 194–203, Jan. 2023.

[19] K. Bajaj, B. Sharma, and R. Singh, *Integration of WSN With IoT Applications: A Vision, Architecture, and Future Challenges*. Cham, Switzerland: Springer, 2020, pp. 79–102.

[20] D. Wang, P. Wang, and C. Wang, "Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 3, pp. 1–26, Jul. 2020.

[21] M. Mounica, R. Vijayasaraswathi, and R. Vasavi, "Detecting Sybil attack in wireless sensor networks using machine learning algorithms," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1042, no. 1, Jan. 2021, Art. no. 012029.

[22] J. S. Yalli, S. B. A. Latif, A. H. A. Hashim, and M. K. Alam, "An improved QoS in the architecture, model and huge traffic of multi-media applications under high speed wireless campus network," *ARPN J. Eng. Appl. Sci.*, vol. 9, no. 12, pp. 1–14, 2014.

[23] M. Elappila and S. Chinara, "Implementation of survivability aware protocols in WSN for IoT applications using contiki-OS and hardware testbed evaluation," *Microprocessors Microsystems*, vol. 104, Feb. 2024, Art. no. 104988. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0141933123002338

[24] A. Seyfollahi, T. Taami, and A. Ghaffari, "Towards developing a machine learning-metaheuristic-enhanced energy-sensitive routing framework for the Internet of Things," *Microprocessors Microsyst.*, vol. 96, Feb. 2023, Art. no. 104747.

[25] O. Iova, F. Theoleyre, and T. Noel, "Using multiparent routing in RPL to increase the stability and the lifetime of the network," *Ad Hoc Netw.*, vol. 29, pp. 45–62, Jun. 2015.

[26] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Gener. Comput. Syst.*, vol. 100, pp. 882–892, Nov. 2019.

[27] R. Vinoth and L. J. Deborah, "An efficient key agreement and authentication protocol for secure communication in industrial IoT applications," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 3, pp. 1431–1443, Mar. 2023.

[28] A. Sunyaev, *Cloud Computing*. Cham, Switzerland: Springer, 2020, pp. 195–236.

[29] M. S. Mekala and P. Viswanathan, "A novel technology for smart agriculture based on IoT with cloud computing," in *Proc. Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)*, Feb. 2017, pp. 75–82.

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

[31] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[32] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *J. Inf. Secur. Appl.*, vol. 42, pp. 95–106, Oct. 2018.

[33] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[34] S. Alraddady, A. S. Li, B. Soh, and M. Alzain, "Deployment of fog computing during Hajj season: A proposed framework," *Proc. Comput. Sci.*, vol. 161, pp. 1072–1079, Jan. 2019.

[35] H. Xiong, T. Yao, H. Wang, J. Feng, and S. Yu, "A survey of public-key encryption with search functionality for cloud-assisted IoT," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 401–418, Jan. 2022.

[36] H.-J. Hong, "From cloud computing to fog computing: Unleash the power of edge and end devices," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2017, pp. 331–334.

[37] A. Khakimov, A. Muthanna, and M. S. A. Muthanna, "Study of fog computing structure," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 51–54.

[38] Q. Duan, S. Wang, and N. Ansari, "Convergence of networking and cloud/edge computing: Status, challenges, and opportunities," *IEEE Netw.*, vol. 34, no. 6, pp. 148–155, Nov. 2020.

[39] C. Ding, A. Zhou, Y. Liu, R. N. Chang, C.-H. Hsu, and S. Wang, "A cloud-edge collaboration framework for cognitive service," *IEEE Trans. Cloud Comput.*, vol. 10, no. 3, pp. 1489–1499, Jul. 2022.

[40] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Gener. Comput. Syst.*, vol. 83, pp. 326–337, Jun. 2018.

[41] F. Bonomi, R. Milito, P. Natarajan, and J. Zhu, *Fog Computing: A Platform for Internet of Things and Analytics*. Cham, Switzerland: Springer, 2014, pp. 169–186.

[42] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "A PUF-based mutual authentication scheme for cloud-edges IoT systems," *Future Gener. Comput. Syst.*, vol. 101, pp. 246–261, Dec. 2019.

[43] A. Celesti, M. Fazio, A. Galletta, L. Carnevale, J. Wan, and M. Villari, "An approach for the secure management of hybrid cloud-edge environments," *Future Gener. Comput. Syst.*, vol. 90, pp. 1–19, Jan. 2019.

[44] M. Goudarzi, M. Palaniswami, and R. Buyya, "Scheduling IoT applications in edge and fog computing environments: A taxonomy and future directions," *ACM Comput. Surv.*, vol. 55, no. 7, pp. 1–41, Jul. 2023.

[45] D. Espinel Sarmiento, A. Lebre, L. Nussbaum, and A. Chari, "Decentralized SDN control plane for a distributed cloud-edge infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 256–281, 1st Quart., 2021.

[46] T. Wang, Y. Lu, J. Wang, H.-N. Dai, X. Zheng, and W. Jia, "EIHDP: Edge-intelligent hierarchical dynamic pricing based on cloud-edge-client collaboration for IoT systems," *IEEE Trans. Comput.*, vol. 70, no. 8, pp. 1285–1298, Aug. 2021.

[47] K. Noda, "Google home: Smart speaker as environmental control unit," *Disab. Rehabil., Assistive Technol.*, vol. 13, no. 7, pp. 674–675, Oct. 2018.

[48] J. Li, J. Jin, L. Lyu, D. Yuan, Y. Yang, L. Gao, and C. Shen, "A fast and scalable authentication scheme in IoT for smart living," *Future Gener. Comput. Syst.*, vol. 117, pp. 125–137, Apr. 2021.

[49] A. Younis, T. X. Tran, and D. Pompili, "Bandwidth and energy-aware resource allocation for cloud radio access networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6487–6500, Oct. 2018.

[50] J. S. Yalli, M. H. Hasan, N. S. Haron, M. U. R. Shaikh, N. Y. Murad, and A. L. Bako, "Quality of data (QoD) in Internet of Things (IoT): An overview, state-of-the-art, taxonomy and future directions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 12, p. 1075, 2023.

[51] K. Singh and D. S. Tomar, "Architecture, enabling technologies, security and privacy, and applications of Internet of Things: A survey," in *Proc. 2nd Int. Conf. I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC)I-SMAC (IoT Social, Mobile, Anal. Cloud) (I-SMAC), 2nd Int. Conf.*, Aug. 2018, pp. 642–646.

[52] H. Kurdi and V. Thayananthan, "Authentication mechanisms for IoT system based on distributed MQTT brokers: Review and challenges," *Proc. Comput. Sci.*, vol. 194, pp. 132–139, Jan. 2021.

[53] X. Xingmei, Z. Jing, and W. He, "Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of Things," in *Proc. 3rd Int. Conf. Comput. Sci. Netw. Technol.*, Oct. 2013, pp. 825–828.

[54] F. M. Ribeiro Junior, R. A. C. Bianchi, R. C. Prati, K. Kolehmainen, J.-P. Soininen, and C. A. Kamienski, "Data reduction based on machine learning algorithms for fog computing in IoT smart agriculture," *Biosyst. Eng.*, vol. 223, pp. 142–158, Nov. 2022.

[55] K. M. Hosny, W. M. El-Hady, and F. M. Samy, "Technologies, protocols, and applications of Internet of Things in greenhouse farming: A survey of recent advances," *Inf. Process. Agricult.*, Apr. 2024, doi: 10.1016/j.inpa.2024.04.002. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214317324000222

[56] P. S. Souza, T. Ferreto, and R. N. Calheiros, "EdgeSimPy: Python-based modeling and simulation of edge computing resource management policies," *Future Gener. Comput. Syst.*, vol. 148, pp. 446–459, Nov. 2023.

[57] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[58] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE Access*, vol. 8, pp. 85714–85728, 2020.

[59] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, 2013.

[60] A. Z. M. Alhowaide, "Towards autonomous IoT idss using ensemble learning and feature selection methods," Ph.D. dissertation, Dept. Sci., Fac. Comput. Sci., Memorial Univ. Newfoundland, St. John's, NL, Canada, 2021.

[61] T. Mohamed, T. Otsuka, and T. Ito, "Towards machine learning based IoT intrusion detection service," in *Proc. Int. Conf. Ind., Eng. Appl. Appl. Intell. Syst.* Cham, Switzerland: Springer, 2018, pp. 580–585.

[62] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 266–282, 1st Quart., 2014.

[63] A. Verma and V. Ranga, "ELNIDS: Ensemble learning based network intrusion detection system for RPL based Internet of Things," in *Proc. 4th Int. Conf. Internet Things, Smart Innov. Usages (IoT-SIU)*, Apr. 2019, pp. 1–6.

[64] A. J. Siddiqui and A. Boukerche, "TempoCode-IoT: Temporal codebook-based encoding of flow features for intrusion detection in Internet of Things," *Cluster Comput.*, vol. 24, no. 1, pp. 17–35, Mar. 2021.

[65] W. Fang, X. Tan, and D. Wilbur, "Application of intrusion detection technology in network safety based on machine learning," *Saf. Sci.*, vol. 124, Apr. 2020, Art. no. 104604.

[66] J. S. Yalli, S. B. A. Latif, and S. Bari, "Interactive multi-media applications: Quality of service guaranteed under huge traffic," *Int. J. Comput. Appl.*, vol. 105, no. 7, pp. 1–8, 2014.

[67] R. Singh, H. Kumar, R. K. Singla, and R. R. Ketti, "Internet attacks and intrusion detection system: A review of the literature," *Online Inf. Rev.*, vol. 41, no. 2, pp. 171–184, Apr. 2017.

[68] F. A. Garba, K. I. Kunya, J. S. Yalli, Z. Kunya, and Z. Ahmad, "A proposed novel low cost genetic-fuzzy blockchain-enabled Internet of Things (IoT) forensics framework," *Sci. Practical Cyber Secur. J.*, vol. 5, no. 1, pp. 2587–4667, 2021.

[69] E. M. Dovom, A. Azmoodeh, A. Dehghantanha, D. E. Newton, R. M. Parizi, and H. Karimipour, "Fuzzy pattern tree for edge malware detection and categorization in IoT," *J. Syst. Archit.*, vol. 97, pp. 1–7, Aug. 2019.

[70] G. Chiesa, D. Di Vita, A. Ghadirzadeh, A. H. M. Herrera, and J. C. L. Rodriguez, "A fuzzy-logic IoT lighting and shading control system for smart buildings," *Autom. Construct.*, vol. 120, Dec. 2020, Art. no. 103397.

[71] S. Doostani, H. Barati, and A. Barati, "A lightweight hierarchical method for improving security in the Internet of Things using fuzzy logic," *Concurrency Comput., Pract. Exper.*, vol. 36, no. 6, Mar. 2024, Art. no. e7959.

[72] S. Nithya, K. Maithili, T. S. Kumar, S. Nethani, M. Sharath, K. G. Gupta, and G. Bhuvaneswari, "A fuzzy logic and cross-layered optimization for effective congestion control in wireless sensor networks to improve efficiency and performance," in *Proc. MATEC Web Conf.*, vol. 392, 2024, p. 01145.

[73] N. Khairova, N. Sharonova, D. Sytnikov, M. Hrebeniuk, and P. Sytnikova, "Recommendation system based on a compact hybrid user model using fuzzy logic algorithms," in *Proc. COLINS*, 2024, pp. 48–62.

[74] Y.-J. Tu and S. Piramuthu, "On addressing RFID/NFC-based relay attacks: An overview," *Decis. Support Syst.*, vol. 129, Feb. 2020, Art. no. 113194.

[75] P. Escobedo, M. Bhattacharjee, F. Nikbakhtnasrabadi, and R. Dahiya, "Smart bandage with wireless strain and temperature sensors and batteryless NFC tag," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 5093–5100, Mar. 2021.

[76] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on Internet of Things security: Requirements, challenges, and solutions," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100129.

[77] B. A. Alzahrani, K. Mahmood, and S. Kumari, "Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure," *IEEE Access*, vol. 8, pp. 76357–76367, 2020.

[78] M. Azrix, N. Walid, A. Zeki, and J. J. Yalli, "Developing a mobile navigation aid," in *Critical Socio-Technical Issues Surrounding Mobile Computing*. Hershey, PA, USA: IGI Global, 2016, pp. 124–136.

[79] X. Mu, J. Xu, Y. Liu, and L. Hanzo, "Reconfigurable intelligent surface-aided near-field communications for 6G: Opportunities and challenges," *IEEE Veh. Technol. Mag.*, vol. 19, no. 1, pp. 65–74, Mar. 2024.

[80] Y. Liu, C. Ouyang, Z. Wang, J. Xu, X. Mu, and A. L. Swindlehurst, "Near-field communications: A comprehensive survey," 2024, *arXiv:2401.05900*.

[81] H. Tran-Dang and D.-S. Kim, "The physical internet in the era of digital transformation: Perspectives and open issues," *IEEE Access*, vol. 9, pp. 164613–164631, 2021.

[82] C. E. Dridi, Z. Benzadri, and F. Belala, "System of systems modelling: Recent work review and a path forward," in *Proc. Int. Conf. Adv. Aspects Softw. Eng. (ICAASE)*, Nov. 2020, pp. 1–8.

[83] B. Dafflon, N. Moalla, and Y. Ouzrout, "The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review," *Int. J. Adv. Manuf. Technol.*, vol. 113, nos. 7–8, pp. 2395–2412, Apr. 2021.

[84] X. Wang, J. Yang, J. Han, W. Wang, and F.-Y. Wang, "Metaverses and DeMetaverses: From digital twins in CPS to parallel intelligence in CPSS," *IEEE Intell. Syst.*, vol. 37, no. 4, pp. 97–102, Jul. 2022.

[85] S. Kim, K.-J. Park, and C. Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 3, pp. 1534–1573, 3rd Quart., 2022.

[86] I. Mavromatis, Y. Jin, A. Stanoev, A. Portelli, I. Weeks, B. Holden, E. Glasspole, T. Farnham, A. Khan, U. Raza, A. Aijaz, T. Bierton, I. Seto, N. Patel, and M. Sooriyabandara, "UMBRELLA: A one-stop shop bridging the gap from lab to real-world IoT experimentation," *IEEE Access*, vol. 12, pp. 42181–42213, 2024.

[87] P. Li, I. Mavromatis, and A. Khan, "Past, present, future: A comprehensive exploration of AI use cases in the UMBRELLA IoT testbed," 2024, *arXiv:2401.13346*.

[88] V. Mygdalis, L. Carnevale, J. R. Martínez-De-Dios, D. Shutin, G. Aiello, M. Villari, and I. Pitas, "OTE: Optimal trustworthy EdgeAI solutions for smart cities," in *Proc. 22nd IEEE Int. Symp. Cluster, Cloud Internet Comput. (CCGrid)*, May 2022, pp. 842–850.

[89] A. Bröring, V. Kulkarni, A. Zirkler, P. Buschmann, K. Fysarakis, S. Mayer, B. Soret, L. D. Nguyen, P. Popovski, S. Samarakoon, M. Bennis, J. Härri, M. Rooker, G. Fritz, A. Bucur, G. Spanoudakis, and S. Ioannidis, "IntellIoT: Intelligent IoT environments," in *Global IoT Summit*. Cham, Switzerland: Springer, 2022, pp. 55–68.

[90] N. Quadar, M. Rahouti, M. Ayyash, S. K. Jagatheesaperumal, and A. Chehri, "IoT-AI/machine learning experimental testbeds: The missing piece," *IEEE Internet Things Mag.*, vol. 7, no. 1, pp. 136–143, Jan. 2024.

[91] G. Reus-Muns, D. Jaisinghani, K. Sankhe, and K. R. Chowdhury, "Trust in 5G open RANs through machine learning: RF fingerprinting on the POWDER PAWR platform," in *Proc. GLOBECOM IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[92] G. Miranda, D. F. Macedo, and J. M. Marquez-Barja, "Estimating video on demand QoE from network QoS through ICMP probes," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1890–1902, Jun. 2022.

[93] N. Y. Murad, M. H. Hasan, M. H. Azam, N. Yousuf, and J. S. Yalli, "Unraveling the black box: A review of explainable deep learning healthcare techniques," *IEEE Access*, vol. 12, pp. 66556–66568, 2024.

[94] M. Ghasemi, S. Kleisarchaki, T. Calmant, L. Gürgen, J. Ghaderi, Z. Kostic, and G. Zussman, "Real-time camera analytics for enhancing traffic intersection safety," in *Proc. 20th Annu. Int. Conf. Mobile Syst., Appl. Services*, Jun. 2022, pp. 630–631.

[95] K. I. Ahmed, M. Tahir, M. H. Habaebi, S. L. Lau, and A. Ahad, "Machine learning for authentication and authorization in IoT: Taxonomy, challenges and future research direction," *Sensors*, vol. 21, no. 15, p. 5122, Jul. 2021.

[96] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, "Artificial intelligence enabled Internet of Things: Network architecture and spectrum access," *IEEE Comput. Intell. Mag.*, vol. 15, no. 1, pp. 44–51, Feb. 2020.

[97] M. Usama, J. Qadir, A. Raza, H. Arif, K. A. Yau, Y. Elkhatib, A. Hussain, and A. Al-Fuqaha, "Unsupervised machine learning for networking: Techniques, applications and research challenges," *IEEE Access*, vol. 7, pp. 65579–65615, 2019.

[98] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, *A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science*. Cham, Switzerland: Springer, 2020, pp. 3–21.

[99] T. Bonny, M. Kashkash, and F. Ahmed, "An efficient deep reinforcement machine learning-based control reverse osmosis system for water desalination," *Desalination*, vol. 522, Jan. 2022, Art. no. 115443.

[100] A. Charmi and M. Yadollahzadeh-Tabari, "EGECC-MAES: Lightweight hybrid encryption algorithm in blockchain for smart health care in the Internet of Things platform," in *Proc. 20th CSI Int. Symp. Artif. Intell. Signal Process. (AISP)*, Feb. 2024, pp. 1–8.

[101] J. Zheng, C. Dike, S. Pancari, Y. Wang, G. C. Giakos, W. Elmannai, and B. Wei, "An in-depth review on blockchain simulators for IoT environments," *Future Internet*, vol. 14, no. 6, p. 182, Jun. 2022.

[102] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain, Res. Appl.*, vol. 3, no. 2, Jun. 2022, Art. no. 100067.

[103] T. R. Gadekallu, T. Huynh-The, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. Benevides da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," 2022, *arXiv:2203.09738*.

[104] K. A. Demir, "Smart education framework," *Smart Learn. Environments*, vol. 8, no. 1, pp. 1–36, Dec. 2021.

[105] V. L. Uskov, J. P. Bakken, K. Gayke, D. Jose, M. F. Uskova, and S. S. Devaguptapu, "Smart university: A validation of 'smartness features-main components' matrix by real-world examples and best practices from universities worldwide," in *Smart Education and e-Learning*. Cham, Switzerland: Springer, 2019, pp. 3–17.

[106] B. Alomar and A. Alazzam, "A smart irrigation system using IoT and fuzzy logic controller," in *Proc. 5th HCT Inf. Technol. Trends (ITT)*, Nov. 2018, pp. 175–179.

[107] S. P. Chatrati, G. Hossain, A. Goyal, A. Bhan, S. Bhattacharya, D. Gaurav, and S. M. Tiwari, "Smart home health monitoring system for predicting type 2 diabetes and hypertension," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 3, pp. 862–870, Mar. 2022.

[108] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, "An overview of security and privacy in smart cities' IoT communications," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 3, Mar. 2022, Art. no. e3677.

[109] T. M. Tan and S. Saraniemi, "Trust in blockchain-enabled exchanges: Future directions in blockchain marketing," *J. Acad. Marketing Sci.*, vol. 51, no. 4, pp. 914–939, Jul. 2023.

[110] R. Peres, M. Schreier, D. A. Schweidel, and A. Sorescu, "Blockchain meets marketing: Opportunities, threats, and avenues for future research," *Int. J. Res. Marketing*, vol. 40, no. 1, pp. 1–11, Mar. 2023.

[111] R. Chaganti, B. Bhushan, and V. Ravi, "A survey on blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions," *Comput. Commun.*, vol. 197, pp. 96–112, Jan. 2023.

[112] J. Hayes, A. Aneiba, and M. Gaber, "SymbIoT: Towards an extensible blockchain integration testbed for IIoT," in *Proc. 1st Workshop Enhanced Netw. Techn. Technol. Ind. IoT Cloud Continuum*, Sep. 2023, pp. 8–14.

[113] M. Symeonides, Z. Georgiou, D. Trihinas, G. Pallis, and M. D. Dikaiakos, "Fogify: A fog computing emulation framework," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Nov. 2020, pp. 42–54.

[114] J. Hasenburg, M. Grambow, and D. Bermbach, "MockFog 2.0: Automated execution of fog application experiments in the cloud," *IEEE Trans. Cloud Comput.*, vol. 11, no. 1, pp. 58–70, Jan. 2023.

[115] U. K. Dayalan, R. A. K. Fezeu, T. J. Salo, and Z.-L. Zhang, "Kaala: Scalable, end-to-end, IoT system simulator," in *Proc. ACM SIGCOMM Workshop Netw. Sens. Syst. Sustain. Soc.*, Aug. 2022, pp. 33–38.

[116] M. Salama, Y. Elkhatib, and G. Blair, "IoTNetSim: A modelling and simulation platform for end-to-end IoT services and networking," in *Proc. 12th IEEE/ACM Int. Conf. Utility Cloud Comput.*, Dec. 2019, pp. 251–261.

[117] H. Baniata and A. Kertesz, "Fobsim: An extensible open-source simulation tool for integrated fog-blockchain systems," *PeerJ Comput. Sci.*, vol. 7, Jan. 2021, Art. no. e431.

[118] S. Thapliyal, S. Singh, M. Wazid, D. P. Singh, and A. K. Das, "Design of blockchain-enabled secure smart health monitoring system and its testbed implementation," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100020.

[119] G. Mahalaxmi, R. Varaprasad, and T. A. S. Srinivas, "Blockchain solutions for IoT devices against DDoS attacks: A review," *IUP J. Inf. Technol.*, vol. 18, no. 4, pp. 25–46, 2022.

[120] A. Srivastava, S. Gupta, M. Quamara, P. Chaudhary, and V. J. Aski, "Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects," *Int. J. Commun. Syst.*, vol. 33, no. 12, Aug. 2020, Art. no. e4443.

[121] A. Akinbi, Á. MacDermott, and A. M. Ismael, "A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models," *Forensic Sci. Int., Digit. Invest.*, vols. 42–43, Oct. 2022, Art. no. 301470.

[122] A. Altaf, F. Iqbal, R. Latif, B. M. Yakubu, S. Latif, and H. Samiullah, "A survey of blockchain technology: Architecture, applied domains, platforms, and security threats," *Social Sci. Comput. Rev.*, vol. 41, no. 5, pp. 1941–1962, Oct. 2023.

[123] M. Mirlashari and S. A. M. Rizvi, "Open challenges of communication security in an IoT environment—A survey," in *IoT With Smart Systems*, vol. 2. Cham, Switzerland: Springer, 2022, pp. 107–116.

[124] A. G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging trends in blockchain technology and applications: A review and outlook," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6719–6742, Oct. 2022.

[125] A. Abdelmaboud, A. I. A. Ahmed, M. Abaker, T. A. E. Eisa, H. Albasheer, S. A. Ghorashi, and F. K. Karim, "Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions," *Electronics*, vol. 11, no. 4, p. 630, Feb. 2022.

[126] L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021.

[127] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, challenges, and future directions," *Int. J. Intell. Syst. Appl.*, vol. 10, no. 6, pp. 40–48, Jun. 2018.

[128] A. Banafa, "IoT and blockchain convergence: Benefits and challenges," *IEEE IoT Newslett.*, vol. 10, Jan. 2017. [Online]. Available: https://iot.ieee.org/newsletter/january-2017.html

[129] W. Liang and N. Ji, "Privacy challenges of IoT-based blockchain: A systematic review," *Cluster Comput.*, vol. 25, no. 3, pp. 2203–2221, Jun. 2022.

[130] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, vol. 10, pp. 96538–96555, 2022.

[131] J. S. Yalli and M. H. Hasan, "A unique PUF authentication protocol based fuzzy logic categorization for Internet of Things (IoT) devices," in *Proc. 12th Int. Conf. Softw. Comput. Appl.*, Feb. 2023, pp. 246–252.

[132] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[133] F. Amsaad, A. Razaque, M. Baza, S. Kose, S. Bhatia, and G. Srivastava, "An efficient and reliable lightweight PUF for IoT-based applications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Jun. 2021, pp. 1–6.

[134] A. Al-Meer and S. Al-Kuwari, "Physical unclonable functions (PUF) for IoT devices," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–31, Dec. 2023.

[135] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K. R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8205–8228, Jun. 2022.

[136] E. P. Kumar and S. Priyanka, "A password less authentication protocol for multi-server environment using physical unclonable function," *J. Supercomput.*, vol. 79, no. 18, pp. 21474–21506, Dec. 2023.

[137] V. R. Vijaykumar, S. R. Sekar, R. Jothin, V. C. Diniesh, S. Elango, and S. Ramakrishnan, "Novel light weight hardware authentication protocol for resource constrained IoT based devices," *IEEE J. Radio Freq. Identificat.*, vol. 8, pp. 31–42, 2024.

[138] V. Kohli, M. N. Aman, and B. Sikdar, "An intelligent fingerprinting technique for low-power embedded IoT devices," *IEEE Trans. Artif. Intell.*, early access, Apr. 10, 2024, doi: 10.1109/TAI.2024.3386498.

[139] J. Preskill, "Quantum computing 40 years later," in *Feynman Lectures on Computation*. Boca Raton, FL, USA: CRC Press, 2023, pp. 193–244.

[140] Z. Yang, M. Zolanvari, and R. Jain, "A survey of important issues in quantum computing and communications," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1059–1094, 2nd Quart., 2023.

[141] R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, and Z. Anwar, "Quantum computing for healthcare: A review," *Future Internet*, vol. 15, no. 3, p. 94, Feb. 2023.

[142] T. Lubinski, S. Johri, P. Varosy, J. Coleman, L. Zhao, J. Necaise, C. H. Baldwin, K. Mayer, and T. Proctor, "Application-oriented performance benchmarks for quantum computing," *IEEE Trans. Quantum Eng.*, vol. 4, pp. 1–32, 2023.

[143] B. Blakely, J. Chung, A. Poczatek, R. Syed, and R. Kettimuthu, "Toward a quantum information system cybersecurity taxonomy and testbed: Exploiting a unique opportunity for early impact," 2024, *arXiv:2404.12465*.

[144] J. Chung, E. M. Eastman, G. S. Kanter, K. Kapoor, N. Lauk, C. H. Pena, R. K. Plunkett, N. Sinclair, J. M. Thomas, R. Valivarthi, S. Xie, R. Kettimuthu, P. Kumar, P. Spentzouris, and M. Spiropulu, "Design and implementation of the Illinois express quantum metropolitan area network," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–20, 2022.

[145] H.-H. Lu, E. M. Simmerman, P. Lougovski, A. M. Weiner, and J. M. Lukens, "Fully arbitrary control of frequency-bin qubits," *Phys. Rev. Lett.*, vol. 125, no. 12, Sep. 2020, Art. no. 120503.

[146] D. Earl, K. Karunaratne, J. Schaake, R. Strum, P. Swingle, and R. Wilson, "Architecture of a first-generation commercial quantum network," 2022, *arXiv:2211.14871*.

[147] B. Halak, T. Gibson, M. Henley, C.-B. Botea, B. Heath, and S. Khan, "Evaluation of performance, energy, and computation costs of quantum-attack resilient encryption algorithms for embedded devices," *IEEE Access*, vol. 12, pp. 8791–8805, 2024.

[148] F. A. Almalki, S. H. Alsamhi, R. Sahal, J. Hassan, A. Hawbani, N. S. Rajput, A. Saif, J. Morgan, and J. Breslin, "Green IoT for eco-friendly and sustainable smart cities: Future directions and opportunities," *Mobile Netw. Appl.*, vol. 28, no. 1, pp. 178–202, Feb. 2023.

[149] P. Mittal, J. Agrawal, R. Chauhan, and S. Devliyal, "A study on the systematic review of green IoT," in *Proc. Int. Conf. Autom. Comput. (AUTOCOM)*, Mar. 2024, pp. 623–630.

[150] N. Hu, Z. Tian, X. Du, N. Guizani, and Z. Zhu, "Deep-green: A dispersed energy-efficiency computing paradigm for green industrial IoT," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 2, pp. 750–764, Jun. 2021.

[151] J. B. Awotunde, S. N. Sur, R. G. Jimoh, D. R. Aremu, D.-T. Do, and B. M. Lee, "FL_GIoT: Federated learning enabled edge-based green Internet of Things system: A comprehensive survey," *IEEE Access*, vol. 11, pp. 136150–136165, 2023.

[152] M. A. Albreem, A. M. Sheikh, M. J. K. Bashir, and A. A. El-Saleh, "Towards green Internet of Things (IoT) for a sustainable future in Gulf cooperation council countries: Current practices, challenges and future prospective," *Wireless Netw.*, vol. 29, no. 2, pp. 539–567, Feb. 2023.

[153] M. B. Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[154] J. S. Yalli, M. H. Hasan, and N. S. Haron, "A convenient user three authentication levels for Internet of Things (IoT) devices," in *Proc. IEEE 11th Conf. Syst., Process Control (ICSPC)*, Dec. 2023, pp. 288–293.

[155] M. Asif, T. A. Khan, N. Taleb, R. A. Said, S. Y. Siddiqui, and G. Batool, "A proposed architecture for traffic monitoring & control system via LiFi technology in smart homes," in *Proc. Int. Conf. Bus. Anal. Technol. Secur. (ICBATS)*, Feb. 2022, pp. 1–3.

[156] T. Kern, P. Dossow, and E. Morlock, "Revenue opportunities by integrating combined vehicle-to-home and vehicle-to-grid applications in smart homes," *Appl. Energy*, vol. 307, Feb. 2022, Art. no. 118187.

[157] V. O. Nyangaresi, "A formally validated authentication algorithm for secure message forwarding in smart home networks," *Social Netw. Comput. Sci.*, vol. 3, no. 5, p. 364, Jul. 2022.

[158] H. T. S. Alrikabi and N. Ali Jasim, "Design and implementation of smart city applications based on the Internet of Things," *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 15, no. 13, p. 4, Jul. 2021.

[159] M. L. Tuballa and M. L. Abundo, "A review of the development of smart grid technologies," *Renew. Sustain. Energy Rev.*, vol. 59, pp. 710–725, Jun. 2016.

[160] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. M. Y. M. Ghias, L. H. Koh, and L. Yang, "Blockchain for future smart grid: A comprehensive survey," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 18–43, Jan. 2021.

[161] M. A. Judge, A. Khan, A. Manzoor, and H. A. Khattak, "Overview of smart grid implementation: Frameworks, impact, performance and challenges," *J. Energy Storage*, vol. 49, May 2022, Art. no. 104056.

[162] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4862–4872, Nov. 2022.

[163] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *J. Netw. Comput. Appl.*, vol. 209, Jan. 2023, Art. no. 103540.

[164] M. Safkhani, N. Bagheri, S. Ali, M. H. Malik, O. H. Ahmed, M. Hosseinzadeh, and A. H. Mosavi, "Improvement and cryptanalysis of a physically unclonable functions based authentication scheme for smart grids," *Mathematics*, vol. 11, no. 1, p. 48, Dec. 2022.

[165] J. Wang, M. K. Lim, Y. Zhan, and X. Wang, "An intelligent logistics service system for enhancing dispatching operations in an IoT environment," *Transp. Res. E, Logistics Transp. Rev.*, vol. 135, Mar. 2020, Art. no. 101886.

[166] A. Patel and T. A. Champaneria, "Fuzzy logic based algorithm for context awareness in IoT for smart home environment," in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2016, pp. 1057–1060.

[167] A. Kirimtat, O. Krejcar, A. Kertesz, and M. F. Tasgetiren, "Future trends and current state of smart city concepts: A survey," *IEEE Access*, vol. 8, pp. 86448–86467, 2020.

[168] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, "A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes," *IEEE Access*, vol. 8, pp. 118433–118471, 2020.

[169] H. Zhu, K.-V. Yuen, L. Mihaylova, and H. Leung, "Overview of environment perception for intelligent vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2584–2601, Oct. 2017.

[170] Z. Md. Fadlullah, F. Tang, B. Mao, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "State-of-the-art deep learning: Evolving machine intelligence toward Tomorrow's intelligent network traffic control systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2432–2455, 4th Quart., 2017.

[171] C. D. Ha, P. T. Minh, T. Van Tien, P. P. Thu, and P. M. Trien, "IoT solutions for smart farming: A comprehensive review on the current trends, challenges and future prospects for sustainable agriculture," *J. Forestry Sci. Technol.*, vol. 8, no. 2, pp. 28–35, 2023.

[172] R. Khalid, O. Samuel, N. Javaid, A. Aldegheishem, M. Shafiq, and N. Alrajeh, "A secure trust method for multi-agent system in smart grids using blockchain," *IEEE Access*, vol. 9, pp. 59848–59859, 2021.

[173] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6206–6221, Jul. 2022.

[174] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[175] V. Terzieva, S. Ilchev, and K. Todorova, "The role of Internet of Things in smart education," *IFAC-PapersOnLine*, vol. 55, no. 11, pp. 108–113, 2022.

[176] J. S. Yalli, S. A. Latif, M. H. Masud, M. K. Alam, and A. H. Abdallah, "A comprehensive analysis of improving QoS and IMM traffic of high speed wireless campus network," in *Proc. IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2014, pp. 12–17.

[177] N. T. Shamsuddin, N. I. A. Aziz, Z. C. Cob, N. L. A. Ghani, and S. M. Drus, "Big data analytics framework for smart universities implementa- tions," in *Proc. 3rd Int. Symp. Inf. Internet Technol. (SYMINTECH)*, M. A. Othman, M. Z. A. A. Aziz, M. S. M. Saat, and M. H. Misran, Eds., Cham, Switzerland: Springer, 2019, pp. 53–62.

[178] M. Mircea, M. Stoica, and B. Ghilic-Micu, "Investigating the impact of the Internet of Things in higher education environment," *IEEE Access*, vol. 9, pp. 33396–33409, 2021.

[179] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E. M. Aggoune, "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk," *IEEE Access*, vol. 7, pp. 129551–129583, 2019.

[180] A. Khattab, A. Abdelgawad, and K. Yelmarthi, "Design and implementation of a cloud-based IoT scheme for precision agriculture," in *Proc. 28th Int. Conf. Microelectron. (ICM)*, Dec. 2016, pp. 201–204.

[181] R. Rayhana, G. Xiao, and Z. Liu, "Internet of Things empowered smart greenhouse farming," *IEEE J. Radio Freq. Identificat.*, vol. 4, no. 3, pp. 195–211, Sep. 2020.

[182] P. Srinivasulu, M. S. Babu, R. Venkat, and K. Rajesh, "Cloud service oriented architecture (CSoA) for agriculture through Internet of Things (IoT) and big data," in *Proc. IEEE Int. Conf. Electr., Instrum. Commun. Eng. (ICEICE)*, Apr. 2017, pp. 1–6.

[183] M. S. Farooq, R. Javid, S. Riaz, and Z. Atal, "IoT based smart greenhouse framework and control strategies for sustainable agriculture," *IEEE Access*, vol. 10, pp. 99394–99420, 2022.

[184] T.-C. Hsu, H. Yang, Y.-C. Chung, and C.-H. Hsu, "A creative IoT agriculture platform for cloud fog computing," *Sustain. Comput., Informat. Syst.*, vol. 28, Dec. 2020, Art. no. 100285.

[185] A. Abdullah, S. Al Enazi, and I. Damaj, "AgriSys: A smart and ubiquitous controlled-environment agriculture system," in *Proc. 3rd MEC Int. Conf. Big Data Smart City (ICBDSC)*, Mar. 2016, pp. 1–6.

JAMEEL SHEHU YALLI (Member, IEEE) received the bachelor's degree in computer science from Al-Qalam University Katsina, Nigeria, in 2010, and the M.Sc. degree in computer and information engineering from International Islamic University Malaysia, in 2015. He is currently pursuing the Ph.D. degree with Universiti Teknologi PETRONAS (UTP), Malaysia.

From 2015 to 2020, he worked in the industry and later joined the academics as an Assistant Lecturer and a Research Assistant with the Department of Computer Science, Federal University Gusau, Nigeria. He has published a few articles and co-authored many. His research interests include the Internet of Things (IoT), security, authentication models, cybercrime, cyber-security, cyber and Islam, wireless communication, and wireless networks.

Mr. Jameel has been a member of the IEEE Computer Society and IEEE Communications Society Malaysia Chapter, since 2015. He is also a member of the International Association of Engineers and a few other local and international memberships.

MOHD HILMI HASAN (Member, IEEE) received the degree in information technology from Universiti Teknologi PETRONAS (UTP), Malaysia, the master's degree in information technology from The Australian National University, Australia, and the Ph.D. degree in information technology from UTP.

Driven by a commitment to innovation, his expertise spans data science, big data analytics, wireless networks, wireless communications, artificial intelligence, machine learning, and fuzzy logic. With numerous publications in reputable journals and conferences, he continues to make significant strides in advancing the frontiers of data and IT. Currently, he contributes to the scientific community through research and mentorship. He is the Chair of the Department of Computer and Information Sciences and an active member of the Centre for Research in Data Science (CeRDaS), UTP. As an Associate Professor, he gathered much experience in teaching, learning, research, supervision, administration, and collaboration.

Dr. Hasan is a member of Malaysia Board of Technologists and is a reviewer of many local and international journals and conferences.

AISHA ABUBAKAR BADAWI received the B.Sc. degree in political science from Bayero University Kano, Nigeria, in 2002, the M.A. degree in strategy and international security from Hull University, U.K., in 2006, and the M.Sc. degree in information security from the University of Derby, U.K., in 2013. She is currently a part-time Lecturer with the School for Computer Science and Informatics, De Montfort University, U.K. She is engaged in teaching, learning, research, and supervision and has a strong passion for community service in the areas of special educational needs and disabilities (SEND) within young learners. Her research interests include but are not limited to cybercrime, cyber security, computer ethics, and also special needs education.