Wireless Personal Communications (2022) 122:1481–1517
https://doi.org/10.1007/s11277-021-08958-3

IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey

Aparna Raj[1] · **Sujala D. Shetty**[1]

Accepted: 9 August 2021 / Published online: 18 August 2021

Abstract
Today almost every person's life revolves around internet and Internet of Things (IoT). IoT is a paradigm which interconnects devices, people, or networks with the ability to process and respond to any physical or virtual communication without a glitch. It is contemplated to be the next era of communication and made devices smarter and more efficient. IoT hits every application area from home controllers and healthcare to agriculture. It utilizes internet connectivity, sensors and numerous other technologies and protocols for data collection and analysis and delivers user required services effectively. In this paper, a detailed review on various architectures, technologies and protocols used in an IoT eco-system is presented. We have also discussed possible layer wise attacks and how new technologies, fog, edge, cloud, artificial intelligence, machine learning and blockchain could be integrated to existing IoT architecture to deliver flawless services and better security. A summary of current research challenges and future directions in this area is also discussed.

Keywords IoT architecture · Cloud computing · Machine learning · Blockchain · Edge computing · IoT security

1 Introduction

Science and Technology added new dimensions to human lives. With the advent of smart devices having capability to communicate with humans as well as with other devices automatically over the internet made our lives even smarter. This constitute the Internet of Things (IoT) which ushered a new epoch where a wide variety of devices or appliances are interconnected and shares information across the web. IoT is an umbrella term that covers technologies, design principles and systems with the ever-growing phenomenon of Internet connected devices—'Things', that extends internet connectivity into physical devices. 'Things' in the context of IoT could be any entity or physical object that has a Unique Id, Embedded System and the ability to transfer data over a network [1]. According to recent

✉ Aparna Raj
p20190003@dubai.bits-pilani.ac.in

Sujala D. Shetty
sujala@dubai.bits-pilani.ac.in

[1] Department of Computer Science, Bits-Pilani, Dubai Campus, Dubai, UAE

CISCO estimation, nearly two-thirds of worldwide population will have internet access and about 14.7 billion connected devices are expected by 2023. Figure 1 represents this estimated value of connected IoT devices by 2023. More than one third of companies use various IoT solutions to optimize processes, improve data collections, for cutting operational costs and for building new revenue streams. IoT is currently in its golden age. Smart City, Industrial Internet of Things (IIoT), Smart Home, Smart Vehicles and Healthcare are some of the major sectors that are likely to meet colossal transformation by 2022.

The term IoT was coined by Kevin Ashton in 1999, while working in Procter & Gamble for developing network of objects using RFID. Then it took 10 more years for the concept to gain some popularity. But today we are living in a world where the number of connected devices exceeds the number of humans, and these devices range from smart wearables to smart homes and even smart cities. In future, the devices are expected to directly communicate with each other over the web [2]. Apart from this there is an emerging paradigm called SIoT, in which different IoT devices interacts and create connections among themselves for achieving common goals. It allows the objects to have their own social networks and enables humans to access the outcome of these automated inter-object interactions, in order to maintain their privacy [3].

Along with the enormous growth and popularity of IoT, there are several challenges to be tackled during its implementation. As an IoT network consists of many heterogeneous devices, compatibility is one of the major issues faced by these devices. Even though there are many reference models, it lacks a single unified architecture for its implementation. Security and Privacy of users are other major challenges faced by the IoT devices. Since most of the devices connects and exchanges data over the internet, there is a huge risk of leakage of personal information plus a single loophole places the entire system down. Hence proper authentication mechanisms, security of the devices and the communication channels should be maintained. Additionally, since IoT devices are power hungry, different energy efficient aspects should also be incorporated during its design stage.

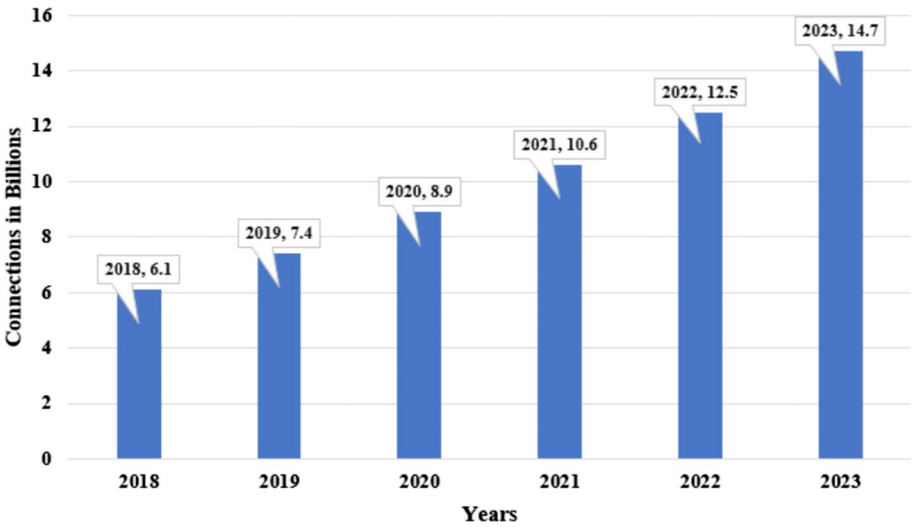

Fig. 1 CISCO's estimation of connected devices from 2018 to 2023

There are several survey papers that encompasses different aspects of IoT technology. In [2] authors have summarized various security challenges and its solution architectures. In [4] authors have proposed various layer wise architecture, security attacks and countermeasures for providing security in IoT. In [5] authors have given a detailed review on various IoT architectures, protocols and applications used. In [6] authors have provided an overview of existing IoT technical details, applications and latest emerging areas. In [7] authors have provided an in-depth survey on IoT, big data analytics and key technologies and challenges. In [8] authors have surveyed various protocols and standards used in IoT. In [9] authors have discussed how IoT revolutionized human life and what are the future technological enhancements required. In [10] a detailed survey on architectures and technologies used are discussed. The outline of the contribution of this paper are:

- Presented a detailed review on different layered architectures, enabling technologies and layer wise description of protocols used.
- Listed out possible security attacks in each layer.
- Listed security solutions that can be provided using recent technologies such as Artificial Intelligence, Machine Learning and Blockchain.
- Advantages and disadvantages on integrating IoT with cloud, fog, and edge.
- An assessment on existing challenges and future research directions.

The rest of the article is organized as follows: Sect. 2 describes the basic components of an IoT eco-system. Section 3 discusses various layered architecture of IoT depending on the applications. In Sect. 4, 5, and 6 various technologies, hardware & software platforms and layer wise descriptions of various protocols used are reviewed. Major advancing computing platforms, i.e., Artificial Intelligence, Machine Learning, Blockchain, Cloud Computing, Fog Computing, Edge Computing, and its integration with IoT and their advantages and disadvantages and various IoT applications are presented in Sect. 7, 8, and 9, respectively. Section 10 describes current challenges and future research opportunities in this area. Finally, Sect. 11 concludes the paper (Table 1).

2 Components of IoT

Fundamental components of an IoT eco-system are as follows:

- Sensors and Actuators: These are the devices that enables interaction with the physical world. They collect data from the surrounding environment and deliver it to the data processing unit. Some of the commonly used sensors are Temperature sensors, Pressure sensors, Light sensors, Ultrasonic sensors etc. Sensors are chosen accordingly as per the needs of various applications.
- Connectivity/Gateways: Data collected by the above devices are sent to a cloud infrastructure for storage and processing. For this the devices make use of different technologies such as Bluetooth, Zigbee, Wi-Fi, Z-Wave, Cellular Networks, NFC, Lora WAN etc. and different protocols such as MQTT, AMQP, DDS, CoAP etc.
- Data Processing: Once the collected data gets into the cloud, cloud analytic software processes the data using various tools and techniques and converts it into useful insights. Later it sends the necessary information to the users as required.

Table 1 List of acronyms

3G	Third generation
AI	Artificial intelligence
AMQP	Advanced message queuing protocol
ARPANET	Advanced research projects agency network
BC	Block chain
CC	Cloud computing
CoAP	Constrained application protocol
CPS	Cyber physical systems
CPU	Central processing unit
DDS	Data distribution service
DNS	Domain name system
DoS	Denial of service
EC	Edge computing
FC	Fog computing
ID	Identification
IDS	Intrusion detection system
IEEE	Institute of electrical and electronics engineers
IETF	Internet engineering task force
IIoT	Industrial internet of things
IoT	Internet of things
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IT	Information technology
LoRa	Long range
LPWAN	Low power wide area network
LR-WPAN	Low rate wireless personal area networks
LTE	Long term evolution
MAN	Metropolitan area network
ML	Machine learning
MQTT	Message queuing telemetry transport
NFC	Near-field communication
OT	Operational technology
QoS	Quality of service
REST	Representational state transfer
RFID	Radio frequency identification
SAS	System architecture specifications
SIoT	Social internet of things
TSMP	Time synchronized mesh protocol
VoIP	Voice over internet protocol
Wi-Fi	Wireless fidelity
WiMAX	Worldwide interoperability for microwave access
WSN	Wireless sensor networks
XML	Extensible markup language

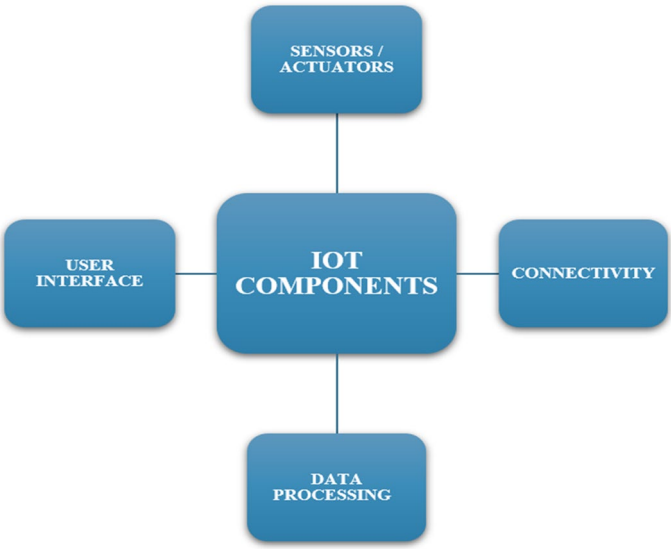

Fig. 2 Basic components of an IoT eco-system

- User Interface: This information is made available to the end user in different ways such as triggering alarms or notification through texts or emails. Figure 2 represents these basic elements.

Some of the features of IoT are its seamless connectivity using different technologies and protocols, assignation of cross-platform technologies and services using CC/BC, providing scalable infrastructure as per user requirements, ability to change the state dynamically according to data usage, device intelligence, and integration of various cross-domain platforms. Some real-world use cases of IoT devices are Amazon Echo, Nest Thermostat, Smart Light, Security systems, Asset Monitoring, Smart Wearables etc.

3 IoT Architecture

IoT does not have a universally agreed single unified architecture. Researchers have proposed various architecture based on the needs of different users and organizations.

3.1 Three Tier Architecture

This is a simplistic architecture that meets the basic demands of IoT devices [4]. It has 3 layers as shown in Fig. 3.

- Perception Layer: This is the lowest layer which recognizes the physical properties of IoT devices. It is also known as the sensor layer. It captures data from the surrounding environment with the help of different sensors and actuators. Later it gathers and

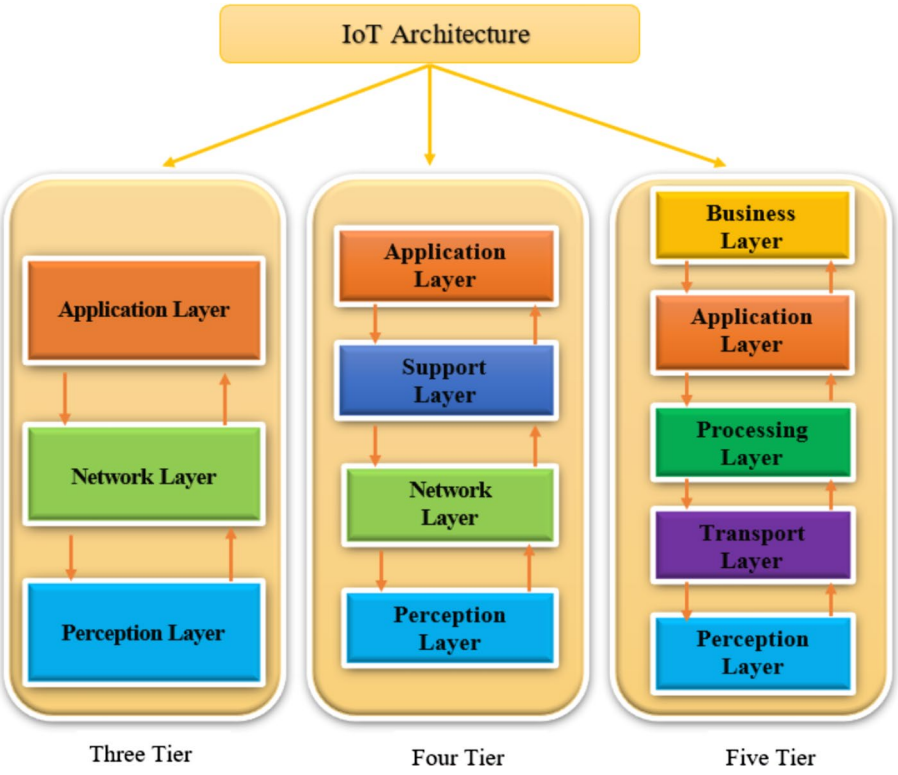

Fig. 3 Three, four, and five tier IoT architecture

process these data and forwards it to the network layer. In case of local and short-range networks, it also deals with IoT node collaborations [11].

- Network Layer: It acts as a bridge between the perception layer and network layer. It routes the data captured by previous layer to different devices, hubs or servers over the internet using any medium for transmission i.e., wired or wireless [5]. This layer includes routing devices, gateways, switches, different cloud computing platforms etc.
- Application Layer: This layer delivers the application specific services to the end user, which guarantees the confidentiality, integrity, and authenticity of the data.

3.2 Four Tier Architecture

Due to the continuous developments in IoT, three tier architecture could not meet the growing demands of various IoT devices. Moreover, as the data is transmitted directly between these layers, it increased the chances of security flaws in the system [12]. Hence researchers proposed a four-tier architecture with an added layer called support layer. The other three layers works similarly as described in three-tier architecture. The functionality of this new layer is as given below.

- Support Layer: It deals with the authenticity of the users and confirms whether the intended users are sending the data using pre-shared keys or passwords. Once the user's

identity is proved, it sends the data to the network layer. This layer is also called as data processing layer. It acts as a software middleware layer between the hardware and IoT applications and supports end-end secured data exchanges, authentication, synchronization, authorization, device management etc.

3.3 Five Tier Architecture

To obtain more finer aspects of IoT and to overcome the security and storage issues that prevailed in the previous architecture, researchers proposed a five-tier architecture. The functionalities of perception layer and application layer remains the same as the previous ones with an addition of 3 more layers as follows.

- Transport Layer: It transfers the sensor data to the processing layer and vice-versa.
- Processing Layer: This layer is also known as the middleware layer. It collects data from the transport layer and stores the data. Later it analyses and processes the data and extracts the needed information and delivers it to the application layer. Therefore, this layer eliminates the transfer of unwanted data thereby improving the performance of the IoT devices.
- Business Layer: This layer manages and controls the whole IoT system including applications, businesses, profit models and deals with users' privacy.

In addition to these three models, several additional reference architectures for IoT are available from various IoT-focused consortia and standard organizations [13]. Following are some of the prominent approaches for providing smart and secure IoT 2021 platforms.

In [14] authors have proposed a three-tier industrial architecture having edge, platform and enterprise layers connected by proximity, access, and service networks. Edge layer makes use of proximity network to collect data from edge devices. Later it forwards the data to the platform layer which processes the data and delivers to the enterprise layer which deals with end user interactions, control commands and domain specific applications.

Cisco [15] follows a seven-layer IoT reference architecture. Layer one consists of the physical devices and device controllers for sending and receiving information, analog to digital conversion, generating data and controlling devices. Layer two is the connectivity layer which deals with reliable and timely information delivery across devices and networks, routing and switching, implementation of various protocols and translations, network analytics and security. Layer three is the fog/edge computing layer which performs data aggregation, filtering, and cleanup, packet analysis and works on network and data level analytics. Layer four is the data accumulation layer which reduces data through filtering and provides persistent storage of data. Next is the data abstraction layer which creates schemas and views of data as needed by various applications by combining, filtering and reformatting data according to the client applications. Then the application layer where the information interpretation occurs and deals with controlling applications, reporting, and generating business intelligence analytics. Final layer is the collaboration and process layer which deals with people and business process that transcends multiple applications. Recently Cisco has introduced an IoT security architecture that delivers enhanced visibility across various IoT and operational technology platforms.

IBM IoT architecture [16] deals with middleware along with added revisions on device handling and management which includes four key components. The connect component

provides device management and ensures the security of device-network connectivity. Information management component deals with metadata management, streaming, parsing, storing, and archiving data. Analytic component provides analytical functionality including text, social data and machine data analytics and can even handle big data. Lastly the risk management component that performs auditing, data protection, risk management and device integrity.

Intel works with its ecosystem partners SAS [17] for connecting devices across the cloud. Intel SAS is having two versions, 1.0 and 2.0. Intel SAS version 1.0 helps the developers and system integrators to securely connect and manage legacy devices that are built without any internet connectivity or intelligence. Intel SAS version 2.0 supports the integration of wide range of smart and connected devices with built in intelligence and connectivity, thus providing them with security, manageability, and integration capabilities. It also facilitates the convergence of OT and IT for CPS and makes it easier to handle larger networks with disparate hardware and software resources.

Another kind is the Lambda architecture [18], which can easily handle massive volumes of data generated by the sensor devices. It handles the real time big data by integrating batch and stream data processing and makes it available for downstream analysis. It consists of three layers batch layer, speed layer and the serving layer. Batch layer consists of immutable, append only data set of records. When a new data arrives, it gets appended to the master data set and the results of batch layer, called batch views are stored persistently. Secondly the speed layer that generates up-to-date real-time views and process the data that are overlooked by the batch layer. Finally, the speed layer combines and stores the data from both batch and speed layers and builds views from the processed data.

4 IoT Technologies

Several long-range and short-range communication technologies are used for enabling the networking functionalities as required by the IoT eco-system [6]. Some of the commonly used as well as some of the emerging IoT technologies are described below.

4.1 RFID

RFID belongs to a group of technologies called Automatic Identification and Data Capture (AIDC) which automatically identifies and collects data from objects and enters it into pcs without human intervention. It is the most popular technology used for numerous IoT applications. RFID stores and retrieves data using radio waves and consists of an RFID tag with a microchip and an antenna for storing ids and exchange data with readers, antenna for detecting tags, reader for exchanging data with the tags in its proximity, and a back-end database server for storing and analyzing the mapping between the tag and the object [19]. There are three types of RFID tags based on the power supply provisioning. Active tags are battery operated and periodically transmit signals and supports longer range transmissions and hence used in asset tracking. Semi-Passive tags contain a battery, but they do not periodically transmit signals as active tags. Battery is used merely to turn the tag on whenever it receives a signal and to reflect the reader's signal back and suited for environmental monitoring applications. Passive tags remain dormant until it receives a signal from the reader ad the electromagnetic energy from the reader powers up the tags. These are used in supply chain management, access control, IoT devices etc. Some use cases of RFID are in ambient

assisted environments to detect elderly people interactions to keep them active longer and to help impaired shoppers to gain assistance about products through headsets [20].

4.2 WSN

These are the key enablers of IoT paradigm, and they comprise large number of self-configured sensor nodes with varying topologies. They consume very little power and mostly are battery or solar power operated. These nodes communicate with each other using radio frequencies and are used to monitor different environmental conditions such as temperature, pressure, motions, pollutants etc. and transmits these data to a base station where the data is collected and analyzed [21]. Nodes in a WSN have limited storage capacity, processing speed, bandwidth and they can be equipped with actuators. Some applications of WSN are Military applications, Environmental monitoring, Healthcare applications, Transportation etc.

4.3 Zigbee

It is a wireless networking protocol used for devices requiring longer battery life and lower data rates like Bluetooth technology. It is commonly used for industrial settings, automation systems, medical devices, and remote-control applications. It operates on IEEE 802.15.4 specification and provides higher security, robustness and is of lower cost. It uses the same wireless band as Bluetooth and Wi-Fi i.e. 2.4 GHz and built as a mesh network which allows the devices to communicate with each other and repeat commands [22].

4.4 Z-Wave

It is a wireless technology used by smart devices to communicate with each other and uses low energy radio waves for device interactions. Most of the home automation and security manufactures offer Z-wave compatible products. It is held and maintained by a private organization. Some of the advantages are, it provides better signal strength than Bluetooth as it has its own dedicated frequency, lower network interference compared to Wi-Fi, also interoperable and higher security [23].

4.5 Bluetooth

It is a short-range wireless communication technology for exchanging data between fixed and mobile devices. It provides lower cost solutions for communication by creating an ad-hoc mobile personal area network supporting continuous streaming data applications. It is best suited for computing and consumer products. In contrast to classic Bluetooth, Bluetooth 4.0 called Bluetooth Low Energy was introduced in 2010 with an add on feature of ultra-low power consumption compared to the former making it suitable for IoT devices and supports multi stream audios [24].

4.6 Wi-Fi

It is one of the most popular wireless communication technologies that uses radio waves for delivering wireless high-speed internet and network connections. Wi-Fi devices are

present everywhere and any products with smart functions depends on it for a steady and smart internet connection. Many generations of Wi-Fi connectivity have been released over the past two decades and the latest upgradation is Wi-Fi 6 with added features as lower latency, higher speed with better household Wi-Fi and improved battery life [25].

4.7 Cellular

IoT applications that require longer distance communications can make use of this technology. They support multiple data or voice connections over a single radio channel and is the technology used by the mobile phone networks. The evolution of different cellular network technologies are: 1G (First Generation) was the first wireless network technology established in 1980's based on analog technology, 2G (Second Generation) networks replaced 1G in 1991 and used digital technology and encryption, 2.5G (Second and a half Generation) networks were later created as an intermediate technology which introduced the first data services, 3G (Third Generation) networks provided the users with a complete data capable service and improved data rates for voice and audio–video streaming, 4G (Fourth Generation) Networks also called as 4G LTE offers better data rates and voice quality and supported high definition calling VoLTE (Voice over LTE) but its coverage area still needs to be expanded, 5G (Fifth Generation) networks which is the latest emerging technology provides lower latency, higher capacity and increased bandwidths compared to 4G [26].

4.8 NFC

It is also a short-range wireless technology that allows two electronic devices to communicate within 4 cm and mostly used for contactless payments. It can also transfer videos, photos, and contacts information between two NFC enabled gadgets. Some advantages of NFC over Bluetooth are: connection between two NFC devices are automatically created when the devices are in close proximity, hence no manual configuration is needed among devices and it is more secured since it have a shorter range and is faster [27]. It is a subset of RFID technology. Some other applications of this technology are medical applications, smart ticketing, logistics and shipping, IoT and 5G etc.

4.9 LoRa

It is a LPWAN protocol based on spread spectrum modulation techniques specially designed for IoT and machine to machine applications. It provides a dedicated connectivity for IoT use cases including smart city and industrial applications with reduced cost. Some of the benefits of this technology are, it provides a robust long-range communication, low power consumption and extended battery life for sensors, supports fully bidirectional communication, use of free unlicensed band, deep indoor penetration, higher scalability and security [28].

4.10 WiMAX

It is a long-range wireless MAN technology that supports both fixed and mobile connections. It provides higher bandwidth supporting longer distance communication with greater

speed together with multiple users [29]. Its commonly used for industrial applications, smart grids, smart meters etc.

4.11 Sigfox

It is the first dedicated LPWAN network for IoT and machine to machine communications. It is a reliable, low power inexpensive mechanism for interconnecting devices and sensors where object sharing is not attached to the networks. It is a software-based solution that reduces the energy consumption of devices. Here the computing and networking is done at a distant cloud rather than on the device itself, delivering high capacity and longer battery life. It is a lightweight protocol for handling small messages and uses ultra-narrow band modulation making it robust to noises throughout long distant communications [30]. Some of the applications that uses this technology are smart parking, risk management, gas tank remote monitoring etc.

4.12 Wi-Fi HaLow

It is a low powered and long-range Wi-Fi technology for IoT devices. It operates on spectrum below 1 GHz and has twice the range as that of other Wi-Fi technologies. It does not require any proprietary hardware or gateways setup and is appropriate for short burst data transactions. It can penetrate through walls and obstructions which make it suitable for indoor localization [31]. Its suitable for applications such as smart city, smart home, connected vehicles, smart healthcare etc.

5 IoT Hardware & Software

There are immense possibilities for IoT development in hardware and software. IoT hardware platforms are chosen accordingly as per the needs of IoT developers for product development or depending on the chosen applications and services. Some of the popular and commonly used hardware platforms are Raspberry Pi, Arduino, Beagle Board, Adafruit, Cloudbit, Samsung Artik, Pinoccio, Particle Photon etc. Table 2 provides some of the basic features, advantages, and disadvantages of some of these platforms. Once the hardware platform is chosen, next step is to choose the software. Many IoT software platforms are available in the market which provides various services such as machine-to-machine integration, device management, data management, protocol translation, security, and storage etc. These software platforms speed up and aids the entire procedure involved in the development of a product. It also eases the data management with the help of inbuilt data analysis tools which is a crucial task regarding IoT. They also offer better cloud storage. Table 3 provides a comparison on some of the commonly used software platforms for IoT.

6 IoT Protocols

An IoT eco-system comprises of huge number of interconnected devices which are power constrained, and it require protocols for efficient communication. These protocols should be chosen in such a manner that they consume a lesser amount of power and should be

Table 2 IoT hardware platforms

Parameters	Raspberry Pi	Arduino	Beagle board
Features	Acts as a fully-fledged minicomputer with Raspbian operating system Handles multiple programs at a time E.g., Audio and video streaming	Acts as a micro controller Handles single program at a time E.g., Opening/closing garage doors	Open-source single board computer Handles multiple programs E.g., Commanding actuators, reading external sensors data
Storage	Requires SD-card	On-board storage	On-board storage
Battery	Difficult to power up using battery	Easily powered using battery	Can be powered using battery
Complexity	Installation of libraries and software's required	Simple to interface sensors and other components	Networking is efficient and easy
Cost	Expensive	Lower cost	Very expensive
Connectivity	Easily connected to internet using Ethernet or USB interfaces	Requires external hardware integration for internet connectivity	Easily connected to internet using Ethernet or USB interfaces
Languages	Supports Python, C, C++, Ruby etc	Arduino language, C, C++etc	C, C++, Python, Perl, Ruby etc
Advantages	Supports variety of programming languages Complete support from Linux family Suitable for software projects Easy setup and continuous task performance	Deep programming knowledge not required Extensibility and huge library support Suitable for hardware-oriented projects Simple and easy to use	Works with open-source cloud 9 platforms Networking simpler and efficient Suitable for both hardware and software Extendable hardware
Disadvantages	Not open-source hardware Cannot handle inductive loads	Less powerful compared to others Difficult to code No graphic interface	No video encoding Limited USB ports to add external devices

Table 3 IoT software platforms

Software platforms	Supported hardware platforms	Protocols used	Estimated cost	Visualization
ArtikCloud	Raspberry Pi, Arduino, Samsung ARTIK	WebSocket, HTTP, COAP, MQTT	Free & paid accounts	Mobile apps., Third party apps., Dashboard
Axeda	Raspberry Pi, Arduino	MQTT, AMMP, REST, SOAP	Free & paid accounts	Home automation
Bugswarm	Arduino	HTTP	Free & paid accounts	Smart irrigation
Carriots	Raspberry Pi, Arduino	MQTT, HTTP	Free & paid accounts	Dashboard, Mobile apps
Cayenne	Raspberry Pi	COAP, MQTT	Free & paid accounts	Dashboard, Mobile apps
Kaa	Raspberry Pi, Intel Edison, Econais, LeafLabs, BeagleBone, Texas Instruments	XMPP, HTTP, COAP, MQTT	Open source	Dashboard, Mobile apps
Leylan	Arduino Yun, Netduino, Raspberry Pi, Spark Core, Texas Instruments	OAuth 2.0, MQTT, HTTP	Open source	Web apps., Third party apps
Sensorcloud	Arduino	HTTP	Paid accounts	Home automation
Smartliving	Raspberry Pi, Arduino, Intel Edison,	Stomp, MQTT, HTTP	Open source	Mobile apps
Temboo	Arduino, Samsung Artik, Texas Instruments	HTTP, COAP, MQTT	Free & paid accounts	Dashboard, Mobile apps
ThingBox	Raspberry Pi	MQTT, HTTP	Open source	Emoncms
ThingSpeak	Raspberry Pi, Arduino	HTTP, MQTT	Open source	Dashboard, Mobile apps
ThingSquare	Raspberry Pi, Arduino	HTTP	Open source	Home automation, Social IoT

Table 3 (continued)

Software platforms	Supported hardware platforms	Protocols used	Estimated cost	Visualization
Ubidots	Raspberry Pi, Arduino Spark Core, Adafruit FONA	UDP, HTTP, COAP, MQTT	Free & paid accounts	Dashboard
Wyliodrin	Raspberry Pi, Arduino, Intel Galileo & Edison, BeagleBone	HTTP, MQTT	Free & paid accounts	Dashboard, Mobile apps

able to reliably connect these devices over the internet. Some of the key protocols used in different layers of IoT are described below. (Here the four-tier IoT architecture is taken as a reference).

6.1 Perception Layer

- IEEE 802.15.4

It is designed for enabling communication between power constrained IoT devices with less complexity and minimal hardware. It defines the physical and mac layer for the working of LR-WPAN and supports short range communications at lower cost and utilizes less power. This low-cost wireless link supports industrial/commercial sensor and actuator devices. To support long range transmissions, all devices must work in unification adopting multi-hop routing [7].

- TSMP

It is a reliable, secure, and low power communication protocol for self-organizing networks of mobile devices called motes. It is a managed network supporting scalable, flexible, self-healing and low maintenance required communication. It supports fully redundant mesh routing and can operate in a noise environment [32]. Some of its applications are in industrial process automation, climate control etc.

- ZigBee, WSN, RFID, Wi-Fi, WiMAX, Cellular technologies are also used by various devices for communication depending on its uses and applications.

6.2 Network Layer

- 6LoWPAN

It is the abbreviation for IPv6 Over Low Power Wireless Personal Networks specifically designed to handle the IPv6 packets transactions over IEEE 802.15.4 links. It make use of fragmentation and header compression mechanisms to efficiently transmit packets over IEEE 802.15.4 networks with reduced transmission overhead and lesser energy consumption which make it apt for multi-hop packet transmission in a mesh network [33]. It provides wireless internet connectivity with low data rates suitable for uncomplicated embedded devices. It is commonly used for smart home, smart agriculture, IIoT etc.

- RPL

It stands for Routing Protocol for Low-Power and Lossy Network, designed by IETF. It is a distance-vector routing protocol for IoT systems. It creates a DODAG (Destination Oriented Directed Acyclic Graph) where only a single route exists from each leaf node to the root through which the traffic is sent and the root node only have the knowledge about the entire DODAG [34].

- CORPL

It is an extension of previous RPL protocol and stands for cognitive RPL. It also makes use of DODAG topology but with little added modifications. It uses opportunistic forwarding for packet routing between nodes. Here rather than the root keeping entire information about the network, any changes to the nodes are immediately updated to its neighbors using periodic update messages through which every nodes have knowledge about the entire traffic [35].

- CARP and E-CARP

Channel-Aware Routing Protocol is designed for under water communication based on distributed networks with light weight packets. It supports gateway redundancy, which ensures the network availability and reliability while providing services. It offers a failover mechanism where in case if the master router fails, then all its tasks and functions are transferred onto the slave router. One disadvantage is that it does not support the reusability of previously collected data and cannot be used for IoT applications that requires excessive data exchanges. E-CARP is the enhanced version of CARP with added feature of saving the previously collected sensory data thereby reducing the communication overhead [36].

- 6TiSCH

It was developed by IETF and is an IPv6 standard for 802.15.4 MAC layer protocols to enable low power industrial grade networks fitting for time-critical applications. It allows Time-Slotted Channel Hopping (TSCH) to reduce the channel fading and interference and make use of IPv6 adaption layer. This property makes it suitable for Low Power Lossy Networks (LLN) and industrial mechanizations [37].

- 6lo

It is the acronym for IPv6 over Networks of Resource-constrained Nodes and provides IPv6 connectivity for constricted node networks with limited resources, memory, and processing power. It was developed by IETF to provide IPv6 connectivity to the data links that are not included by 6TiSCH and 6LoWPAN. It makes use of 6LoWPAN stack for low power adaption, stateless header compression and for reduced multicast and reliable communications. It focuses on smaller works without considering larger cross-layer efforts [38]. Two of its specifications are IPv6 over Bluetooth Low Energy which is an adaption layer standard for Bluetooth 4.0 Media Access Control layer protocol and IPv6 over G.9959 which provides a basic level of security [39].

- IPv4 and IPv6

Internet Protocol version 4 (IPv4) is one of the core network layer protocols developed by ARPANET in 1983 for identifying devices on a network based on 32 bit addressing scheme. It is a connectionless protocol and requires less memory. But the addressing space is quickly depleting as the number of devices connected to the internet is increased exponentially. Some other disadvantages are lack of quality of services, security, and insufficient protocol extensibility. Internet Protocol version 6 (IPv6) is the successor of IPv4 initiated by IETF in early 1994 and can accommodate more IP addresses. It follows 128-bit, hierarchical addressing scheme and is a connectionless protocol used by huge number of devices. It is suitable for neighboring node interactions and provided with built in security.

Even though both protocols can co-exist in a network, but they cannot communicate with each other (dual Stack).

6.3 Support Layer

- UDP

User Datagram Protocol is a connectionless protocol widely used for time-sensitive transactions such as DNS lookup, video play backing and WSN. Even though it does not guarantee any reliable data transmission, they can be used for applications which are flexible to data packet losses during the transit. It does not require any handshake mechanism as that of TCP. Hence it is faster having minimum overhead and minimum CPU usage providing consistent performance but it is unreliable and lacks ordering functionality and error checking [40]. So, it is best fit for delay tolerant applications such as gaming, audio–video transmissions, etc.

- DCCP

Datagram Congestion Control Protocol is a message-oriented protocol which is more secure than TCP. It uses a six-byte long packet ID which makes it difficult to hack the packets and hence used for time sensitive applications as VoIP, media streaming etc. DCCP provides unreliable flow of datagrams with acknowledgments, reliable handshake mechanism, and congestion control [41].

- SCTP

Stream Control Transmission Protocol is a reliable message-oriented protocol which make use of congestion control and four-way handshaking for securing communications. It also supports multi homing connections where the endpoints can have multiple IP addresses and redundant paths to improve resilience and reliability [42]. Some of its applications are in 3G/LTE networks etc.

- RSVP

Resource Reservation Protocol is a signaling protocol that allows the receivers to stockpile resources to ensure the needed QoS during the traffic flow. It operates on the top of both IPv4 and IPv6 allowing simplex data flows. RSVP is designed for senders, receivers, and routers to communicate with each other [43]. They are commonly used for multimedia and real time applications such as teleconferencing, videoconferencing etc.

- QUIC

Quick UDP Internet Connections works over UDP using an encrypted protocol designed to secure and accelerate HTTP traffic, eventually replacing TCP and TLS over the web. Some of its features are its built-in security, ability to multiplex different HTTP requests over the same TCP connection, migration of connections between cellular data and Wi-Fi, header compressions to lessen redundancies, and the ability to overcome reflection attacks [44]. Chrome web browser connections uses this protocol to connect with google servers.

- RPL

Routing Protocol for Low Power and Lossy Networks is a distance vector routing protocol developed for 6LoWPAN constrained networks, to route the packet with minimum latency over the network. It consumes minimal power and efficiently handle the packet losses by delivering the packets to the endpoints whenever it is available and based on IPv6 standards making it suitable for IoT applications [45].

- DTLS

Datagram Transport Layer Security supports the communication of datagram-based applications which protects them from eavesdropping, message tampering and forgery. It consumes less power, lower overhead, reduced latency, and provides end-end encryption [46]. It can be used in online gaming, video conferencing, VoIP etc.

6.4 Application Layer

- CoAP

It stands for Constrained Application Protocol which allows IoT devices with limited hardware to join a network with less bandwidth and power. It works like HTTP (Hypertext Transfer Protocol) which is a client/server protocol and hence called as a request/response protocol, but with some modified functionalities from HTTP to support constrained device interactions following a RESTful architecture. It was originally designed for machine-to-machine communications and is a light-weight protocol. It consumes fewer resources compared to HTTP and runs over UDP supporting both unicasting and multicasting [47]. It has two layers: the messaging sublayer for detection of duplicate messages and to provide reliable communication since UDP lacks built-in error recovery mechanism, the request-response sublayer for handling REST communications to ensure security and scalability of the system. It has four messaging types: confirmable and non-confirmable messages which are used to achieve the reliability of CoAP, reset message when communication failure or missing messages occurs and acknowledgement message. Some of its features are it supports on-demand subscriptions utilizing publish/subscribe mechanism, client resource discovery, flexible communications with different devices and maintains the integrity and confidentiality of the data transmissions [48].

- MQTT

Message Queue Telemetry Transport is a publish/subscribe protocol supporting light-weight machine to machine communications. Here devices can publish messages to other devices or subscribe a topic of interest from other devices. MQTT consists of three components publisher, subscriber, and a broker. Client can act as a publisher/subscriber and server acts as a broker who coordinates the subscription messages, filter the messages, and authenticate the client, provides quality of services and allows long term storage of messages on request. It is a many-many communication protocol and runs over TCP [49]. Some of the real-world applications using MQTT are for energy meters, healthcare, Facebook notifications etc.

- AMQP

Advanced Messaging Queuing Protocol is like MQTT but with an additional feature of storing and forwarding data. It was designed for financial applications and provides reliable transactions (net banking). It supports both request/response and publish/subscribe models and runs over TCP. Here the broker is divided into two components: the exchange component that receives messages from publishers and forwards to message queues based on priorities and the message queue stores these messages until the client software processing is done and later on forwards it to corresponding clients based on some primacies. Microsoft, Bank of America, JP Morgan etc. are some of the applications that make use of this protocol [50].

- DDS

Data Distribution Service is a broker less publish/subscribe protocol designed for real time machine to machine communications. It uses multicasting and provides high QoS, reliable communications and quick data integration for its applications. DDS has two sublayers data-centric publish-subscribe (DCPS) and Data-Local Reconstruction Layer (DLRL). DCPS delivers information to the subscribers and DLRL is an optional layer which allows the integration of DDS into the application layer [51]. Some of its applications are in IIoT, smart grid, robotics, air-traffic control etc.

- XMPP

Extensible Messaging and Presence Protocol is an instant messaging protocol for providing chatting, audio, and video calls over the internet. Since it uses XML, it supports low-latency messaging, and hence its applicability is extended into IoT devices. Even though it provides higher flexibility, it requires higher bandwidth, CPU usage and does not guarantee QoS but can be used for object to object communication based on XML messaging [52].

- SMQTT

It stands for Secure MQTT which adds security to the existing MQTT protocol based on lightweight attribute-based encryption. It supports broadcast encryption where a single encrypted message is delivered to multiple nodes making it apt for IoT applications. This protocol is also based on publish/subscribe model and enables communication security and is resistant to variety of attacks. But its key generation and encryption algorithms depends on the developers [53].

7 Advanced Computing Paradigms

7.1 Cloud Computing and IoT

IoT devices generates huge amounts of data and CC paves way for these data to reach their destinations and enables these devices to function more efficiently. CC is a paradigm born from the need of utilizing computation as a utility [54]. It is defined as the on-demand

delivery of computing services including storage, servers, networking, databases, and processing power over the web on a pay as you go basis. Instead of owning the entire computing infrastructure by themselves, companies can rent access to any of these services from cloud service providers where big data analytics, decision making, and computation takes place centrally at distinct cloud data centers. CC provides 3 generic services as follows:

- Platform as a Service (PaaS): It provide platforms and environments required for the developers to build different applications and services. It offers clients, the flexibility of developing, running, and managing web-based applications and supports the overall management of different applications. e.g., Microsoft Azure etc.
- Infrastructure as a service (IaaS): It provides users with a virtualized environment for accessing various computing resources such as bandwidth, servers, storage etc. Hence for small scale industries rather than having the entire infrastructure, they can rent the necessary services on a paid manner. e.g., Amazon Web Services, Cisco Meta Cloud, Google Compute Engine etc.
- Software as a Service (SaaS): It is a software distributed model which allows clients to have access to various applications hosted by third party service providers over the internet. e.g., Twitter, Instagram, Facebook, Dropbox, Cisco WebEx etc.

IoT deployments generally consists of a huge number of sensor nodes to collect and deliver data to a centralized location where the analysis and processing is done. Mostly cloud acts as this centralized area for storing these big data and extracting the required information. It enables the users to access information from anywhere with an internet connectivity [55]. Some advantages of using CC for IoT devices are privacy and security, accessibility to remote computing services, robust data integration and provides various services for small scale businesses, seamless inter-device communications with better connectivity, reliability, and computing power.

Some drawbacks of Cloud Computing are, the difficulty in managing the traffic and congestion of massive data flows within a network, delay sensitive applications experiences greater latency and market monopoly, where top multinational enterprises could only afford to set up a cloud infrastructure and to define and deploy proprietary protocols. Since it is a centralized architecture, it requires more down time i.e., a single node failure affects the working of all other nodes in the network. These factors let the beginning of a post-cloud era and the development of Edge and Fog Computing [56].

7.2 Edge Computing and IoT

The increased interest in decentralized paradigms opened the way for EC, where the data is stored and processed at network edge rather than on a distant cloud data center. It overpowered certain challenges that CC cannot address such as bandwidth, connectivity, infrastructure needs and latency. EC focuses more on the things side where the storage happens in the device, and the data is analyzed and applied in real time closer to the intended users. Here the data is not required to travel to a centralized server for the device to determine what function to be executed, thereby reducing the latency, and enhancing the performance of the devices. EC is commonly used by telecoms and middleware companies and some examples for EC devices are Smart Phones, Micro Data Centers and Cloudlets. Edge devices not only consumes data but also generates data and performs computing tasks on the data sent to and fro the cloud and can act as a standalone node [57]. EC services prevents DDoS attacks and

provide uninterrupted services to the users, reduces network bottleneck, less energy consumption and network problems at distant location rarely affects the local edge customers. Some disadvantages are, it lacks programmability, no standardized security protocol, requires more hardware for storage and provides incomplete data [58].

7.3 Fog Computing and IoT

IoT devices requires latency aware computation for real time application processing. Data produced by these devices are generally stored in a cloud infrastructure which is not suitable for time sensitive applications. To address this issue, FC, which resides between cloud and end devices is proposed [59]. Main aim of FC is to extend the services and functionalities offered by cloud near to the users for optimizing device performance [60]. Major difference between EC and FC is that EC leverages the computing capabilities on the devices or on a gateway device whereas, in FC this happens in the processors connected to the LAN or in the LAN hardware itself and has more processing capabilities than EC. Hence in this case data analytics and intelligence occurs far away from the users compared to EC but closer than that of CC.

IoT Devices are connected to fog devices which resides near users and are responsible for intermediate computation and storage which results in effective distribution of computing, storage, networking, and management services along cloud to things continuum. It provides a transient storage and sends the periodic data updates to the cloud. This is mostly chosen by service providers and data processing companies. FC meets todays application requirements for local content storage, resource pooling, real-time processing and focuses more on the infrastructure side. Any devices having storage, processing, and networking capability can act as a fog node. Main characteristics of FC are low latency and location awareness, geographic distribution and end device mobility, capacity of processing high number of nodes, provides wireless access, faster processing and fewer resource consumption, supports real-time applications and heterogeneity [61]. Some disadvantages are it requires more infrastructure, maintenance cost, complexity and power consumption as larger number of nodes get connected to the network.

Opportunistic FC is an upcoming concept in FC where, traditional FC with fixed resources fails to fully meet the demands of high-velocity, mobile and real time IoT services in hazardous or resource-poor environments. In such scenarios opportunistic fog can co-exist with fog nodes giving them the capability to dynamically adapt to the changing framework as required [62]. Some real-world use cases of FC are in smart fog based video surveillance for crime assistance in smart transportation [63], monitoring elderly people, home automation systems, IIoT etc. Figure 4 represents the features of CC, EC, FC and their applications and middleware.

FC and EC cannot replace CC nor superior to each other, but they fulfill the requirements of each applications in a separate manner and are ultimately chosen by the user who determines which paradigm is required and matches the needs of their applications.

8 IoT Security

IoT security is a very challenging area that deals with safeguarding the connected devices and the networks involved by means of appropriate security measures. Since all the devices are connected over the internet there are higher chances of attacks if the devices are not properly protected. One of the major challenges is that most of the manufactures focus on getting their products to the market quickly rather than concentrating on providing end-end

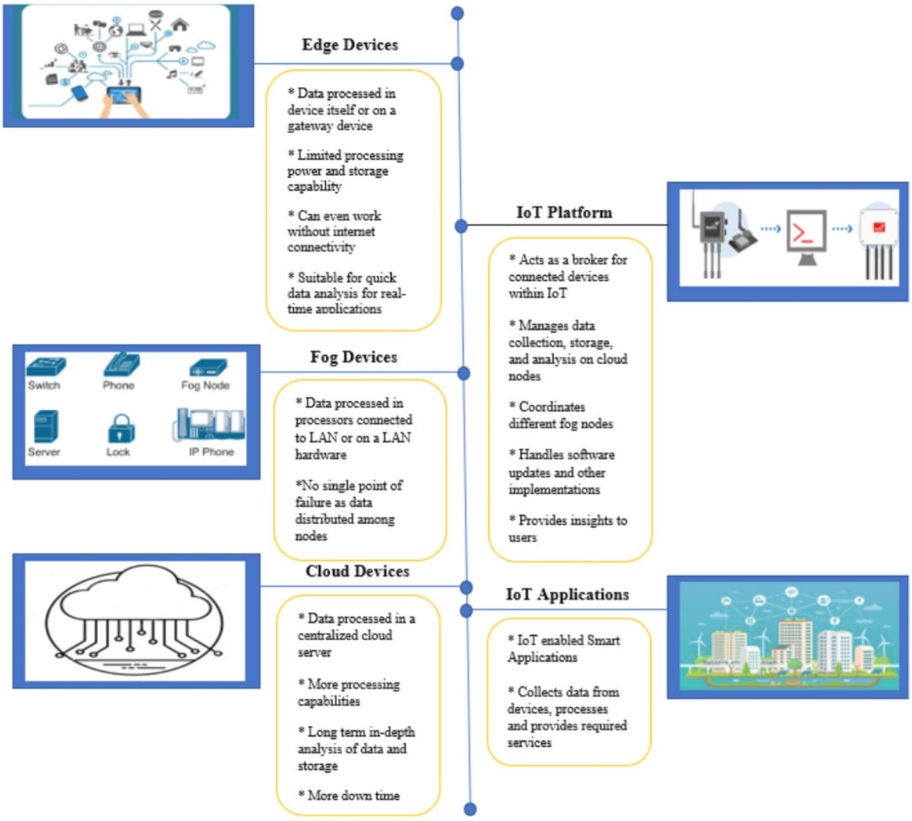

Fig. 4 CC, EC, and FC features

security from the beginning. As the IoT devices are resource constrained it is difficult to implement security features as it requires more hardware and cost, lack of standardized architecture, and the use of default passwords also leads to security infringements. Some factors to be considered for ensuring security are: firewalls should be provided in IoT networks to filter the incoming packets to the devices, IoT devices software should be authorized, updates and patches on these devices should be done without expending additional bandwidth, all the devices should be authenticated before connecting to the network [64]. Figure 5 represents four-tier architecture and possible security measures.

8.1 Security Attacks in each Layer of IoT

8.1.1 Perception Layer

- Node Capturing: Here an attacker gain access or replace a gateway node and leaks the communication between the sender and the receiver. The attacker may even capture the cryptographic keys and shares it with a malicious node, who can thereby pretend as a legitimate node and join the network [65].

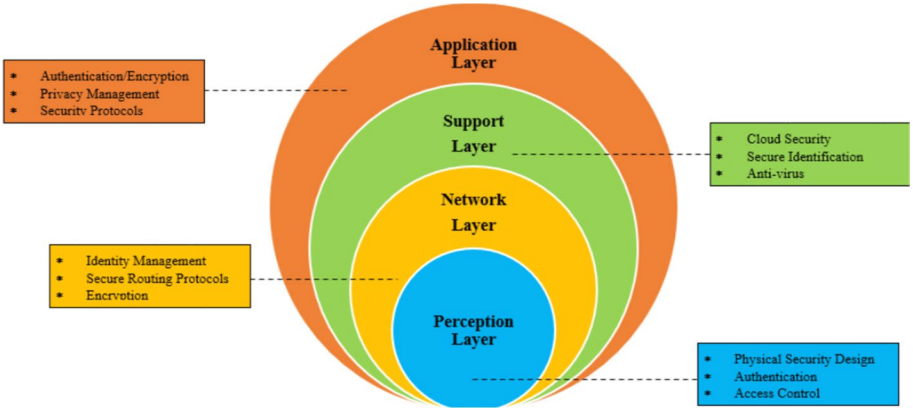

Fig. 5 IoT four-tier architecture with possible security measures

- Eavesdropping: Here an attacker can easily get access over a communication happening amid unsecured devices or networks and steals the information being sent or received for malicious works [66].
- Malicious Code Injection: Once an attacker captures a node, he can inject malicious codes into the memory of the node through which he can gain control over the entire system or make the system behave abnormally. This usually happens when the devices are updated through air without much security [67].
- False Data Injection: Here the attacker can inject false data onto the captured node and transmit it onto different applications. Later on, the applications provides wrong services receiving this faulty data which affects the efficiency of the IoT system [68].
- Booting Attacks: Since the inbuilt security features of a device are not enabled during the booting process, attacker tries to gain access over a node while it is rebooting [69].
- Side Channel Attacks and Cryptanalysis: In cryptanalysis the attacker tries to procure algorithm vulnerabilities applying various mathematical formulas and break into the system. Side Channel Attacks deals with snooping on the power consumption of a device or the keystrokes to steal the encryption key [70].
- Sleep Deprivation Attacks: Here the attacker tries to drain the power of IoT devices through infinite loops or falsely maximizes the power consumption which minimizes their lifetime. This results in denial of services by these devices [71].

8.1.2 Network Layer

- Dos Attack: Here an attacker floods the target nodes or network with unwanted traffic either making the node fail to respond to legitimate user requests or crashing the node. There are multiple ways to launch DoS attacks such as buffer overflow, ping of death, teardrop etc. A variant of DoS is Distributed DoS in which multiple systems targets a single node with DoS attack and makes it difficult to recover from the failure. Due to the heterogeneity and lack of strong configurations, many of the IoT devices are prone to these attacks [72].
- Man-in-the-Middle Attack: Here an attacker secretly eavesdrops the communication between two parties and gain access over the real time traffic. Later on, the adversary

can inject false information's between the transmission and make the node perform some inadvertent actions [73].

- Phishing Site Attack: Here the opponent sends fraudulent communications to different users, which appears as legitimate messages and somehow compromises the user id and password with minimum effort. Once acquiring the user's sensitive information, they can launch various attacks onto the hacked IoT devices [74].
- Routing Attack: Here the adversary tries to change the route of the data transit. Sinkhole attack is a kind of routing attack in which the attacker advertises a fake shortest route to the nodes to re-route their traffic through it and later can even launch DoS attacks on the compromised nodes. Wormhole attack is another kind in which the attacker nodes tries to strategically position themselves in the network creating a virtual tunnel and advertises their shortest routes. Once any legitimate nodes chose the given route and starts communication, the malicious nodes record the packet transactions and tunnels it to other locations. Another type is out of band attack which provides alternate out of band channels for communication [75].
- Storage Attack: With the help of weak protocols, the attacker somehow gain access over storage devices or cloud which stores user's sensitive information. Once they gain access into the cloud they may alter the data and provides wrong details [76].

8.1.3 Support Layer

- Malware Injection and Flooding in Cloud: Here the adversary injects malicious code or even a virtual machine onto the cloud and gains access over user's sensitive information. Later on, they launch Dos and floods the cloud which depletes its quality [77].
- Signature Wrapping attack: Here the signature algorithm is manipulated by the attacker to gain access over protected resources and modify its contents [78].
- SQL Injection Attack: In such attacks the adversary tries to inject malicious codes into the system or execute malicious commands and can even get complete information about the system and gain control over it [79].

8.1.4 Application Layer

- Data Thefts: IoT applications usually contain user's personal data and since the data is sent over the network there are greater chances of data theft. A single loophole in the system may even fail the entire system [80].
- Malicious Code Attack: Here the attacker utilizes cross-site scripting to break into the system which results in seizing and paralyzing the entire IoT system [81].
- Secure on-boarding: When a new sensor node is added to the network it passes the encryption key to the corresponding services through the gateways which are prone to eavesdropping or other forms of attack. Then the attacker can gain access to the encryption keys [82].
- Reprogram Attacks: Here the attacker can alter the device parameters if it is not protected well and can induce dangerous actions [83].

8.2 IoT Security Using Artificial Intelligence & Machine Learning

AI is a technology that targets computers do human-like reasoning [84]. Some advantages of AI powered IoT are, it provides predictive maintenance to avoid unforeseen

device failures, can improve operational efficiency and risk management, developing fully automated devices, enables improved services and customer satisfaction etc. ML techniques are adopted to enhance the security of IoT devices, to achieve automation, detecting anomalies, malwares, or misuses in a system. Different ML algorithms can be used in network-based solutions for identifying authenticated devices to join a network, monitoring incoming and outgoing traffic and creating profiles for detecting normal and abnormal behaviors [85]. Even though there are many algorithms, few of the AI and ML solutions to overcome the threats discussed in previous section are described below.

- Dos/DDoS Attack: This is one of the most malicious attack that floods a system and obstructs the legitimate traffic and may even collapse the system. In [86] authors have proposed an online approach using ML to detect Dos/DDos attacks based on Random Forest (RF) algorithm. The proposed approach can act as a sensor that can be installed in a network and crosschecks the network traffic with signatures of previous traffic to identify the attack. Another approach for detecting this type of attack is by using a Convolutional Neural Network (CNN) [87]. In [88] authors have proposed a light weight intrusion detection scheme called secure-MQTT using fuzzy rule interpolation for identifying such attacks.
- Spoofing Attacks: It can be prevented using different ML algorithms [2] such as Q-Learning, Dyna-Q, Deep Neural Network (DNN), Support Vector Machines (SVM) etc. In [89] authors have proposed a two stage DNN for identifying spoofing attack with a small false alarm rate.
- Malware Detection: In [90] authors have proposed a framework using Deep Learning (DL) with feature extraction to detect malwares in IoT devices. In [91] authors proposed a framework using K-Nearest Neighbor (KNN) algorithm in a map reduce environment for malware detection.
- Eavesdropping: Some of the ML techniques that can detect and prevent this attack are SVM [92], Q-Learning [93], Non-parametric Bayesian technique [94].
- Jamming attack: Kernelized SVM [95], Deep Q-network (DQN) [96] are some of the ML techniques that can be used for preventing jamming attacks. Table 4. Represents different security attacks and its countermeasures using AI an ML.

Still there exists some limitations in applying more of AI and ML techniques in IoT due to the power constrained nature and energy consumption of these devices. ML and DL algorithms uses labelled data in learning processes and these data sets requires more storage space [97]. Hence utilizing minimum learning data and its deployment on these resource constrained devices are challenging. Also, lack of interoperable tools suiting

Table 4 AI & ML based security techniques

Security attacks	AI & ML techniques
Dos/DDoS	Random forest, CNN, fuzzy logic
Spoofing	Q-learning, Dyna-Q, SVM, DNN
Malware detection	DL, K-NN, random forest
Eavesdropping	SVM, Q-learning, non-parametric Bayesian
Jamming	SVM, DQN, Q-learning

different architecture and rapidly changing environment where new training data is continuously engendered restricts in developing a fully secured IoT framework.

8.3 IoT Security Using Blockchain

BC is another breakthrough technology which provides a trustworthy information sharing service, with the capability to address certain IoT security issues utilizing a distributed, transparent, immutable, and secure model. It is a decentralized ledger of transactions based on cryptography comprising of a block header, list of transactions and previous block hash. All this information is stored in a Merkle tree which is a hash-based data structure containing each individual transaction and the root of hash tree [98]. Figure 6 represents the working of the BC architecture. Initially user requests a transaction, and it is represented as a block. Then it is verified by different computers or nodes present in the network and once the transaction is approved by the majority of the participants, the block is added onto the BC along with other blocks which further cannot be modified [99].

Some of the benefits of using BC in IoT are, data generated by IoT devices can be stored using BC which makes it difficult for the hackers to break the hash and access or modify its contents. Hence it delivers a robust and tamper-proof mechanism to store user sensitive data and hence thwarts data loss and spoofing attacks. Also, BC being a decentralized ledger, no organizations can take control over the data and only the authorized users have the authority to verify the past transactions. It also supports IoT companies to reduce the overall infrastructure cost in processing and the use of smart contracts which are set of rules automatically triggered when certain conditions are met, also eases fully automated tasks and can thus eliminate the need of any centralized architecture [100].

Some of the use cases of BC and IoT are Chain of Things (CoT) [101] which is a research lab for developing applications merging these technologies such as chain of security, chain of solar, chain of shipping etc., IOTA [102] an open and scalable distributed ledger supporting frictionless data transfer, in supply chain management combining IoT sensors data with BC, smart logistics etc. There are also certain challenges in combining

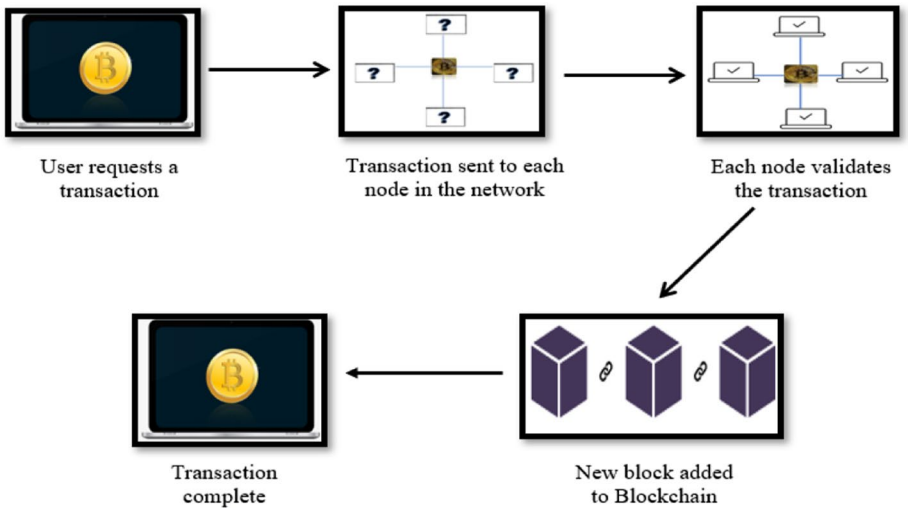

Fig. 6 Blockchain architecture

these two technologies: The block generation time required by BC is slow compared to data generated by IoT devices creating latencies in the transaction processing, power hungry nature of both technologies and the varied processing time of sensors in the connected devices. BC also requires wider storage capability which is limited for the constrained IoT devices. The difficulty in integration of various IoT platforms and its legal issues are also some of the drawbacks.

9 IoT Applications

IoT has a very vast number of applications and it is almost used in everyday life. Even though there are many, some of the major examples are as follows:

- Smart City

It is an urban area that involves the use of various technologies for providing services and enhancing the quality of life of citizens. It spans a variety of applications including traffic management, environmental monitoring, security, smart parking, smart governance etc.

- Smart Home

It involves remote monitoring and accessing the appliances at home using a smart phone or laptop. It provides security, energy management, maintenance and some of the applications includes temperature controller, door lock management etc.

- Smart Health:

Healthcare is a fundamental area and its integration with IoT provides more smarter services to people such as monitoring elderly people, helping them to stay active longer, growing the independence of impaired people, smart pills for monitoring patches, wearables such as smart watches, smart bands for detecting various diseases symptoms, remotely monitoring health conditions of patients by doctors, emergency services and provides ambient assisted living [103]. Figure 7 represents various IoT Applications.

- Smart Grid

It delivers a variety of operations such as smart meters for monitoring and identifying energy fraudulence, identifying the behavior of customers and electricity suppliers, use of renewable energy sources etc.

- Smart Transportation

It aims at delivering more efficient and accessible transportation services to people, providing better traffic management, route optimization [104], smart parking, road anomaly detection and accident prevention, connecting vehicles etc.

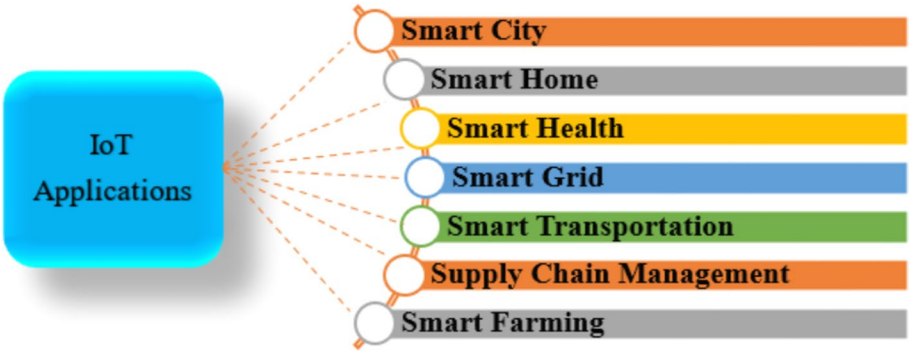

Fig. 7 IoT applications

- Supply Chain Management

It helps in tracking and managing the flow of goods from raw materials to service delivery, inventory information management for suppliers, tracking commodities in transit, preventing unplanned downtime, facility and inventory management, quality control, smart retail, chain optimizations, ensuring industrial safety, connecting factories etc.

- Smart Farming

It helps the farmers in monitoring their fields with the help of drones, to improve the quality of farming through automated soil monitoring sensors, water management, providing smart green house, livestock monitoring etc.

10 IoT Challenges and Future Research Directions

IoT deployments are varying accordingly with each application from smart homes to connected vehicles and to tackle the current IoT adoption barriers, one need to address the challenges early from the design stage to the implementation outcomes. Some of the open issues needed to be addressed are data privacy and protection, high implementation cost, uncertainty in accomplishing goals, insufficient solution architecture etc.

- Big Data and Connectivity: Since IoT devices produces huge amounts of data, the flow of these data to and fro from devices, infrastructure, cloud, and applications providing a smooth connectivity is really a challenging issue [105]. Also the number of new devices connected to the network is increasing day by day raises the challenge even more as each device will be utilizing different technologies [106]. Also power constrained nature of these devices limits the applicability of new technologies such as BC, ML etc. to a full extend [107]. Hence new technologies that consumes less power such as Sigfox, LoRa etc. need to be considered widely.
- Security and Privacy: To provide more security and privacy, companies are in the wake of continuous fragmentation in IoT implementation resulting in higher costs and less customer satisfaction [108]. Still many IoT devices transmit data openly dur-

ing transit or at rest due to the inability of connected devices in adopting advanced cryptographic standards which leads to data harvesting and selling [109]. And so, before storing user sensitive data organizations should model privacy and compliance rules to protect the identity of users. Security algorithms should be designed in such a manner that it lowers the number of message handovers to utilize minimum bandwidth and efficiency. Most of the security factors are focusing on enhancing network and cloud protection rather than focusing on endpoints and also air update vulnerabilities act as an entry point for hackers into the network and access private data. Hence these loopholes must be identified, and devices should be given periodic database upgradations of known anomalies [110].

- Standards, Interoperability and Coexistence: Biggest barrier in businesses from adopting this technology are the interoperability issues including syntactic, semantic, and cross-domain interoperability [111]. To fully deploy these factors without any failure and to ensure service quality companies must include multiple strategies from operational, tactical, strategical to technological trials requiring more time which hinders the products early market entry. Lack of a unified architecture forces each device to choose one based on their needs and this even more increases the algorithm and device complexity. Providing intelligence to devices by adopting various advancing technologies and smart algorithms helps them to automatically discover devices and services without human intervention and react accordingly. Cross-domain interoperability should be considered more utilizing semantic web technologies and interworking application programming interfaces [112]. Congestion in radio channel is another challenging issue faced by IoT devices which increases the chance of lossy connection while working in a crowded area due to the bordering interference [113]. Hence coexistence signaling should be carried out to find the device operability in a mixed signal environment [114].
- Scalability, Availability and Reliability: Adding new devices or services into an IoT network should not degrade the performance of existing devices with varying processing, storage, and memory capabilities [115]. Since it involves heterogeneity, it must be designed to handle extendible processes and services. Software and hardware compatibility should be provided to the customers even when failure transpires [9]. In case of mission critical applications, the system should be reliable and fast in data collection, communication and decision making where an erroneous decision can lead the entire system to fail and provide wrong services. Hence proper automated bootstrapping, IoT data pipelining and multi-dimensional scaling can be combined to enhance system capabilities [116].
- QoS and Energy Efficiency: From user perspective, Quality of Service refers to the communication quality of the services provided from connection establishment to service delivery [117]. It involves four main parameters as packet loss, latency, jitter, and mean opinion score. Certain factors such as hardware/software failure, overloaded networks etc. may lead to packet loss, unordered packet delivery, delay in packet transmission time between sender and receiver, which reduces the overall service quality [118]. Such communication errors should be rapidly recognized and rectified using efficient software, programs, or models. Since IoT devices are power constrained and in case of remote applications where battery power is the only resolution more advancing techniques like energy harvesting needs to be utilized [119]. Solar energy, wind energy, thermoelectrical energy, mechanical energy from piezoelectric materials etc. can be considered for powering up IoT devices [120]. Also,

Table 5 A summary of studies with respect to architectures and challenges

IoT parameters	References	Concepts covered
Architecture	[4–13]	Includes different layered architectures and functions of each layer
Technologies	[14–27]	Long-range and short-range technologies, emerging technologies
Protocols	[28–50]	Layer wise description of protocols used and its functions
IoT & cloud	[51–53]	Features of cloud, its integration with IoT and its advantages and disadvantages
IoT & edge	[54, 55]	Edge features and advantages in integration with IoT, its applications
IoT & fog	[56–60]	Integration of fog with IoT and its features, added security provided
Security attacks	[62–80]	Layer wise attacks
AI & ML in IoT	[81–93]	AI and ML adoption for preventing security attacks, advantages, and disadvantages
BC in IoT	[95–98]	Integration of BC with IoT, added security features
Security & privacy	[105–107]	Existing challenges in adopting security and privacy
Interoperability	[108–111]	General issues, parameters to be adapted
QoS	[115–118]	Issues that prevent QoS

energy efficient protocols must be designed adding deep sleep–wake up cycles, discontinuous reception, AI edge processing, fog edge processing etc.

- Regulatory Issues: Due to the unregulated network data flow IoT is facing many social and legal problems. It includes privacy preservation, data security, safety, data usability, trust etc. and legal regulations on private data collected needs to be strictly executed without infringing people's privacy. Difficulty in accurately identifying owners for data collection and the absence of users public and private data border lines are some of the challenging issues in applying ethics into IoT environment [121] (Table 5).

11 Conclusion

IoT is all prepared to amalgamate with different technologies to re-shape the whole world making lives even smarter, effortless, and prosperous. Modern IoT eco-systems are complex and since user's private data are being transferred, any breach directly affects the people's lives adversely. To provide better security and privacy there is a need of unified architecture, protocols, and technologies. The objective of this paper is to provide a through summary on IoT eco-system to help the researchers to understand the basics and in-depth knowledge of various technologies and protocols used. We have also discussed various security threats and the assimilation of advancing technologies in IoT which benefit the future researchers.

Funding Not Applicable.

Data Availability Not Applicable.

Code Availability Not Applicable.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Alli, A. A., & Alam, M. M. (2020). The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications. *Internet of Things, 9*, 100177. https://doi.org/10.1016/j.iot.2020.100177
2. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access, 7*, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045
3. Afzal, B., Umair, M., Asadullah Shah, G., & Ahmed, E. (2019). Enabling IoT platforms for social IoT applications: Vision, feature mapping, and challenges. *Future Generation Computer Systems, 92*, 718–731. https://doi.org/10.1016/j.future.2017.12.002
4. Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors (Switzerland), 18*(9), 2796. https://doi.org/10.3390/s18092796
5. Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*. https://doi.org/10.1155/2017/9324035
6. Perwej, Y., Ahmed, M., Kerim, B., & Ali, H. (2019). An extended review on internet of things (IoT) and its promising applications. *Communications on Applied Electronics, 7*(26), 8–22. https://doi.org/10.5120/cae2019652812
7. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095
8. Salman, T., & Jain, R. (2017). *Advanced computing and communications*, vol. 1, no. 1.
9. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*. https://doi.org/10.1186/s40537-019-0268-2
10. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200
11. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 336–341. doi: https://doi.org/10.1109/ICITST.2015.7412116.
12. Bairagi, V. K., Joshi, S. L., & Barshikar, S. H. (2018). A survey on internet of things. *International Journal of Computer Sciences and Engineering, 6*(12), 492–496. https://doi.org/10.26438/ijcse/v6i12.492496
13. Bouras, M. A., Lu, Q., Dhelim, S., & Ning, H. (2021). A lightweight blockchain-based IoT identity management approach. *Future Internet, 13*(2), 1–14. https://doi.org/10.3390/fi13020024
14. Shi-Wan, L., et al. (2019). The industrial internet of things volume G1 : Reference architecture. *Ind. Internet Consort. White Pap*, vol. Version 1, p. 58 Seiten.
15. Islam, R., Rahman, M. W., Rubaiat, R., Hasan, M. M., Reza, M. M., & Rahman, M. M. (2021). LoRa and server-based home automation using the internet of things (IoT). *Journal of King Saud University—Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2020.12.020
16. Requirements, F., et al. The IBM advantage for implementing the CSCC cloud customer reference architecture for internet of things (IoT).
17. INTEL. (2016). The Intel® IoT platform architecture specification white paper internet of things (IoT). pp. 1–11.
18. Qadah, E., Mock, M., Alevizos, E., & Fuchs, G. (2018). Lambda architecture for batch and stream processing. *CEUR Workshop Proc*, vol. 2083, no. October, pp. 109–116. [Online]. Available: https://d1.awsstatic.com/whitepapers/lambda-architecure-on-for-batch-aws.pdf.
19. rfid tags green iot. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7997698 (accessed Jun. 28, 2020).

20. Parada, R., Melià-Seguí, J., Morenza-Cinos, M., Carreras, A., & Pous, R. (2015). Using RFID to detect interactions in ambient assisted living environments. *IEEE Intelligent Systems, 30*(4), 16–22. https://doi.org/10.1109/MIS.2015.43
21. Arshad, R., Zahoor, S., Shah, M. A., Wahid, A., & Yu, H. (2017). Green IoT: An investigation on energy saving practices for 2020 and beyond. *IEEE Access, 5*, 15667–15681. https://doi.org/10.1109/ACCESS.2017.2686092
22. Stephen, A., Arockiam, L., & Scholar, R. (2021). Attacks against Rplin Iot: A survey. vol. 25, no. 4, pp. 9767–9786. [Online]. Available: http://annalsofrscb.ro.
23. Badenhop, C. W., Graham, S. R., Ramsey, B. W., Mullins, B. E., & Mailloux, L. O. (2017). The Z-Wave routing protocol and its security implications. *Computers & Security, 68*, 112–129. https://doi.org/10.1016/j.cose.2017.04.004
24. Gulati, K., Kumar Boddu, R. S., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2021). A review paper on wireless sensor network techniques in internet of things (IoT). *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.05.067
25. Chung, M. A., & Chang, W. H. (2020). Low-cost, low-profile and miniaturized single-plane antenna design for an internet of thing device applications operating in 5G, 4G, V2X, DSRC, WiFi 6 band, WLAN, and WiMAX communication systems. *Microwave and Optical Technology Letters, 62*(4), 1765–1773. https://doi.org/10.1002/mop.32229
26. Singh, S., Sanwar Hosen, A. S. M., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access, 9*, 13938–13959. https://doi.org/10.1109/ACCESS.2021.3051602
27. Basir, R., et al. (2019). Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors (Switzerland), 19*(21), 1–38. https://doi.org/10.3390/s19214807
28. Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the limits of LoRaWAN. *IEEE Communications Magazine, 55*(9), 34–40. https://doi.org/10.1109/MCOM.2017.1600613
29. Fizza, K., et al. (2021). QoE in IoT: A vision, survey and future directions. *Discover Internet of Things*. https://doi.org/10.1007/s43926-021-00006-7
30. Vejlgaard, B., Lauridsen, M., Nguyen, H., Mogensen, P., & Sørensen M. (2017). Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE.
31. Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. *IEEE Communications Surveys & Tutorials, 21*(3), 2568–2599. https://doi.org/10.1109/COMST.2019.2911558
32. Patnaik, R., Padhy, N., & Srujan Raju, K. (2021). A systematic survey on IoT security issues, vulnerability and open challenges. *Advances in Intelligent Systems and Computing, 1171*(January), 723–730. https://doi.org/10.1007/978-981-15-5400-1_68
33. Thread Group. (2015). Thread Usage of 6LoWPAN. *White Pap,* [Online]. Available: https://threadgroup.org/ourresources#Whitepapers.
34. Dhumane, A., Bagul, A., & Kulkarni, P. (2015). A review on routing protocol for low power and lossy networks in IoT. *International Journal of Advanced Engineering and Global Technology, 3*(12), 1440–1444.
35. Wu, Y. (2020). > accepted by IEEE Communications Magazine< 2.
36. Nur, R., Saharuna, Z., Irmawati, I., Irawan, I., & Wahyuni, R. (2019). Gateway redundancy using common address redundancy protocol (CARP). *IJITEE (International Journal of Information Technology and Electrical Engineering), 2*(3), 71. https://doi.org/10.22146/ijitee.43701
37. Vilajosana, X., et al. (2019). IETF 6TiSCH : A tutorial to cite this version : IETF 6TiSCH : A tutorial.
38. Gomez, C., Paradells, J., Bormann, C., & Crowcroft, J. (2017). From 6LoWPAN to 6Lo: Expanding the universe of IPv6-supported technologies for the internet of things. *IEEE Communications Magazine, 55*(12), 148–155. https://doi.org/10.1109/MCOM.2017.1600534
39. Hong, Y., Choi, Y., Shin, M., & Youn, J. (2015). Analysis of design space and use case in IPv6 over NFC for resource-constrained IoT devices. In *Int. Conf. ICT Converg. 2015 Innov. Towar. IoT, 5G, Smart Media Era, ICTC 2015*, pp. 1009–1012. doi: https://doi.org/10.1109/ICTC.2015.7354725.
40. Masirap, M., Amaran, M. H., Yussoff, Y. M., Rahman, R. A., & Hashim, H. (2016). Evaluation of reliable UDP-based transport protocols for internet of things (IoT). In *ISCAIE 2016—2016 IEEE Symp. Comput. Appl. Ind. Electron*, pp. 200–205. doi: https://doi.org/10.1109/ISCAIE.2016.7575063.

41. Hussain, F. K., Rahayu, W., & Takizawa, M. (2021). Special issue on Intelligent fog and internet of things (IoT)-based services. *World Wide Web, 24*(3), 925–927. https://doi.org/10.1007/s11280-021-00888-1
42. Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things, 11*, 100227. https://doi.org/10.1016/j.iot.2020.100227
43. Anuar, B., & Hepworth, E. (2003). WLRP: A resource reservation protocol for quality of service in next-generation wireless networks. In *Proceedings of the 28th annual IEEE international conference on local computer networks (LCN'03)* (vol. 742. no. 1303/03).
44. Megyesi, P., Krämer, Z., & Molnár, S. (2016). How quick is QUIC?. In *2016 IEEE Int. Conf. Commun. ICC 2016*. doi: https://doi.org/10.1109/ICC.2016.7510788.
45. Kharrufa, H., Al-Kashoash, H. A. A., & Kemp, A. H. (2019). RPL-based routing protocols in IoT applications: A review. *IEEE Sensors Journal, 19*(15), 5952–5967. https://doi.org/10.1109/JSEN.2019.2910881
46. Urien, P. (2016). Three innovative directions based on secure elements for trusted and secured IoT platforms. In *2016 8th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2016*. doi: https://doi.org/10.1109/NTMS.2016.7792482.
47. Khalid, L. F., & Ameen, S. Y. (2021). Secure Iot integration in daily lives: A review. *Journal of Information Technology and Informatics, 1*(1), 6–12.
48. Mohammed Sadeeq, M., Abdulkareem, N. M., Zeebaree, S. R. M., Mikaeel Ahmed, D., Saifullah Sami, A., & Zebari, R. R. (2021). IoT and cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal, 1*(2), 1–7. https://doi.org/10.48161/qaj.v1n2a36
49. Kumar, R. P. (2018). Applications in internet of things (IoT). In *2018 2nd Int. Conf. Inven. Syst. Control*, no. Icisc, pp. 1156–1161.
50. Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In *2017 IEEE Int. Symp. Syst. Eng. ISSE 2017—Proc.* doi: https://doi.org/10.1109/SysEng.2017.8088251.
51. White, T., Johnstone, M. N., & Peacock, M. (2017). An investigation into some security issues in the DDS messaging protocol. In *Proc. 15th Aust. Inf. Secur. Manag. Conf. AISM 2017*, pp. 132–139. doi: https://doi.org/10.4225/75/5a84fcff95b52.
52. hjp: doc: RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core. https://www.hjp.at/doc/rfc/rfc6120.html (accessed Jul. 04, 2020).
53. Secure mqtt. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7280018&casa_token=ruwbaN2lssUAAAAA:e6Ppy2aEiuFNGVOd0sMa1lD2NmiKly8K67r3qkQ9UF8L1fAK7NPrrVuB9bmuEeg0is7tUXMcd6M&tag=1 (accessed Jul. 04, 2020).
54. De Donno, M., Tange, K., & Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, IoT, edge, and fog. *IEEE Access, 7*, 150936–150948. https://doi.org/10.1109/ACCESS.2019.2947652
55. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975. https://doi.org/10.1016/j.future.2016.11.031
56. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems, 56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021
57. Yu, W., et al. (2017). A survey on the edge computing for the internet of things. *IEEE Access, 6*(c), 6900–6919. https://doi.org/10.1109/ACCESS.2017.2778504
58. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
59. Naha, R. K., et al. (2018). Fog computing: Survey of trends, architectures, requirements, and research directions. *IEEE Access, 6*, 47980–48009. https://doi.org/10.1109/ACCESS.2018.2866491
60. Omoniwa, B., Hussain, R., Javed, M. A., Bouk, S. H., Member, S., & Malik, S. A. (2018). Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet of Things Journal, 6*(3), 4118–4149.
61. Mukherjee, M., et al. (2017). Security and privacy in fog computing: Challenges. *IEEE Access, 5*, 19293–19304. https://doi.org/10.1109/ACCESS.2017.2749422
62. Fernando, N., Loke, S. W., Avazpour, I., Chen, F. F., Abkenar, A. B., & Ibrahim, A. (2019). Opportunistic fog for IoT: Challenges and opportunities. *IEEE Internet of Things Journal, 6*(5), 8897–8910. https://doi.org/10.1109/JIOT.2019.2924182

63. Neto, A. J. V., Zhao, Z., Rodrigues, J. J. P. C., Camboim, H. B., & Braun, T. (2018). Fog-based crime-assistance in smart IoT transportation system. *IEEE Access, 6*, 11101–11111. https://doi.org/10.1109/ACCESS.2018.2803439
64. Sruthi, M., & Kavitha, B. R. (2016). A survey on Iot platform. *International Journal of Scientific Research and Modern Education (IJSRME) ISSN (online), I*(I), 2455–5630.
65. Lin, J. C. W., & Yeh, K. H. (2021). Security and privacy techniques in IoT environment. *Sensors (Switzerland), 21*(1), 1–5. https://doi.org/10.3390/s21010001
66. Networks, S. (2021). Sensor networks. pp. 1–19.
67. Gautam, S., Malik, A., Singh, N., & Kumar, S. (2019). Recent advances and countermeasures against various attacks in IoT environment. In *2nd Int. Conf. Signal Process. Commun. ICSPC 2019—Proc,* pp. 315–319. doi: https://doi.org/10.1109/ICSPC46172.2019.8976527.
68. Bostami, B., Ahmed, M., & Choudhury, S. (2019). False data injection attacks in internet of things. In *Performability in internet of things* (pp. 47–58). Cham: Springer. https://doi.org/10.1007/978-3-319-93557-7_4.
69. Lv, Z. (2020). Security of internet of things edge devices. *Software: Practice and Experience*. https://doi.org/10.1002/spe.2806
70. Standaert, F. X. (2010). Introduction to side-channel attacks. In: I. Verbauwhede (Eds.), Secure integrated circuits and systems. Integrated Circuits and Systems. Boston, MA: Springer. https://doi.org/10.1007/978-0-387-71829-3_2.
71. Mahalakshmi, G., Nadu, T., & Nadu, T. (2018). Denial of sleep attack detection using mobile agent in wireless sensor. *International Journal for Research Trends and Innovation, 3*(5), 139–149.
72. Kim, H., Kang, E., Broman, D., & Lee, E. A. (2020). Resilient authentication and authorization for the internet of things (IoT) using edge computing. *ACM Trans. Internet Things, 1*(1), 1–27. https://doi.org/10.1145/3375837
73. Čekerevac, Z., Dvorak, Z., Prigoda, L., & Čekerevac, P. (2017). Internet of things and the man-in-the-middle attacks–security and economic risks. *MEST J, 5*(2), 15–25. https://doi.org/10.12709/mest.05.05.02.03
74. Gupta, K. S., & Jayant, K. P. (2019). A review study on phishing attack techniques for protecting the attacks. *Globus-An International Journal of Management and IT, 10*(2), 22–25.
75. Singh, K. J., & Kapoor, D. S. (2017). Create your own internet of things: A survey of IoT platforms. *IEEE Consumer Electronics Magazine, 6*(2), 57–68. https://doi.org/10.1109/MCE.2016.2640718
76. Boo, E. S., Raza, S., Höglund, J., & Ko, J. G. (2019). Towards supporting IoT device storage and network security using DTLs. In *MobiSys 2019—Proc. 17th Annu. Int. Conf. Mob. Syst. Appl. Serv,* pp. 570–571. doi: https://doi.org/10.1145/3307334.3328630.
77. Ravi, N., & Shalinie, S. M. (2020). Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. *IEEE Internet of Things Journal, 7*(4), 3559–3570. https://doi.org/10.1109/JIOT.2020.2973176
78. Quasim, M. T. (2021). Challenges and applications of internet of things (IoT) in Saudi Arabia.
79. Zolanvari, M., Teixeira, M. A., Gupta, L., Khan, K. M., & Jain, R. (2019). Machine learning-based network vulnerability analysis of industrial internet of things. *IEEE Internet of Things Journal, 6*(4), 6822–6834. https://doi.org/10.1109/JIOT.2019.2912022
80. Li, W., Logenthiran, T., Phan, V. T., & Woo, W. L. (2019). A novel smart energy theft system (SETS) for IoT-based smart home. *IEEE Internet of Things Journal, 6*(3), 5531–5539. https://doi.org/10.1109/JIOT.2019.2903281
81. Mahmoud, C., & Aouag, S. (2019). Security for internet of things: A state of the art on existing protocols and open research issues. In *Proceedings of the 9th international conference on information systems and technologies* (pp. 1–6). https://doi.org/10.1145/3361570.3361622.
82. Gupta, H., & Van Oorschot, P. C. (2019). Onboarding and software update architecture for IoT devices. In *2019 17th Int. Conf. Privacy, Secur. Trust. PST 2019—Proc*. doi: https://doi.org/10.1109/PST47121.2019.8949023.
83. Hind, M., Noura, O., Amine, K. M., & Sanae, M. (2020). Internet of things: Classification of attacks using CTM method. In *ACM Int. Conf. Proceeding Ser*. doi: https://doi.org/10.1145/3386723.3387876.
84. Ghosh, A., Chakraborty, D., & Law, A. (2018). Artificial intelligence in Internet of things. *CAAI Transactions on Intelligence Technology, 3*(4), 208–218. https://doi.org/10.1049/trit.2018.1008
85. Samie, F., Bauer, L., & Henkel, J. (2019). From cloud down to things: An overview of machine learning in internet of things. *IEEE Internet of Things Journal, 6*(3), 4921–4934. https://doi.org/10.1109/JIOT.2019.2893866

86. De Lima Filho, F. S., Silveira, F. A. F., De Medeiros Brito Junior, A., Vargas-Solar, G., & Silveira, L. F. (2019). Smart detection: An online approach for DoS/DDoS attack detection using machine learning. *Security and Communication Networks*. https://doi.org/10.1155/2019/1574749
87. Nguyen, S. N., Nguyen, V. Q., Choi, J., & Kim, K. (2018). Design and implementation of intrusion detection system using convolutional neural network for DoS detection. In *ACM Int. Conf. Proceeding Ser*, pp. 34–38. doi: https://doi.org/10.1145/3184066.3184089.
88. Haripriya, A. P., & Kulothungan, K. (2019). Secure-MQTT: An efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things. *EURASIP Journal on Wireless Communications and Networking*. https://doi.org/10.1186/s13638-019-1402-8
89. Ying, X., Mazer, J., Bernieri, G., Conti, M., Bushnell, L., & Poovendran, R. (2019). Detecting ADS-B spoofing attacks using deep neural networks. In *2019 IEEE Conf. Commun. Netw. Secur. CNS 2019*, pp. 187–195. doi: https://doi.org/10.1109/CNS.2019.8802732.
90. Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2020). DL-Droid: Deep learning based android malware detection using real devices. *Computers & Security, 89*, 101663. https://doi.org/10.1016/j.cose.2019.101663
91. Čech, P., Lokoč, J., & Silva, Y. N. (2020). Pivot-based approximate k-NN similarity joins for big high-dimensional data. *Information Systems, 87*, 101410. https://doi.org/10.1016/j.is.2019.06.006
92. Xu, X., Zhang, Y., Tang, M., Gu, H., Yan, S., & Yang, J. (2019). Emotion recognition based on double tree complex wavelet transform and machine learning in internet of things. *IEEE Access, 7*, 154114–154120. https://doi.org/10.1109/ACCESS.2019.2948884
93. Xu, Y., Xia, J., Wu, H., & Fan, L. (2019). Q-learning based physical-layer secure game against multiagent attacks. *IEEE Access, 7*, 49212–49222. https://doi.org/10.1109/ACCESS.2019.2910272
94. Kim, M. (2019). Game theoretic approach of eavesdropping attack in millimeter-wave-based WPANs with directional antennas. *Wireless Networks, 25*(6), 3205–3222. https://doi.org/10.1007/s11276-018-1713-4
95. Hachimi, M., Kaddoum, G., Gagnon, G. & Illy, P. (2020). Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5G cloud radio access networks. In *2020 international symposium on networks, computers and communications (ISNCC)*. IEEE.
96. Xu, Y., Lei, M., Li, M., Zhao, M., & Hu, B. (2019). A new anti-jamming strategy based on deep reinforcement learning for MANET. In *IEEE Veh. Technol. Conf*, vol. 2019-April, pp. 1–5. doi: https://doi.org/10.1109/VTCSpring.2019.8746494.
97. Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine learning for security and the internet of things: The good, the bad, and the ugly. *IEEE Access, 7*, 158126–158147. https://doi.org/10.1109/ACCESS.2019.2948912
98. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy Challenges. *Internet of Things, 8*, 100107. https://doi.org/10.1016/j.iot.2019.100107
99. Raj, A., Maji, K., & Shetty, S. D. (2021). Ethereum for internet of things security. *Multimedia Tools and Applications, 80*(12), 18901–18915.
100. Atlam, H. F., & Wills, G. B. (2019). Technical aspects of blockchain and IoT. In *Advances in computers* (vol. 115, pp. 1–39). Elsevier.
101. Ali, Samad, et al. (2020). 6G white paper on machine learning in wireless communication networks. arXiv preprint arXiv:2004.13875.
102. Shabandri, B., & Maheshwari, P. (2019). Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle. In *2019 6th Int. Conf. Signal Process. Integr. Networks, SPIN 2019*, no. September 2016, pp. 1069–1075. doi: https://doi.org/10.1109/SPIN.2019.8711591.
103. Pirmagomedov, R., & Koucheryavy, Y. (2019). IoT technologies for augmented human: A survey. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100120
104. Zantalis, F., Koulouras, G., Karabetsos, S., & Kandris, D. (2019). A review of machine learning and IoT in smart transportation. *Future Internet, 11*(4), 1–23. https://doi.org/10.3390/FI11040094
105. Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: A contemporary survey. *Wireless Personal Communications, 108*(1), 363–388. https://doi.org/10.1007/s11277-019-06407-w
106. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical Systems and Signal Processing, 135*, 106382. https://doi.org/10.1016/j.ymssp.2019.106382
107. Lin, F., et al. (2019). Survey on blockchain for internet of things. *Journal of Internet Services and Information Security, 9*(2), 1–30. https://doi.org/10.22667/JISIS.2019.05.31.001

108. Rathee, G., Garg, S., Kaddoum, G., & Choi, B. J. (2020). A decision-making model for securing IoT devices in smart industries. *IEEE Transactions on Industrial Informatics, 3203*(c), 1–1. https://doi.org/10.1109/tii.2020.3005252
109. Balliu, M., Bastys, I., & Sabelfeld, A. (2019). Securing IoT Apps. *IEEE Security and Privacy, 17*(5), 22–29. https://doi.org/10.1109/MSEC.2019.2914190
110. Sharma, B. B., & Kumar, N. (2021). Iot-based intelligent irrigation system for paddy crop using an internet-controlled water pump. *International Journal of Agricultural and Environmental Information Systems, 12*(1), 21–36. https://doi.org/10.4018/IJAEIS.20210101.oa2
111. Ahmad, A., Cuomo, S., Wu, W., & Jeon, G. (2019). Intelligent algorithms and standards for interoperability in internet of things. *Future Generation Computer Systems, 92*, 1187–1191. https://doi.org/10.1016/j.future.2018.11.015
112. Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications, 24*(3), 796–809. https://doi.org/10.1007/s11036-018-1089-9
113. Vermesan, O. 2018. *Advancing IoT platforms interoperability*.
114. Oktian, Y. E., Witanto, E. N., & Lee, S.-G. (2021). A conceptual architecture in decentralizing computing, storage, and networking aspect of IoT infrastructure. *IoT, 2*(2), 205–221. https://doi.org/10.3390/iot2020011
115. Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in internet of things: Features, techniques and research challenges. *International Journal of Computational Intelligence Research, 13*(7), 1617–1627.
116. Ryan, P., & Watson, R. (2017). Research challenges for the internet of things: What role can or play? *Systems, 5*(1), 24.
117. Badawy, M. M., Ali, Z. H., & Ali, H. A. (2019). QoS provisioning framework for service-oriented internet of things (IoT). *Cluster Computing*. https://doi.org/10.1007/s10586-019-02945-x
118. Raj, J. S., & Basar, A. (2019). Qos optimization of energy efficient routing in Iot wireless sensor networks. *Journal of ISMAC, 01*(01), 12–23. https://doi.org/10.36548/jismac.2019.1.002
119. Singh, M., Baranwal, G., & Tripathi, A. K. (2020). QoS-aware selection of IoT-based service. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-020-04601-8
120. Zeadally, S., Shaikh, F. K., Talpur, A., & Sheng, Q. Z. (2020). Design architectures for energy harvesting in the internet of things. *Renewable and Sustainable Energy Reviews, 128*(May), 109901. https://doi.org/10.1016/j.rser.2020.109901
121. Atlam, H. F., & Wills, G. B. (2020). *IoT security, privacy, safety and ethics*. Springer International Publishing.

Aparna Raj is a research scholar at Dept. of Computer Science, Bits Pilani, Dubai campus. She has received her M.Tech. (Computer and Communication Engineering) and B.Tech. (Information Technology) from Karunya University and Calicut University, India in 2010 and 2012 respectively. Her research interests are in the areas of IoT and Machine Learning.

Dr. Sujala D. Shetty is currently working as Associate Professor in Dept. of Computer Science BITS Pilani, Dubai Campus. She joined the dept. in September 2002. She received her B.E. degree in Computer Science from Bangalore Institute of Technology and Master's degree in Computer Science from Manipal Institute of Technology in 1994 and 2002 respectively. She received her Ph.D. from Bits Pilani, Rajasthan, India, in 2010. She has 23 years of teaching experience. Previously she has worked in Manipal Institute of Technology. She has guided many thesis, dissertations and projects undertaken by the undergraduate and post graduate students. She has handled classes for both undergraduate, postgraduate and distance education students. Her research areas are Big Data, Artificial Intelligence, IoT, Web Services, and Network Security. She has successfully guided one PhD student and is currently guiding two PhD students. She is the faculty advisor for ACM and ACM-W. She is instrumental in starting ACM-W in 2019. ACM-W is the Women in Tech arm of ACM. ACM-W at BITS Dubai was the first such chapter for women in U.A.E. Also, ACM chapter under her leadership was awarded Student Chapter Excellence Award for Outstanding Chapter Activities by ACM headquarters, New York in April 2020.