Internet of Things: Basic Concepts and Decorum of Smart Services

Aradhana Behura, Suneeta Satpathy, Sachi Nandan Mohanty, and Jyotir Moy Chatterjee

1 Introduction

Internet of things (IoT) is a term used to describe an environment where billions of objects, constrained in terms of resources ("things"), are connected to the Internet and interacting autonomously. With so many objects connected in IoT solutions, the environment in which they are placed becomes smarter. A software, called middleware, plays a key role since it is responsible for most of the intelligence in IoT, integrating data from devices, allowing them to communicate and make decisions based on collected data. Then, considering requirements of IoT platforms, a reference architecture model for IoT middleware is analyzed, detailing the best operation approaches of each proposed module, as well as proposes basic security features for this type of software. This chapter elaborates on a systematic review of the related literature, exploring the differences between the current Internet and IoT-based systems, presenting a deep discussion of the challenges and future perspectives on IoT middleware. Finally, it highlights the difficulties for achieving and enforcing a universal standard. Thus, it is concluded that middleware plays a crucial role in IoT

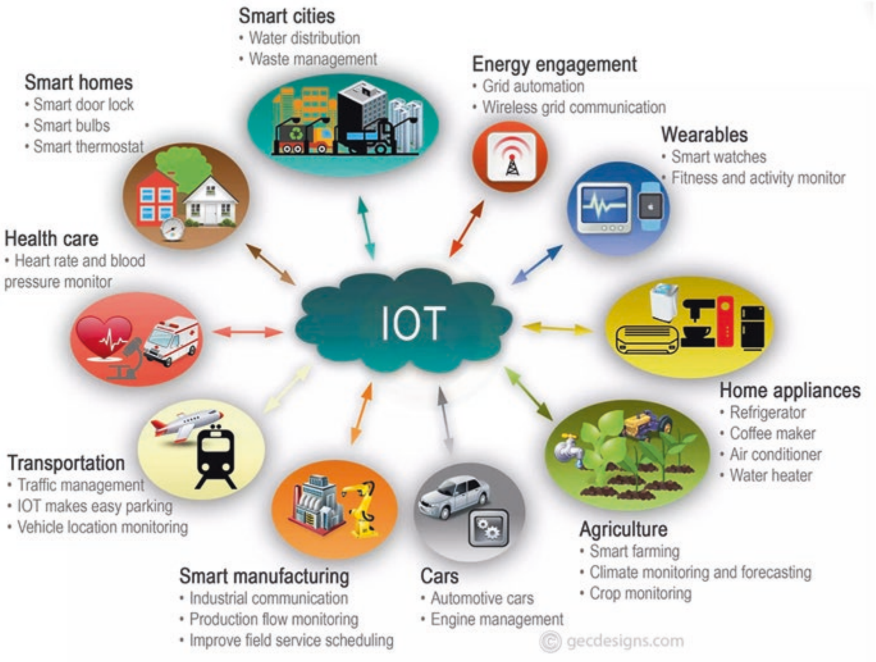
A. Behura (✉)
Gandhi Institute For Technological Advancement, Bhubaneswar, Odisha, India
e-mail: anuradha_cse@gita.edu.in

S. Satpathy
Sri Sri University, Cuttack, Odisha, India

S. N. Mohanty
Vardhaman Engineering College (Autonomous), Hyderabad, India

J. M. Chatterjee
Lord Buddha Education Foundation, Kathmandu, Nepal

S. Nandan Mohanty et al. (eds.), *Internet of Things and Its Applications*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-77528-5_1



(a): Application Of IOT in modern age

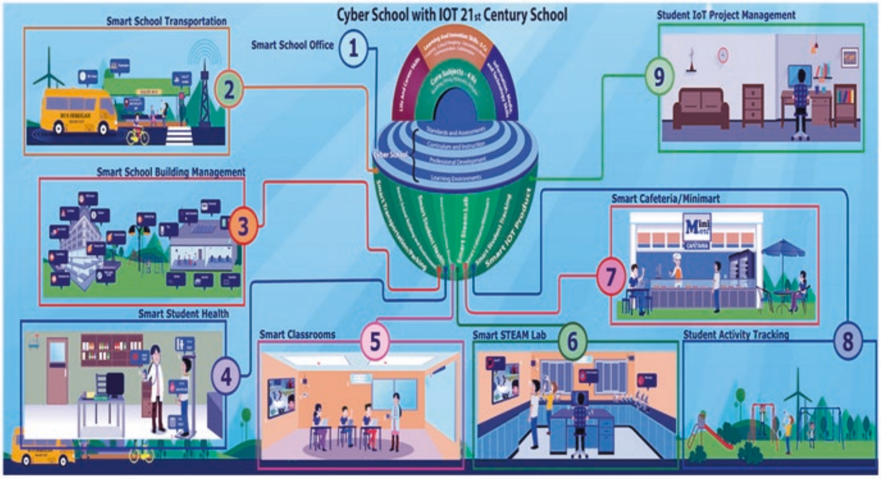
Fig. 1 Application of IoT in modern age

solutions, and the proposed architectural approach can be used as a reference model for IoT middleware. Figs. 1 and 2 describe the IoT methodology.

- **Security and Surveillance**
WSNs are essential components of military command and power, message passing, computing, intellect power, monitoring, attacking systems and observations. The sensor nodes and devices guarantee observation of enemy, battleground monitoring, conflict destruction evaluation, attacking, and nuclear, botanical, and enzymatic blast discovery techniques.

- **Environmental Monitoring**
Several WSN implementations in earth science research are covered by environmental sensor networks, associating sensing volcanoes, glaciers, forests, and oceans. To recognize slight soil movements and modifications, a landslide detection system utilizes WSN in several parameters that happen before or during landslides.

- **Health Applications**
To observe patient's physiological data and to trace and detect patients to manage drug administration and doctor's sensor networks are associated in modern health care centers. Different uses are found in glucose level detection, organ scanning, general health monitoring, and cancer detection. Inside a human body implanting



(b): Role of IOT in 21st Century

Fig. 2 Role of IoT in the twenty-first century

wireless biomedical sensors is promising though great challenges such as ultra-safety, security, and minimal maintainability of the system are associated.

- **Industrial Applications**

For machinery Condition-Based Maintenance (CBM) WSNs are enlarged as they guarantee high cost savings and allow new works. Through wireless sensors, earlier inaccessible locality, rotating machinery, dangerous or regulated regions, and mobile assets are reached.

- **Structural Monitoring**

Wireless sensors monitors moves inside premises, framework such as flyovers, cross over, tunnels and hills, monitor assets remotely, permitting engineering works without expensive site visits.

We learn various levels from Figs. 3, 4, 5, 6, 7 and 8.

Any technology available today has not reached its 100 % capability. It always has a gap to go. So, we can say that *Internet of things* has a significant technology in a world that can help other technologies reach their accuracy and complete 100 % capability as well.

Let’s take a look over the major advantages and disadvantages of Internet of things.

Advantages of IoT

Internet of things facilitates several advantages in day-to-day life in the business sector. Some of its benefits are given below:

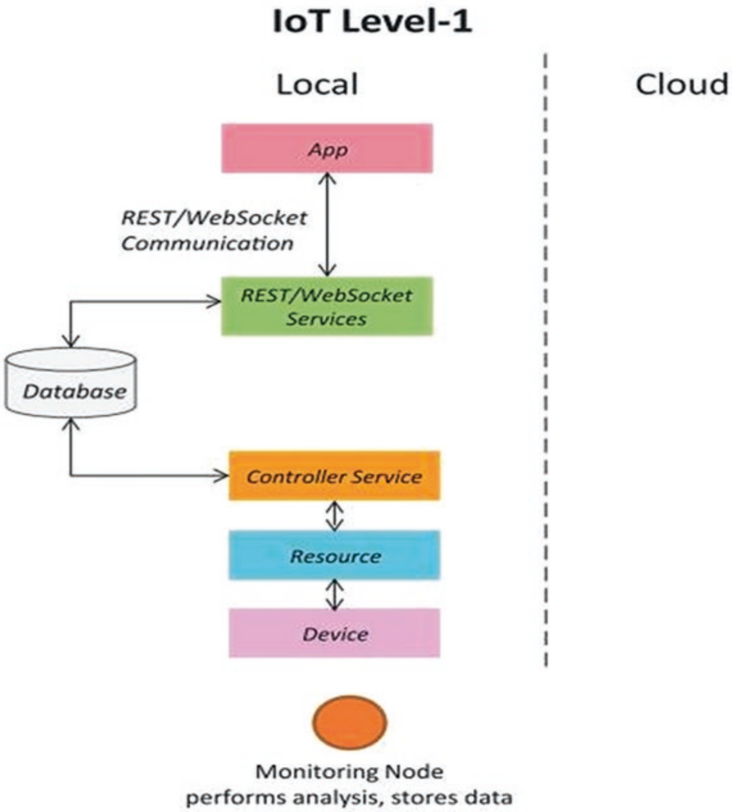


Fig. 3 Level 1 architecture of IoT

- **Efficient resource utilization:** If we know the functionality and the way how each device works, we definitely increase the efficient resource utilization as well as monitor natural resources.
- **Minimize human effort:** As devices of IoT interact and communicate with each other and do a lot of tasks for us, then they minimize human effort.
- **Save time:** As it reduces human effort, then it definitely saves out time. Time is the primary factor which can save through IoT platform.
- **Enhance data collection**
- **Improve security:** Now, if we have a system where all these things are interconnected, then we can make the system more secure and efficient.

Disadvantages of IoT

As the Internet of things facilitates a set of benefits, it also creates a significant set of challenges. Some of the IoT challenges are given below:

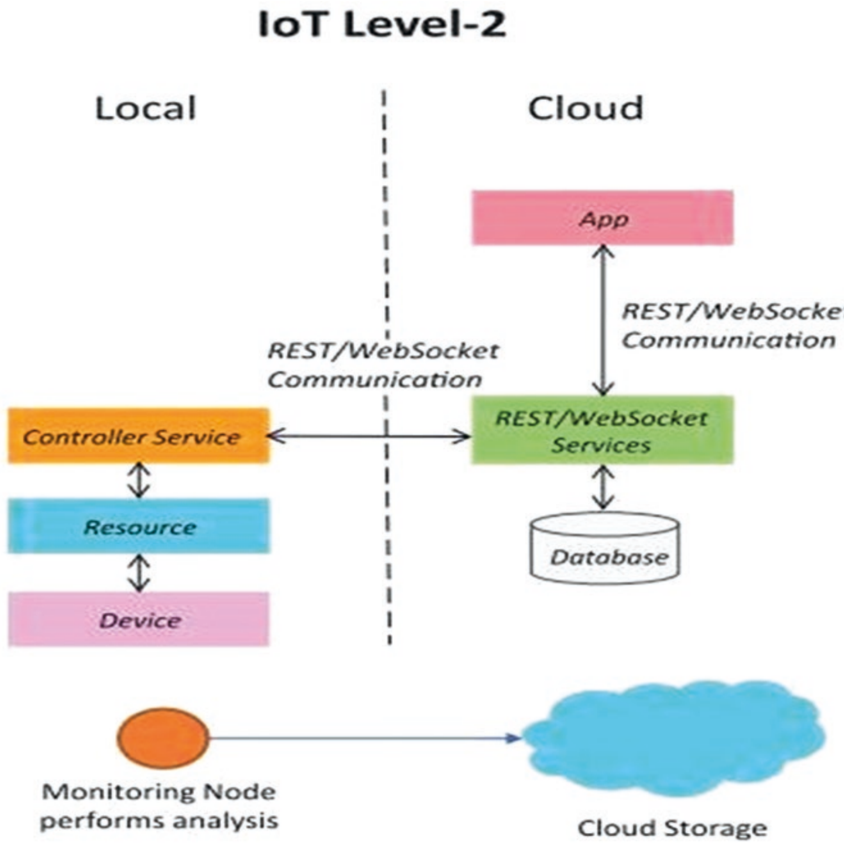


Fig. 4 IoT level-2 architecture

- **Security:** As IoT systems are interconnected and communicate over networks, the system offers little control despite any security measures, and it can lead to various kinds of network attacks.
- **Privacy:** Even without the active participation of the user, the IoT system provides substantial personal data in maximum detail.
- **Complexity:** The designing, developing, maintaining, and enabling of large technologies to IoT system are quite complicated.

1.1 Level of IoT

- The level-1 system of IoT has a single node/device that performs sensing and/or actuation, stores data, performs analysis, and hosts the application. These systems are suitable for modelling low-cost and low-complexity solutions where the

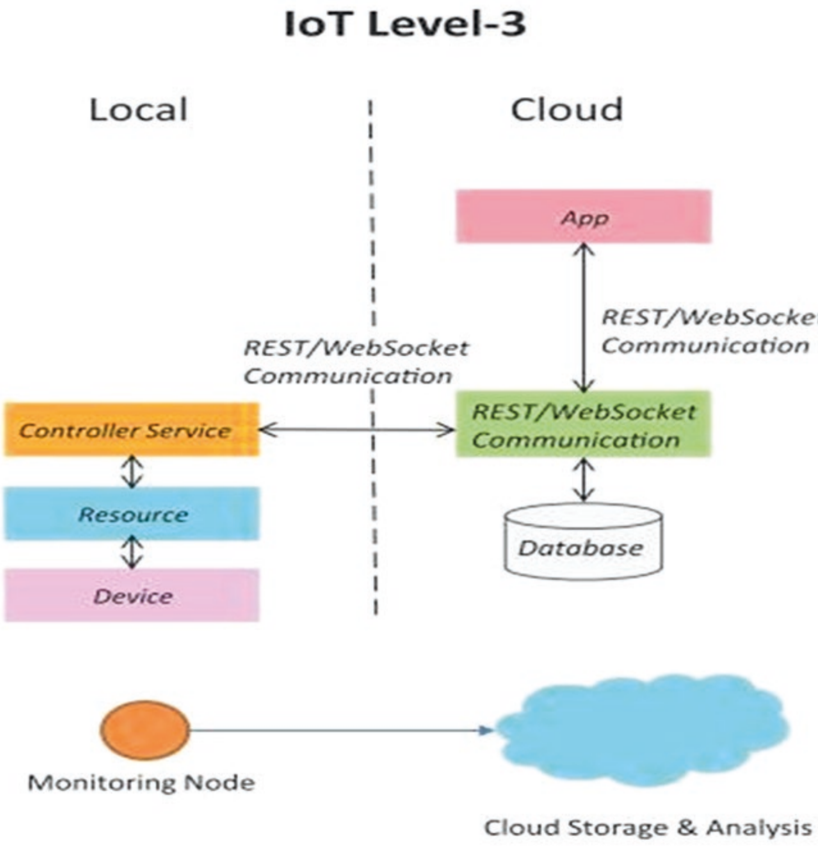


Fig. 5 IoT level-3 architecture

data involved is not big and the analysis requirements are not computationally intensive.

- A level-2 IoT system has a single node that performs sensing and/or actuation and local analysis.
- Data is stored in the cloud and application is usually cloud based.
- Level-2 IoT systems are suitable for solutions where the data involved is big; however, the primary analysis requirement is not computationally intensive and can be done locally itself.
- A level-3 IoT system has a single node. Data is stored and analyzed in the cloud, and application is cloud based.
- Level-3 IoT systems are suitable for solutions where the data involved is big and the analysis requirements are computationally intensive.
- Level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud based.

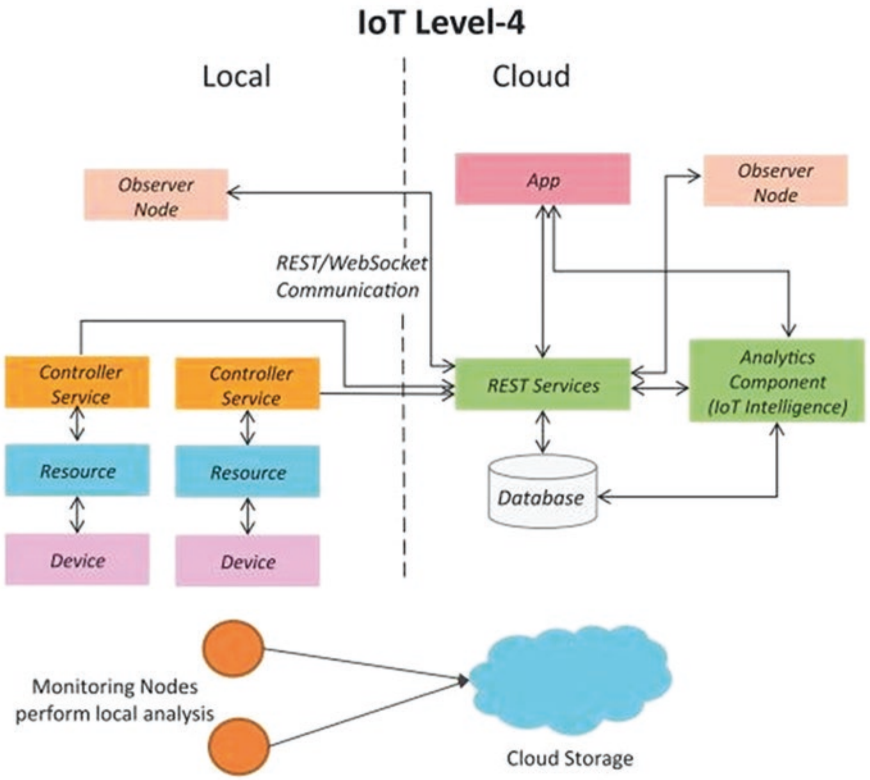


Fig. 6 IoT level-4 architecture

- This contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices.
- These systems are suitable for solutions where multiple nodes are required, the data involved is big, and the analysis requirements are computationally intensive.
- A level-5 IoT system has multiple end nodes and one coordinator node.
- The end nodes perform sensing and/or actuation.
- Coordinator node collects data from the end nodes and sends to the cloud.
- Data is stored and analyzed in the cloud and application is cloud-based.
- Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive.
- A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud.
- Data is stored in the cloud and application is cloud based.
- The analytics component analyzes the data and stores the results in the cloud database.
- The results are visualized with the cloud-based application.

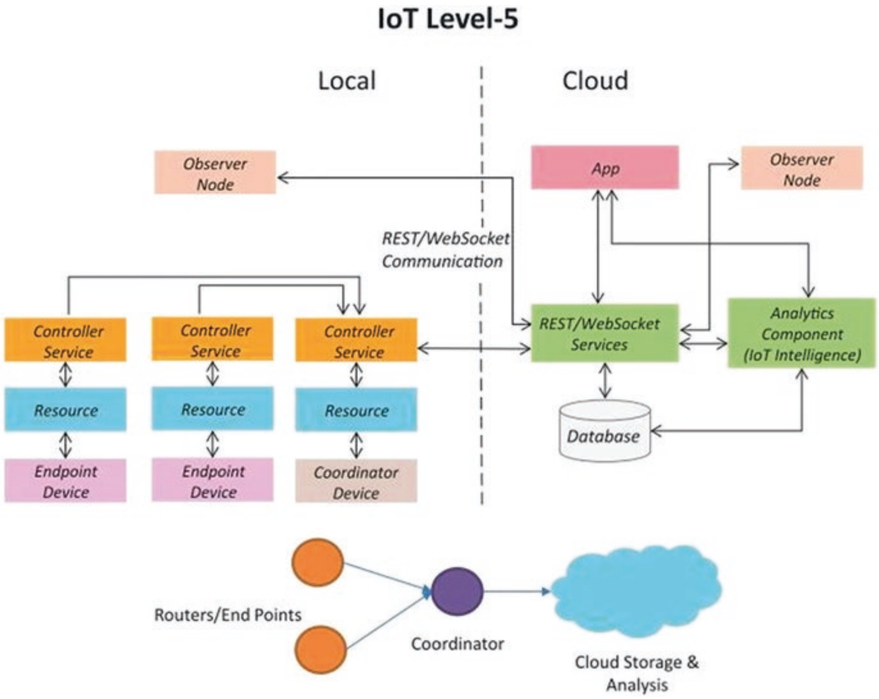


Fig. 7 IoT level-5 architecture

- The centralized controller is aware of the status of all the end nodes and sends control commands to the nodes.

A dynamic network infrastructure with self-configuring capabilities is based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network, often communicating data associated with users and their environments.

The "things" in IoT usually refer to IoT devices which have unique identities and can perform remote sensing, actuating, and monitoring capabilities.

- IoT devices can:
  - Exchange data with other connected devices and applications (directly or indirectly)
  - Collect data from other devices and process the data locally
  - Send the data to centralized servers or cloud-based application back ends for processing the data
  - Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints

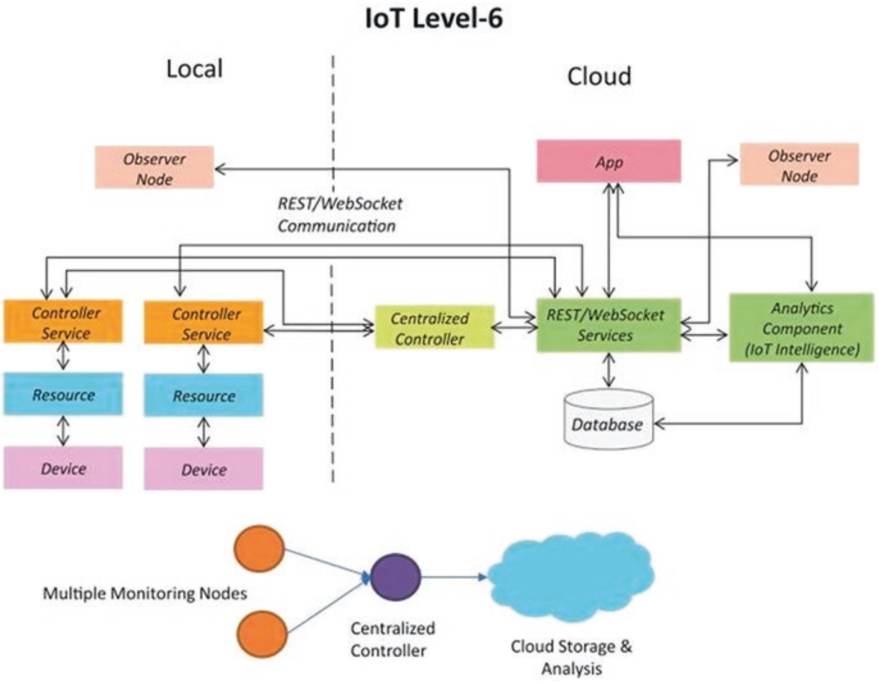


Fig. 8 IoT level-6 architecture

- Logical design of an IoT system refers to an abstract representation of entities and processes without going into the low-level specifics of the implementation.
- An IoT system comprises a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication, and management (Fig. 9).

The policy of IoT-based smart farming made by different countries for standardization also has been discussed:

- Then the challenges that come to improve IoT-based smart farming

1.2 Discussion of Major Components for IoT-Based Smart Farming

Major components of IoT-based smart farming:

- Software used in AI
- Control unit connectivity
- Auto mode

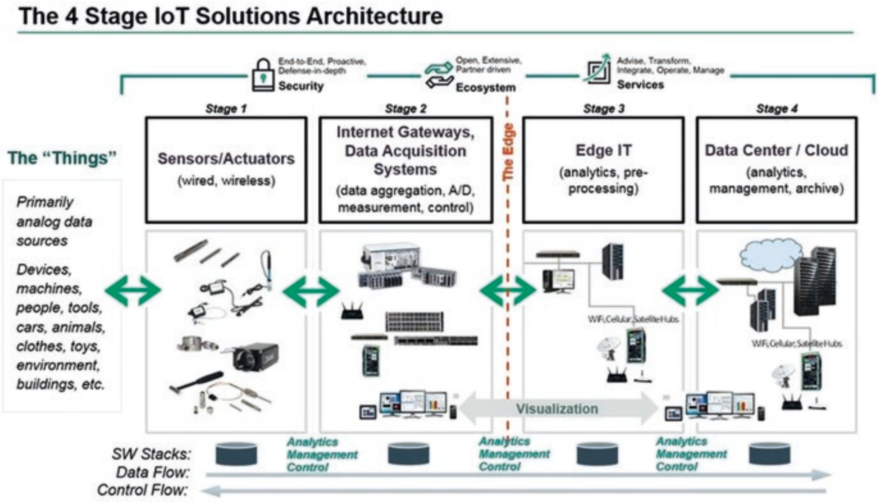

The 4 Stage IoT Solutions Architecture
End-to-End, Proactive, Defense-in-depth
Security
Open, Extensive, Partner driven
Ecosystem
Advise, Transform, Integrate, Operate, Manage
Services
Stage 1
Stage 2
Stage 3
Stage 4
The "Things"
Primarily analog data sources
Devices, machines, people, tools, cars, animals, clothes, toys, environment, buildings, etc.
Sensors/Actuators
(wired, wireless)
Internet Gateways, Data Acquisition Systems
(data aggregation, A/D, measurement, control)
The Edge
Edge IT
(analytics, pre-processing)
Data Center / Cloud
(analytics, management, archive)
WiFi,Cellular,SatelliteHubs
WiFi,Cellular,SatelliteHubs
Visualization
SW Stacks:
Data Flow:
Control Flow:
Analytics
Management
Control
Analytics
Management
Control
Analytics
Management
Control

Fig. 9 IoT architecture

Automatically sprays the affected area with the help of four latitudes and longitudes

- Manual mode
  Manually instructs the sprayer (right, left, and both) to cover only the affected area Communication between device is too much fast.
  The driver gets full access to all the files with Bluetooth Low Energy (BLE) technology providing excellent communication between devices within close proximity.

2 IoT's Role in Application

For observing various environmental situations, a WSN includes numerous distributed sensors like motion, sound, pressure, temperature, and images. For further mandatory measures in WSNs, data sensation by this sensor is forwarded to the fusion center [8, 56, 9, 10]. Communication of data is endangered to various critical situations to the base station [21–24]. For example, when the sender transmits the data from source node to the destination node to a hacker, it won't be difficult to change the original message which the sensor node received; thus, WSN is not a closed system where there are rare reliability considerations such as wires configuration. Judgement considered in the ground of the message is not accurate when the fusion center gets in current data [12–20]. Nowadays, WSN is utilized as a process in business and industrial implementations [51–55].

Here we will discuss about various types of anomolies in the field of WSN. In this transmission, all nodes must link with different nodes and also attach with one sensor, each sensor network joining with faithful communication different ports situated in the network. It includes radio transceiver and intent antenna operations situated in the process application and this antenna managed by the process micro-controller inserted to that specific process transmission in wireless sensor network application process.

Basically, there are four main features and some optional elements in a wireless sensor node.

- Specific detecting part is inhabited by each sensor node that accommodates an A/D converter, and one and various sensors are employed for data acquisition.
- Memory is used for storing output where for another information every sensor node has a processor, more storage capacity, and a micro-controller.
- For transmission of data using wireless medium, an RF unit is utilized.
- A particular unit for supplying energy to detectors.
- Technique to locate the position conviction.

2.1 WSNs

By taking the help of MEMS, WSNs obtained worldwide attention which guaranteed smart sensor development. Smart sensors have realistic processing and computing resources [49, 48, 26].

Detector nodes detect, estimate, and collect message in surroundings. According to a local commitment process, they broadcast detected information. WSNs incorporate structured and unstructured types. An unstructured WSN has a heavy sensor node cluster and is utilized in an ad hoc manner [27–29, 47]. WSNs are recently utilized in below the earth and submarine. According to surroundings, detectors have varying problems with some restrictions. Some varieties of wireless sensor networks are multimedia, terrestrial, underground, mobile, and underwater. Whether in temporary or arranged earlier in temporary network, detectors fall in a target area arbitrarily. Many deployment models are optimal placement, grid placement and in two dimensional and three-dimensional view planes [30, 31].

In terrestrial WSNs, secure data transmission in heavy surrounding is very much essential. Terrestrial sensor nodes deliver data packet to the base station (BS) [46, 32, 33, 45, 34, 35]. Possessing little battery power and rare facility to recharge, such as solar cells, terrestrial sensor nodes have a secondary energy source. Sensor nodes must preserve energy. Through multi-hop optimal routing power for a terrestrial WSN is preserved, in-network data aggregation, decreasing delays, eliminating data concurrency, very small data communication range and utilizing very small duty-cycle operations [25, 50].

Underground WSNs have several sensor nodes to judge underground situations hiding underground or in caves or mines [44, 36, 37]. To send message from detector point to central station large number of sink point situated on the earth. Concerning utilization and conservation of appliances, a wireless sensor network is costlier than a terrestrial wireless sensor network. For secure transmission towards lands, stones, dilute substance and inorganic materials holds below earth detector points are more costly materials and it should prefer. Underground WSN utilize power, planning, and cost considerations such as terrestrial WSNs. For underground WSNs, efficiency is very much essential. Underground sensor nodes have very less battery energy as compared to terrestrial WSNs and when installed are very difficult to recharge or restore a battery. The important motive is to develop a network efficiency for preserving power that is feasible through secure data transmission protocols.

2.2 Characteristics of the Wireless Sensor Network

WSNs have various important features such as little energy, very small-scale sensor nodes, energy harvesting, node collapse, node portability, strong environment, recognized incidents versatility, node diversity, active network topology, large-scale deployment, and abandoned functions [38].

WSNs' important qualities are:

2.1.1.1. Utilizing batteries or energy harvesting energy utilization restrictions for nodes
2.1.1.2. Potentiality to control with the node collapses
2.1.1.3. Portability of nodes
2.1.1.4. Active configuration of a network
2.1.1.5. Transmission collapses
2.1.1.6. Diversity of position
2.1.1.7. Quality of resistance to a severe atmospheric situation
2.1.1.8. Very easily accessible
2.1.1.9. Abandoned functions
2.1.1.10. Energy utilization

2.3 Wireless Architecture

This architecture contains five layers which are described below:

Physical layer: Decreasing the path loss consequence and shading an enlarged authenticity is the goal of this layer. This layer enables link setup, bit transmission channel, encoding, frequency sensing, signal creation, and inflation.

Data link layer: This layer guarantees interoperability in inter-node connection. It can manage error recognition, multiplexing, continuous data delivery, and avoidance of packet loss.

Network layer: The finest route for secure routing is established by this layer. This is in control of forwarding a message from a particular point to base station,

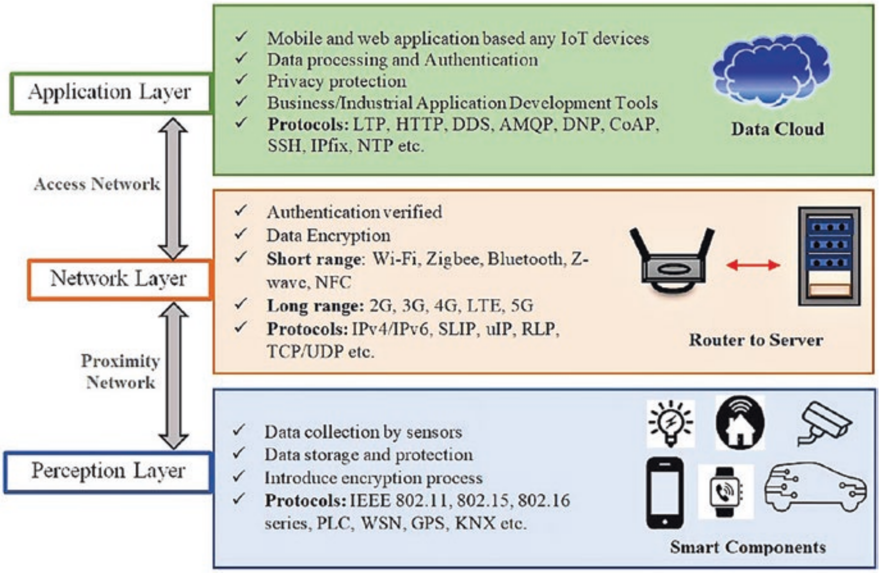

Application Layer
Access Network
Network Layer
Proximity Network
Perception Layer
✓ Mobile and web application based any IoT devices
✓ Data processing and Authentication
✓ Privacy protection
✓ Business/Industrial Application Development Tools
✓ Protocols: LTP, HTTP, DDS, AMQP, DNP, CoAP, SSH, IPfix, NTP etc.
Data Cloud
✓ Authentication verified
✓ Data Encryption
✓ Short range: Wi-Fi, Zigbee, Bluetooth, Z-wave, NFC
✓ Long range: 2G, 3G, 4G, LTE, 5G
✓ Protocols: IPv4/IPv6, SLIP, uIP, RLP, TCP/UDP etc.
Router to Server
✓ Data collection by sensors
✓ Data storage and protection
✓ Introduce encryption process
✓ Protocols: IEEE 802.11, 802.15, 802.16 series, PLC, WSN, GPS, KNX etc.
Smart Components

Fig. 10 IoT level [57]

point to point, point to the Cluster Head, point to sink, and reverse. LEACH and PEGASIS protocols relate the techniques to consume power and to increase sensor life. WSNs utilize identity-related protocols for routing, LEACH offers cluster-based data delivery, and PEGASIS is a chain protocol. To generate an efficient routing protocol, in WSN, a network node performs as a router, and it utilizes transmission mechanism. By encryption and decryption techniques, efficient routing is secured.

Transport layer: This layer links data transmission with outer networks that are interrelated to sensor network of the Internet. It is the one of the challenging tasks in WSN.

Application Layer: By securing data transmission to lower layers, this layer offers complete output. For the application software to receive efficient results, it is responsible for management and data cluster and transmission. Security protocols in sensor networks (SPINS) enable data integrity, replay conservation, low cost, and semantic security (Fig. 10).

Various implementations are encouraged by WSNs: a few are revolutionary, whereas various are virtually necessary. The latter's applications are unbelievable target tracking; environment monitoring; oil, water, and gas monitoring; accurate farming; providing chain management; systematic health monitoring; transport facility; active volcano monitoring; healthcare application [39, 40]; below-ground mining; and human job monitoring.

2.4 *Network Topology Construction Phase with Efficient Processing*

The procedure of the application in wireless sensor networks is stopped with sensible data process which includes a way of communication in data transmission [41–43]. Data communication obtained from warehouse repository with sensible data broadcast with compatible data relative with compatible executions in all sensor exist in the wireless sensor network real time application process management executions. In this situation of data communication, we reach our goal for construction in wireless sensor network application development. We retrieve resources of the wireless sensor networks, various types of protocols and algorithms were evolved with relative data delivery situated in every node termination [4, 5, 11] (Fig. 11).

For each sensor nodes exist in the process transmission wireless networks control topology. We transmit data transmission in commercial technical development, in data delivery of the wireless sensor networks exist in the process communication based on the quality of the service and other features exist in the processing application development. Topology will be modified its structure every time in all data delivery with sensible data delivery exist in the wireless sensor network application process. In general, secure data delivery can be possible in wireless sensor application development but in those data, exist in the delivery process message broadcasting creates a misbehaving nodes packet dropping in sensible data delivery process. In given application processes, successful application of packet dropping is an

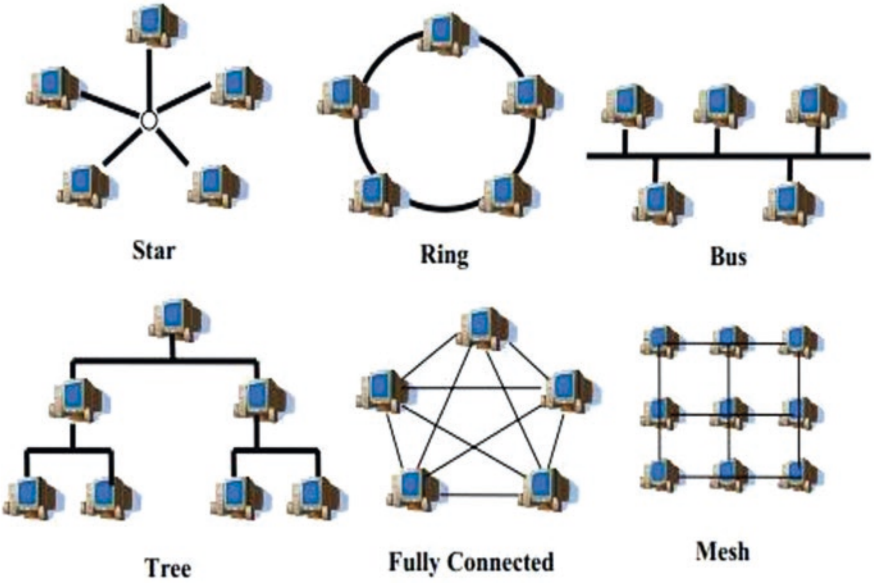


Fig. 11 Network topology construction phase with efficient processing

important issue. In this chapter, to recognize misbehaving nodes in wireless sensor network application processes, we suggest expansion of enhanced adaptive acknowledgement schema with sensible data delivery in process transmission of wireless sensor network application development processes. To protect the attacker from false acknowledgment packets, we enlarge this through digital signature.

2.5 IoT Agricultural Network Architecture

From the perspective of agricultural application architecture, it was found that current research are more concentrated on the gateway hardware, and the embedded gateway middleware application is relatively few on the one hand; on the other hand, the AIoT data sharing layer's research is seriously lacking; each application system usually sends the perceived data directly to the AIoT application layer; therefore, it is difficult to achieve the effect of further guiding to agricultural production for the lack of data mining and analysis. Finally, the chapter discussed on further research and application direction of the AIoT technology.

- **IoT Agricultural Platform**
  The IoT agriculture network includes both the analytics model and cloud model.
- **Big Data Analytics**
  Big data analytics largely involves collecting data from different sources, in a way that it becomes available to be consumed by analysts and deliver data products useful to IoT-based smart farming. The process of converting large amounts of unstructured raw data retrieved from different sources to a data product useful for smart farming forms the core of big data analytics. It also determines productivity and optimal cost analysis. IoT agricultural network platform is based on big data analytics. And this network consists of six components mainly:

- Farmer
- Farming experience
- Analysis of big data
- Monitoring and sensing
- Storage services
- Communication protocol and physical implementation

In IoT, this platform provides a backbone on information such as fertility, climate condition, how much moisture is present in the air, online crop monitoring, etc.

In recent years, we can say that agriculture is the backbone of India. Farmers select a large number of suitable crops, vegetables, and fruits. The plant plays a major role as main source of energy and livelihood. In this chapter, we discussed an IoT technology-assisted UAV (unmanned vehicle) procedure-based disease prediction system to identify the disease during its creation in the green ground. This system emphases on IoT with machine learning mechanisms to accomplish disease prediction process in green fields. Imagga cloud is used for the detection of affected leaf. The leaf can be detected by considering the highest confidence tag value as well as its threshold value. The IoT-supported UAV model is basically used to transfer many images to the Imagga cloud. This observes the ground at systematic time intervals by taking images from the field. In this chapter, a challenge has been prepared to display the affected leaf by taking the help of machine learning technique, so that the wastage of agricultural item can be minimized. The chapter prolonged to progress a computerized integrated system to monitor the rice during its production as well as its post-production activities in a better way. While some creature hosts may give their pathogens a steady scope of internal heat levels, plant pathogens are commonly significantly more presented to the components. Natural product infection will in general react to environmental change; however, various collaborations occur among host, pathogen, and potential vectors. At times, the activities of land administrators may likewise confuse elucidation of environmental change impacts. Some biological agents directly or indirectly affect the plant through plant diseases [34]. These biological agents are known as pathogens. Some common pathogens are viruses, bacteria, fungi, and nematodes. Besides these pathogens, some non-pathogenic disease may occur when pH, moisture, and climate are altered with respect to environment. From Fig. 18, we are able to know the role of UAV in agriculture.

3 Cloud and Fog Infrastructure for Data Security

Cloud computing infrastructure is composed up of many components such as storage, hardware, networking, and virtualization, each integrated with one another into a single architecture supporting various types of important operations. Proper security mechanism is required so that the intruder cannot alter any sensitive information (Fig. 12).

As cloud computing in agriculture continues to increase, so too will the number of questions about it.

Figure 1 describes a secure steganography-based fog as well as mobile edge computing environment. Basically, steganography consisted of two main processes, namely, embedding process and extracting process. At some point of the embedding method, watermark is embedded into the multimedia records (virtual records). The original digital data (multimedia content) will be slightly modified after embedding the watermark; this modified data is called watermarked data. At the same time as in extraction manner, this embedded watermark is extracted from the watermarked facts and recovers the original multimedia information. The extracted watermark is then compared with the authentic watermark; if the watermark is identical, it effects in authenticated data. During the transmission of the watermarked data over the public network through cloud or fog, attacker may tamper the data, and any modification in the data can be detected by comparing the extracted watermark with the original watermark. The proposed quantum steganography system ensures the authentication and security for fog cloud IoT users.

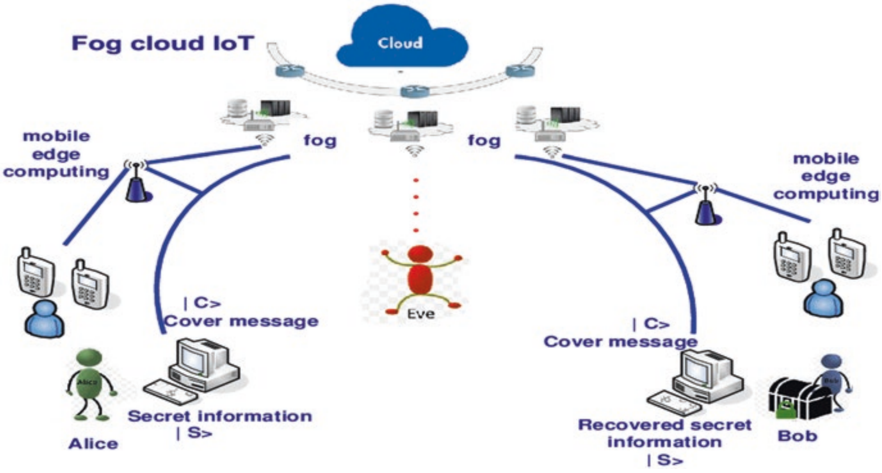


Fig. 12 Architecture of security system [2]

In this chapter, we discussed the role of Internet of things in smart healthcare through wireless body area network. There are many existing algorithms that prove better performance. Sensors (retina artificial arm chips) [6–8] inside the retina can be embedded to help one blind human being to see once more. For WBAN, the sufferers accompanied by heart disease [9], asthma, diabetes, Alzheimer's, Parkinson's, and so on can be performed. [10]. Inside conventional programs, there is a necessity for sufferers for staying inside hospital, yet WBAN confesses these sufferers for continuing through usual everyday schedule of them. It mitigates pharmaceutical work cost and also foundation cost. Biosensor nodes choose one route which has smallest distance towards sink node as well as absorbs small energy. We can integrate WBAN with cloud technology to improve efficiency, larger performances as well as utilities as well as greater reliability and so on, even so this will quiet inside its advance phase as well as might possess various oppositions as well as practical problems [22]. Thus, here we study dual sink technique utilizing clustering inside body area network. This is very important at improving duration of network with effectively using nodes battery lifetime. Here, we can get optimized result in terms of less collision, faster packet delivery rate, and less sensor node failure rate by using a nature-inspired algorithm. In the future, we can optimize [42, 43] by selecting efficient cluster head through the help of machine learning and Internet of things efficiently. We can learn about WBAN from Figs. 13, 14, 15, 16 and 17; Table 1)

- Efficient saturated information storing and retrieving: WSNs are visualized to give global sensation of data, reserve, and satisfy supplying facility in context with global computing. A growing saturated network saving information as well as recovery technique has been presented newly for the reason of secure data management. Therefore, large experimental attempts have been given in such a problem.

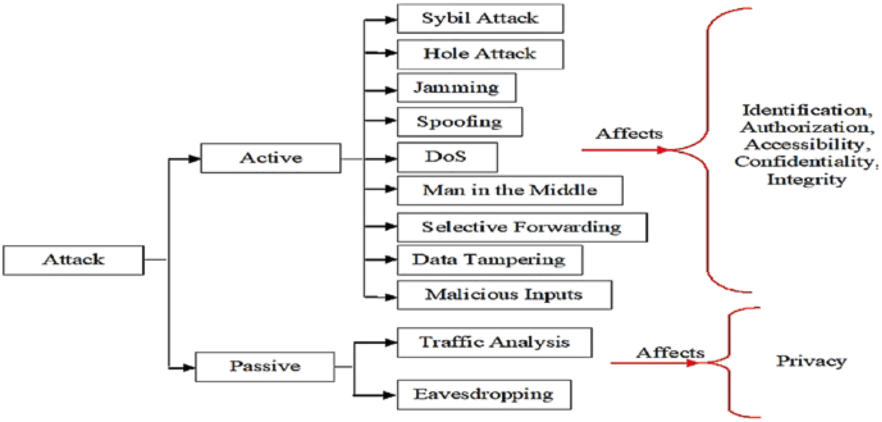


Fig. 13 Various types of attack

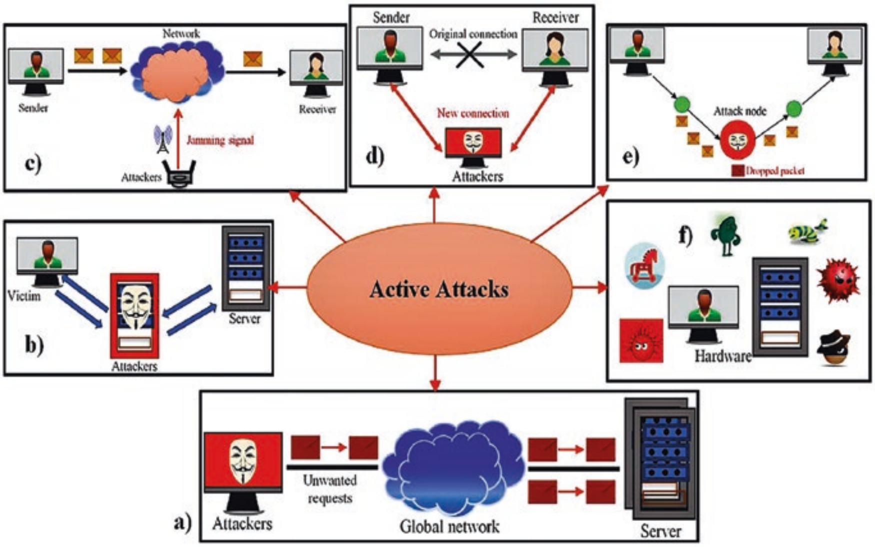
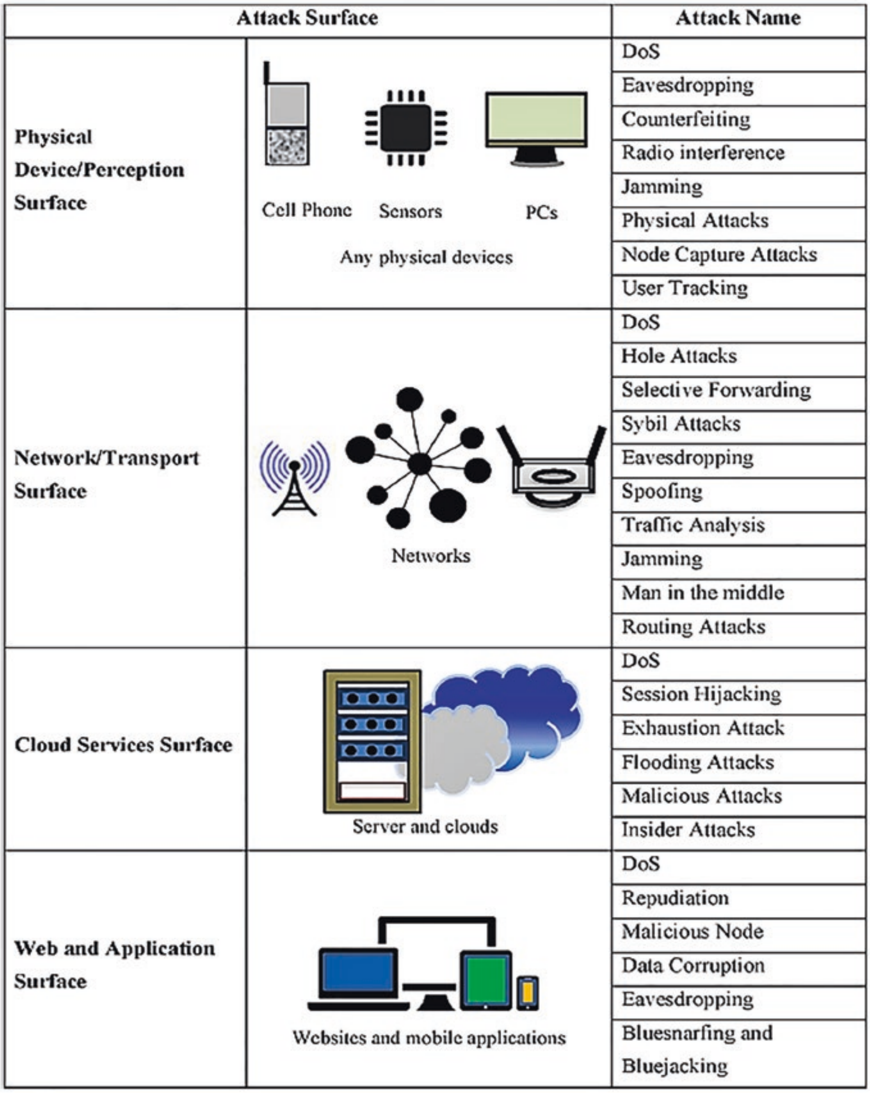


Fig. 14 Representation of various types of cyberattacks
a) Denial-of-Service attack
b) Spoofing and Sybil attacks
c) Jamming attack
d) Man-in-the-middle attack
e) Selective forwarding attack
f) Malicious input attack

- Secure data aggregation: In various applications, for the reason of deducting the transmission cost and efficiency expenditure in data collection, the raw data felt by each and every sensor should be combined. In this dissertation, we learned



Attack Surface		Attack Name
Physical Device/Perception Surface	Cell Phone Sensors PCs Any physical devices	DoS
		Eavesdropping
		Counterfeiting
		Radio interference
		Jamming
		Physical Attacks
		Node Capture Attacks
		User Tracking
Network/Transport Surface	Networks	DoS
		Hole Attacks
		Selective Forwarding
		Sybil Attacks
		Eavesdropping
		Spoofing
		Traffic Analysis
		Jamming
		Man in the middle
		Routing Attacks
Cloud Services Surface	Server and clouds	DoS
		Session Hijacking
		Exhaustion Attack
		Flooding Attacks
		Malicious Attacks
		Insider Attacks
Web and Application Surface	Websites and mobile applications	DoS
		Repudiation
		Malicious Node
		Data Corruption
		Eavesdropping
		Bluesnarfing and Bluejacking

Fig. 15 Types of attack surface

about event boundary detection which is an important form of data collection. Therefore, as required by the given applications, data aggregation in WSNs can be of different forms. Each different type of data collection may need personalized efficient communication techniques. So, in order to deduct the complexity of the protocol stack, general techniques should also be grown. Various research should be created along this area.

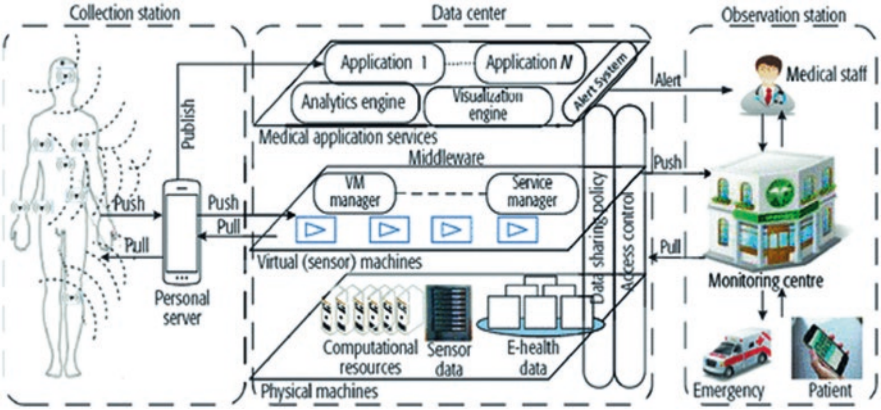


Fig. 16 IoT architecture for smart healthcare [1]

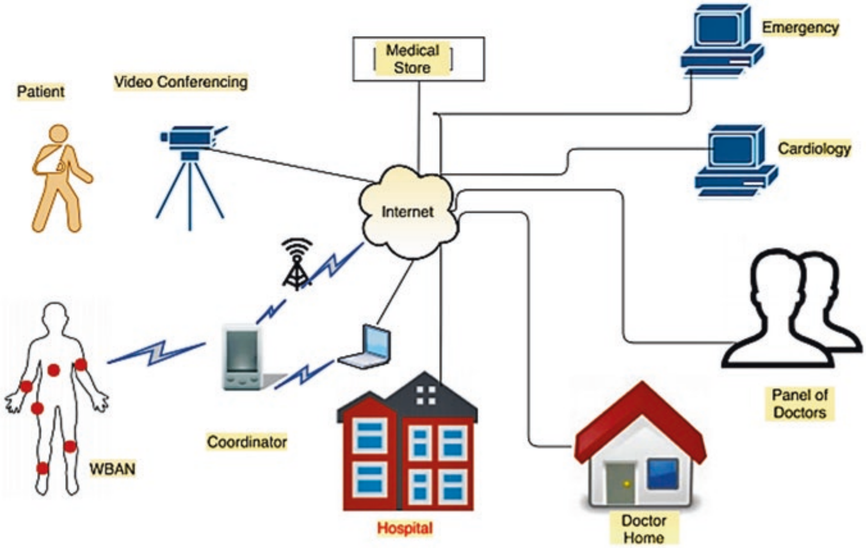
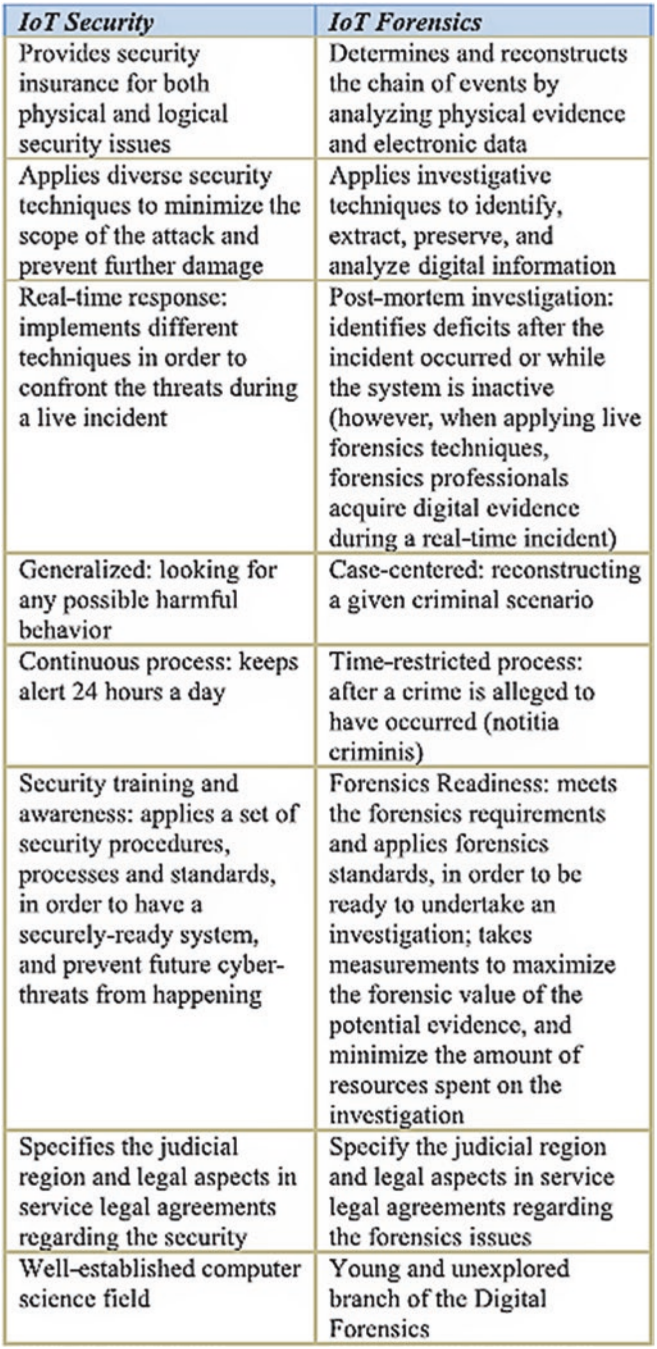


Fig. 17 WBAN architecture [55]

- Privacy-aware security services: Recent security research in WSNs seldomly judge privacy problem. Therefore, in various applications, information and network transmission confidentiality can be a large problem. Privacy-aware security services should be again enlarged as WSNs are visualized to become more and more extensive.

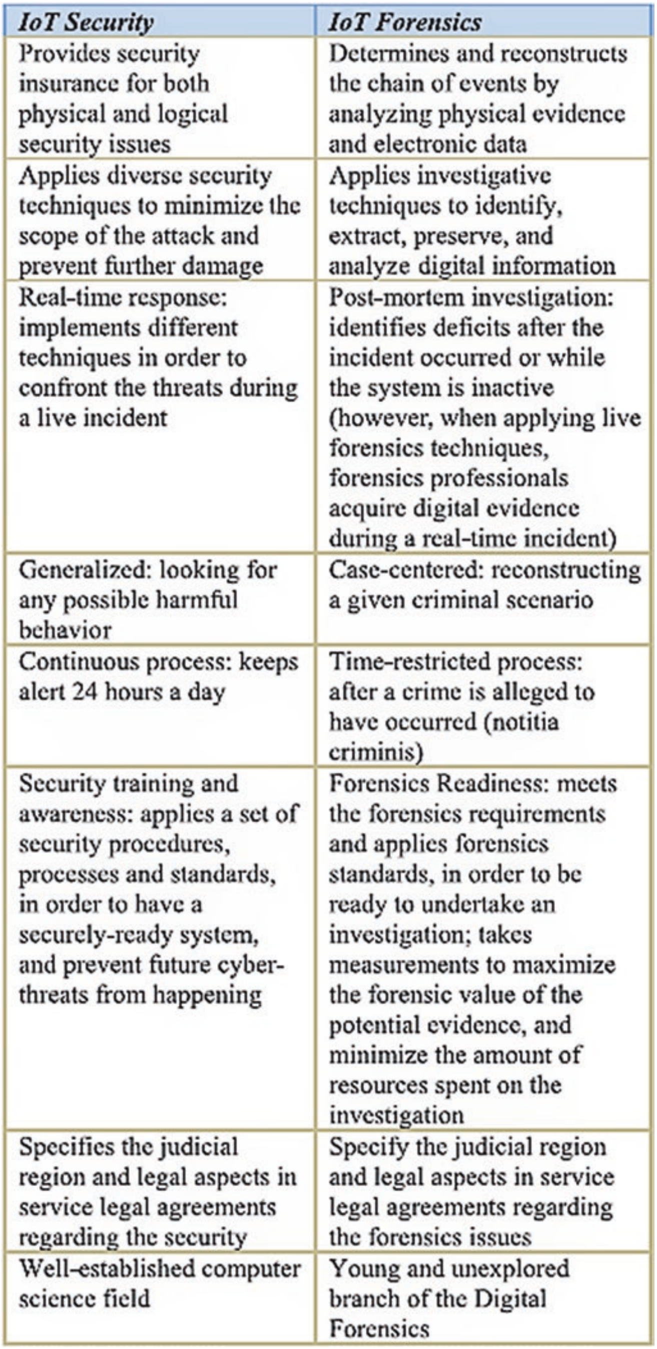
Here we will discuss about various types of anomolies in the field of WSN. These anomalies are elaborately classified below:

Table 1 Difference between IoT security and IoT forensics



IoT Security	*IoT Forensics*
Provides security insurance for both physical and logical security issues	Determines and reconstructs the chain of events by analyzing physical evidence and electronic data
Applies diverse security techniques to minimize the scope of the attack and prevent further damage	Applies investigative techniques to identify, extract, preserve, and analyze digital information
Real-time response: implements different techniques in order to confront the threats during a live incident	Post-mortem investigation: identifies deficits after the incident occurred or while the system is inactive (however, when applying live forensics techniques, forensics professionals acquire digital evidence during a real-time incident)
Generalized: looking for any possible harmful behavior	Case-centered: reconstructing a given criminal scenario
Continuous process: keeps alert 24 hours a day	Time-restricted process: after a crime is alleged to have occurred (notitia criminis)
Security training and awareness: applies a set of security procedures, processes and standards, in order to have a securely-ready system, and prevent future cyber-threats from happening	Forensics Readiness: meets the forensics requirements and applies forensics standards, in order to be ready to undertake an investigation; takes measurements to maximize the forensic value of the potential evidence, and minimize the amount of resources spent on the investigation
Specifies the judicial region and legal aspects in service legal agreements regarding the security	Specify the judicial region and legal aspects in service legal agreements regarding the forensics issues
Well-established computer science field	Young and unexplored branch of the Digital Forensics

Table 1 (continued)



IoT Security	*IoT Forensics*
Provides security insurance for both physical and logical security issues	Determines and reconstructs the chain of events by analyzing physical evidence and electronic data
Applies diverse security techniques to minimize the scope of the attack and prevent further damage	Applies investigative techniques to identify, extract, preserve, and analyze digital information
Real-time response: implements different techniques in order to confront the threats during a live incident	Post-mortem investigation: identifies deficits after the incident occurred or while the system is inactive (however, when applying live forensics techniques, forensics professionals acquire digital evidence during a real-time incident)
Generalized: looking for any possible harmful behavior	Case-centered: reconstructing a given criminal scenario
Continuous process: keeps alert 24 hours a day	Time-restricted process: after a crime is alleged to have occurred (notitia criminis)
Security training and awareness: applies a set of security procedures, processes and standards, in order to have a securely-ready system, and prevent future cyber-threats from happening	Forensics Readiness: meets the forensics requirements and applies forensics standards, in order to be ready to undertake an investigation; takes measurements to maximize the forensic value of the potential evidence, and minimize the amount of resources spent on the investigation
Specifies the judicial region and legal aspects in service legal agreements regarding the security	Specify the judicial region and legal aspects in service legal agreements regarding the forensics issues
Well-established computer science field	Young and unexplored branch of the Digital Forensics

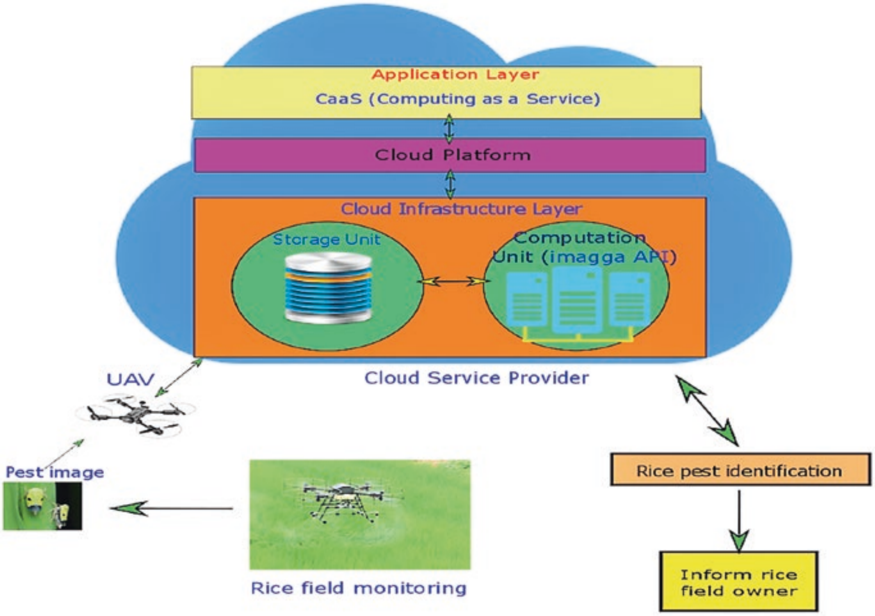


Fig. 18 Possible disease symptoms on plants with the help of UAV [59]

- Attacks on confidentiality and legitimacy: confidentiality and legitimacy of transmission paths should be secured by decryption methods from packet replay anomalies, eavesdropping, and changes of data packets.
- Attacks on network availability: Denial-of-service (DoS) attack are called attacks on availability. This chooses all layers of a sensor network.
- Stealthy attack against service integrity: the aim of the attacker in a stealthy attack is to create the network to receive an incorrect data value. For example, through the sensor node, a hacker encompasses detector point and inserts an incorrect message.

Having the detector network accessible for its deliberate work is necessary in these attacks. DoS attack is very dangerious for WSN should allow day today actual problem to our body and security of human being. Any effort to dispose, disturb, and ruin the networking system is generally known as denial-of-service. Moreover, incidents which eradicate system strength to carry out the involvement can be a DoS attack.

The network layer of WSNs is unsafe because of various types of attacks.

- **Transport Layer Attacks**

Transport layer attacks which can be launched in a wireless sensor network involves de-synchronization and flooding attacks.

- **Node Replication Attack**

A hacker or intruder appending it's connecting points with a survived wireless network in this type of attack by replicating identification number with existing survived point in networking. For a given sensor network, we would like to detect a node replication attack, i.e., an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the network. Ideally, we would like to detect this behavior without centralized monitoring, since centralized solutions suffer from several inherent drawbacks (see Section 3.1). The scheme should also revoke the replicated nodes, so that nonfaulty nodes in the network cease to communicate with any nodes injected in this fashion. We evaluate each protocol's security by examining the probability of detecting an attack given that the adversary inserts L replicas of a subverted node. The protocol must provide robust detection even if the adversary captures additional nodes. We also evaluate the efficiency of each protocol. In a sensor network, communication (both sending and receiving) requires at least an order of magnitude more power than any other operation [14], so our first priority must be minimizing communication, both for the network as a whole and for the individual nodes (since hotspots will quickly exhaust a node's power supply). Moreover, sensor nodes typically have a limited amount of memory, often on the order of a few kilobytes [14]. Thus, any protocol requiring a large amount of memory will be impractical [3].

- **Attacks on Privacy**

As spontaneous data assembling through systematic and deliberate deployment of sensors is feasible for WSNs, it is at risk to the abundant resources. In a WSN, secrecy maintenance of delicate data is an especially very tough challenge. However, to obtain sensitive data, a challenger may collect apparently safe data and finds for combining information gathered through various detector points.

(i) In mobile computing and wireless research methodology, WSN is attracting more interest over the last decade. Use of wireless network is abundant and is increasing a lot such as in strategic battlefield. Anyhow, these networks are unsafe to various security threats because of their saturated nature and implementation in rural areas, which can directly influence their result.

(ii) In Wireless Multimedia Sensor Networks (WMSNs), various components are responsible for the outline in networking system. It is permitted for the transmission of many streams of theory. The pattern of a WMSN is basically affected by various constituents, which are described in this part.

(iii) There are various necessities to the large area of implementations predicted on WMSNs. The availability of inexpensive hardware such as CMOS cameras and microphones that can ubiquitously capture multimedia content from the environment has fostered the development of Wireless Multimedia Sensor Networks (WMSNs) i.e., distributed systems of wirelessly networked devices deployed to retrieve video and audio streams, still images, and scalar sensor data. WMSNs will enable new applications such as multimedia surveillance, traffic enforcement and control systems, advanced health care delivery, structural health monitoring, and industrial process control. Many of these applications require the sensor network paradigm to be re-thought in view of the need to deliver multimedia content with predefined levels of quality of service (QoS).

QoS-compliant delivery of multimedia content in sensor networks is a challenging, and largely unexplored task. First, embedded sensors are constrained in terms of battery, memory, processing capability, and achievable overall rate, while delivery of multimedia flows may be a resource intensive task. Secondly, in multi-hop wireless networks the attainable capacity of each wireless link depends on the interference level perceived at the receiver. Hence, capacity and delay attainable at each link are location dependent, vary continuously, and may be bursty in nature, thus making QoS provisioning a challenging task. Lastly, functionalities handled at different layers of the communication protocol stack are inherently and strictly coupled due to the shared nature of the communication channel.

In our work, we look at cross layer design of WMSNs with the unique requirements of multimedia content in mind. In recent years, there has been intense research and considerable progress in solving numerous wireless sensor networking challenges. However, the key problem of enabling real-time quality-aware video streaming in large-scale multi-hop wireless networks of embedded devices is still open and largely unexplored. We look at a variety of ways to solve some of these problems. With a very lengthy period of time flowing, these data is created and need assisted message forwarding. Therefore, a powerful base is needed to carry out QoS and evaluate application-specific needs. Concerning a union of bounds on power utilization, accuracy, authenticity, delay, tampering, or network lifetime, these demands may exist to more domains and can be demonstrated with others.

(iv) Large data flow rate: Generally, video data needs data flow rate which is a magnitude greater and carried out with presently obtainable detector. Data rates such as one order of magnitude greater may be needed for high-end multimedia sensors, with equivalent energy consumption. So, it requires to be supported with a large amount of data with less energy utilization method. With regard to UWB (ultrawide band), delivery mechanism appears especially favorable for WMSNs.

(v) Power consumption: In WSNs, Power consumption is a basic involve in traditional wireless sensor networks. Multimedia applications generate large amounts of information, which need efficient data delivery powers with large computing.

(vi) Multiple media coverage: In specific video sensors, various multiple media detectors have greater sense power. Tiny wireless devices and the enormous growth of wireless communication technologies have already established the stage for large-scale deployment of wireless sensor networks (WSNs). A typical WSN consists of a large number of small, low-cost sensor nodes, which are distributed in the target area for collecting data of interest. Most of the time, WSN is used for monitoring, tracking and event management related applications. WSN is not a new topic as many inventions have been done and countless applications have been successfully implemented.

Normally, a multimedia sensor device includes a sensing unit, processing unit (CPU), communication module, co-ordination sub-system, storage unit and an optional mobility/actuation unit. Sensing units usually have two sub-units: sensors [digital micro cameras, microphones and/or scalar sensors (for example, temperature sensors, humidity sensors, fire sensors, pressure sensors and gas sensors)], and analogue to digital converters (ADCs). Most of the sensors generate analogue signals which should be converted into digital form by using ADCs as these are to be fed into the CPU. The CPU executes the system software in charge of coordinating sensing and communication tasks for signal processing, and it is interfaced with a storage unit. A communication Tx/Rx module interfaces the device to the network. In many applications, it has been observed that around 70 per cent of the battery is consumed for transceiver processes and the remaining 30 per cent consumption includes computational tasks, signal processing, co-ordination systems and sensor sub-units.

A coordination sub-system coordinates the operation of different network devices by performing various tasks, such as network synchronisation and location management. A mobility actuation unit can enable the movement or manipulation of objects, like motor, to track the object. The whole system is powered by a compact power unit that may be supported by an energy-scavenging unit, such as solar cells. Table II gives an overview of the features of hardware platforms for WMSNs.

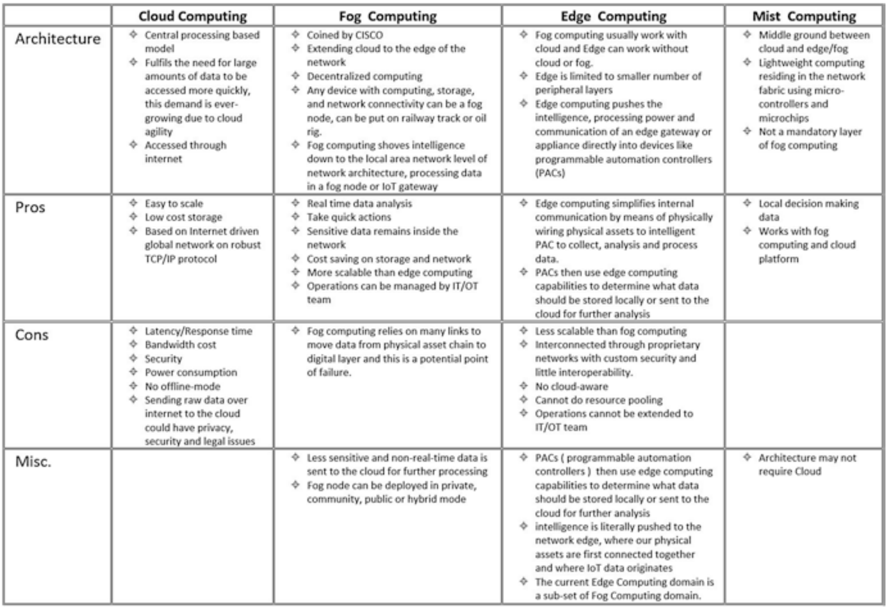
(vii) Connecting other wireless technologies: By corelating regional "islands" of sensors through different Wi-Fi schemes, sensor networks must be added. Without giving up on the reliability of the performance, this is necessary to be secured within each and every individual technology. When the network is used for various mission-critical applications, this problem is very dangerous like that in a strategic battlefield. In real-life deployment scenarios, accidental collapse of nodes often occurs. Traditional security mechanisms with large overhead of computation and transmission are impossible in WSNs due to resource constraints in the sensor nodes (Table 2 and Figs. 16, 17 and 18).

- Irrigation Monitoring System

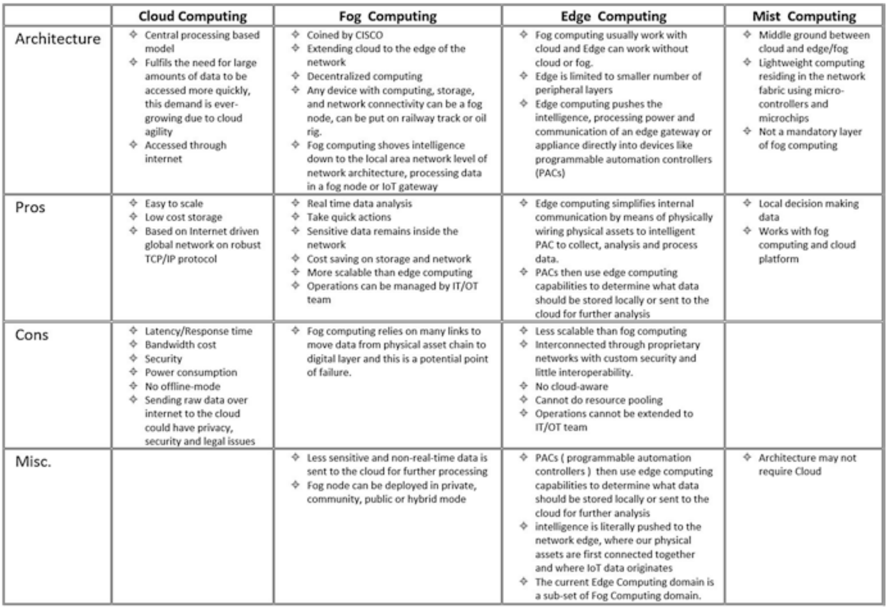
Older irrigation technologies led to a lot of water wastage, discouraging people to take up farming, particularly in a parched area like Dhanbad, despite owning lands and forcing them to migrate to other cities for employment. The project will help those with less farming skill in coming out with a more proficient way of irrigation with the sprinkler system. Temperature, moisture, and humidity readings are continuously monitored using sensors and are managed by the AgroPro app, which is available for download on the Google Play Store.

"The automatic soil monitoring and irrigation system will help farmers tackle water management issues and enhance the crop yield thereby generating means for their livelihood. We had conducted a survey last September and got to know about the problems faced by farmers. This helped us in developing the project to address their issues," said Ranjan. The basic setup costs around Rs 10, 000 for 21, 000 square feet of land. The solar-powered smart irrigation system aims to provide an

Table 2 Comparisons between cloud computing, edge computing, fog computing, and mist computing



	Cloud Computing	Fog Computing	Edge Computing	Mist Computing
Architecture	✧ Central processing based model ✧ Fulfils the need for large amounts of data to be accessed more quickly, this demand is ever-growing due to cloud agility ✧ Accessed through internet	✧ Coined by CISCO ✧ Extending cloud to the edge of the network ✧ Decentralized computing ✧ Any device with computing, storage, and network connectivity can be a fog node, can be put on railway track or oil rig. ✧ Fog computing shoves intelligence down to the local area network level of network architecture, processing data in a fog node or IoT gateway	✧ Fog computing usually work with cloud and Edge can work without cloud or fog. ✧ Edge is limited to smaller number of peripheral layers ✧ Edge computing pushes the intelligence, processing power and communication of an edge gateway or appliance directly into devices like programmable automation controllers (PACs)	✧ Middle ground between cloud and edge/fog ✧ Lightweight computing residing in the network fabric using micro-controllers and microchips ✧ Not a mandatory layer of fog computing
Pros	✧ Easy to scale ✧ Low cost storage ✧ Based on Internet driven global network on robust TCP/IP protocol	✧ Real time data analysis ✧ Take quick actions ✧ Sensitive data remains inside the network ✧ Cost saving on storage and network ✧ More scalable than edge computing ✧ Operations can be managed by IT/OT team	✧ Edge computing simplifies internal communication by means of physically wiring physical assets to intelligent PAC to collect, analysis and process data. ✧ PACs then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis	✧ Local decision making data ✧ Works with fog computing and cloud platform
Cons	✧ Latency/Response time ✧ Bandwidth cost ✧ Security ✧ Power consumption ✧ No offline-mode ✧ Sending raw data over internet to the cloud could have privacy, security and legal issues	✧ Fog computing relies on many links to move data from physical asset chain to digital layer and this is a potential point of failure.	✧ Less scalable than fog computing ✧ Interconnected through proprietary networks with custom security and little interoperability. ✧ No cloud-aware ✧ Cannot do resource pooling ✧ Operations cannot be extended to IT/OT team	
Misc.		✧ Less sensitive and non-real-time data is sent to the cloud for further processing ✧ Fog node can be deployed in private, community, public or hybrid mode	✧ PACs (programmable automation controllers) then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis ✧ intelligence is literally pushed to the network edge, where our physical assets are first connected together and where IoT data originates ✧ The current Edge Computing domain is a sub-set of Fog Computing domain.	✧ Architecture may not require Cloud



	Cloud Computing	Fog Computing	Edge Computing	Mist Computing
Architecture	✧ Central processing based model ✧ Fulfils the need for large amounts of data to be accessed more quickly, this demand is ever-growing due to cloud agility ✧ Accessed through internet	✧ Coined by CISCO ✧ Extending cloud to the edge of the network ✧ Decentralized computing ✧ Any device with computing, storage, and network connectivity can be a fog node, can be put on railway track or oil rig. ✧ Fog computing shoves intelligence down to the local area network level of network architecture, processing data in a fog node or IoT gateway	✧ Fog computing usually work with cloud and Edge can work without cloud or fog. ✧ Edge is limited to smaller number of peripheral layers ✧ Edge computing pushes the intelligence, processing power and communication of an edge gateway or appliance directly into devices like programmable automation controllers (PACs)	✧ Middle ground between cloud and edge/fog ✧ Lightweight computing residing in the network fabric using micro-controllers and microchips ✧ Not a mandatory layer of fog computing
Pros	✧ Easy to scale ✧ Low cost storage ✧ Based on Internet driven global network on robust TCP/IP protocol	✧ Real time data analysis ✧ Take quick actions ✧ Sensitive data remains inside the network ✧ Cost saving on storage and network ✧ More scalable than edge computing ✧ Operations can be managed by IT/OT team	✧ Edge computing simplifies internal communication by means of physically wiring physical assets to intelligent PAC to collect, analysis and process data. ✧ PACs then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis	✧ Local decision making data ✧ Works with fog computing and cloud platform
Cons	✧ Latency/Response time ✧ Bandwidth cost ✧ Security ✧ Power consumption ✧ No offline-mode ✧ Sending raw data over internet to the cloud could have privacy, security and legal issues	✧ Fog computing relies on many links to move data from physical asset chain to digital layer and this is a potential point of failure.	✧ Less scalable than fog computing ✧ Interconnected through proprietary networks with custom security and little interoperability. ✧ No cloud-aware ✧ Cannot do resource pooling ✧ Operations cannot be extended to IT/OT team	
Misc.		✧ Less sensitive and non-real-time data is sent to the cloud for further processing ✧ Fog node can be deployed in private, community, public or hybrid mode	✧ PACs (programmable automation controllers) then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis ✧ intelligence is literally pushed to the network edge, where our physical assets are first connected together and where IoT data originates ✧ The current Edge Computing domain is a sub-set of Fog Computing domain.	✧ Architecture may not require Cloud

IoT solution in automating the watering process using an Arduino-based microcontroller and sensors. It is an energy-efficient and eco-friendly system that generates electricity from photovoltaic cells to supply water to the plants from water pumps. The watering process is driven by the moisture content of the soil using sensors. Threshold limits are set for soil moisture sensor to ensure efficient and effective use of water resource. The main microcontroller unit controls the system whenever the sensor is across threshold value. Also, the system has built-in temperature and humidity sensors to monitor the climate condition on a specific environment. Another sensor is implemented to measure the water tank level which serves as storage capacity that supplies the water to the system. With the integration of IoT, automated irrigation can be easily accessed and remotely monitored over a mobile application through a wireless communication device. With these smart irrigation techniques, it replaces the traditional irrigation system that helps decrease manual intervention and mistakes.

4 COVID Handling Using IoT

To minimize the spread rate of the fatal COVID disease, scientists are trying and doing research to identify disease-affected persons. From Figs. 19, 20 and 21, we came to know about the architecture of the process, fog computing framework, and customer registration process. The number of infected as well as suspected people can be found by using this method nationwide. There are many terminologies used here, which we will discuss below:

- ARC: Automatic Risk Checker (ARC)
- CA: Cloud Application

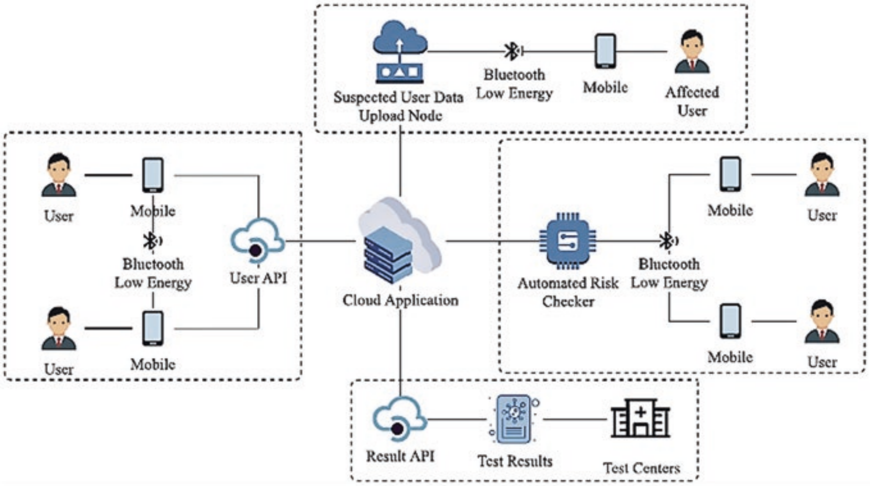


Fig. 19 Application of COVID system overview [58]

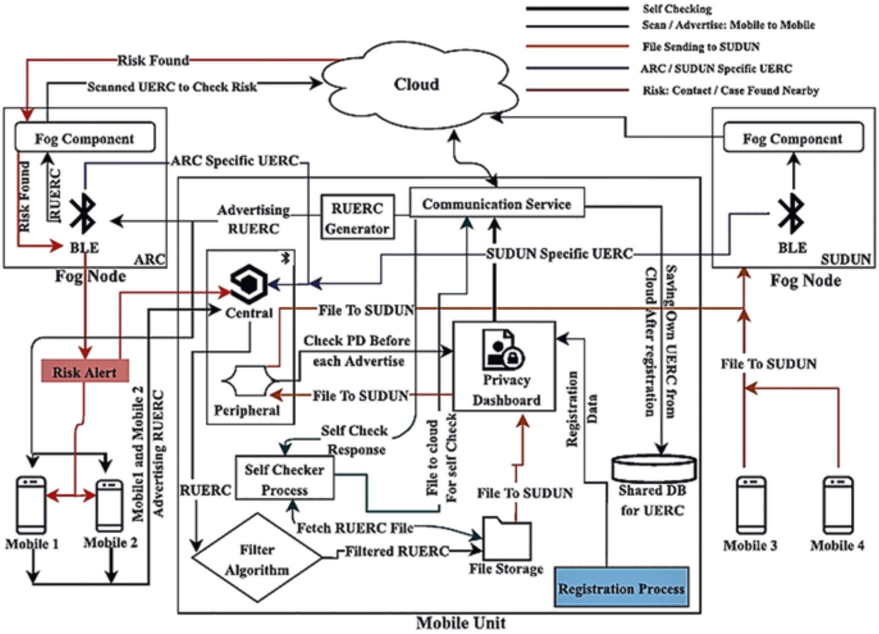


Fig. 20 Fog computing framework [58]

- SUDUN: Suspected User Data Uploader Node
- UERC: Unique Encrypted Reference Code
- RUERC: Rotational Unique Encrypted Reference Code
- BLE: Bluetooth Low Energy Technology

5 Conclusion

IoT is a technology that provides a platform where a network of devices can communicate, explore data, and practice information manually to cater to the needs of individuals or organizations. Enabling autonomous interaction between the interconnected devices and objects gives rise to another emerging interdisciplinary area as well as influencing new paradigms on the Internet. Among the other extension of IoT, Internet of behavior is the recent one and can be compiled under fields like technology, data analytics, and behavioral science.

This chapter's objective is to explore the concepts and applications related to Internet of things with the vision to identify and address its behavioral applications focusing into decisions, intensifications, and companionship while using the technology in healthcare solutions, agriculture and supply chain, industry, and other

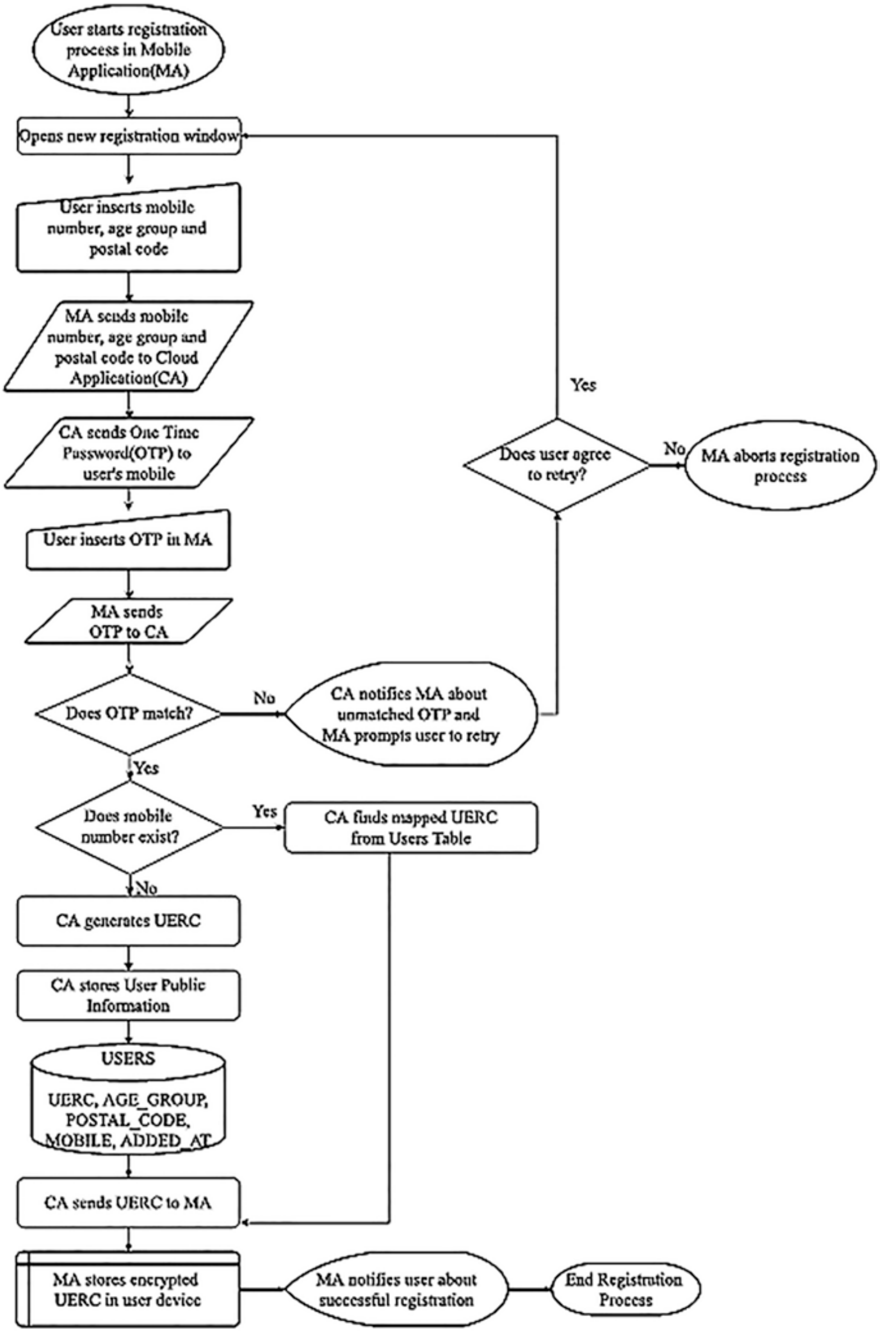

User starts registration process in Mobile Application(MA)
Opens new registration window
User inserts mobile number, age group and postal code
MA sends mobile number, age group and postal code to Cloud Application(CA)
CA sends One Time Password(OTP) to user's mobile
User inserts OTP in MA
MA sends OTP to CA
Does OTP match?
No
CA notifies MA about unmatched OTP and MA prompts user to retry
Does user agree to retry?
Yes
No
MA aborts registration process
Yes
Does mobile number exist?
Yes
CA finds mapped UERC from Users Table
No
CA generates UERC
CA stores User Public Information
USERS
UERC, AGE_GROUP, POSTAL_CODE, MOBILE, ADDED_AT
CA sends UERC to MA
MA stores encrypted UERC in user device
MA notifies user about successful registration
End Registration Process

Fig. 21 Registration process of the user [58]

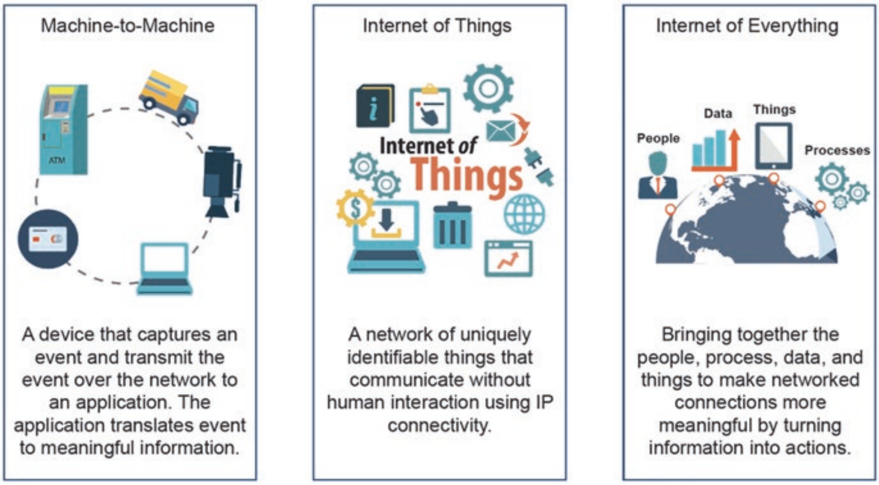

Machine-to-Machine
ATM
A device that captures an event and transmit the event over the network to an application. The application translates event to meaningful information.
Internet of Things
Internet of Things
A network of uniquely identifiable things that communicate without human interaction using IP connectivity.
Internet of Everything
People
Data
Things
Processes
Bringing together the people, process, data, and things to make networked connections more meaningful by turning information into actions.

Fig. 22 Differences among M2M, IoT, and IOE

smart applications. Due to this all-in-one embedded nature of IoT and its behavioral applications, its architectural design, implementation, operational manageability, and maintenance are raising numerous prevalent concerns that serve as challenges for researchers and academicians (Fig. 22).

References

1. P.J. Escamilla-Ambrosio, A. Rodríguez-Mota, E. Aguirre-Anaya, R. Acosta-Bermejo, M. Salinas-Rosales, Distributing computing in the Internet of Things: cloud, fog and edge computing overview, in *NEO 2016*, Studies in computational intelligence, ed. by Y. Maldonado, L. Trujillo, O. Schütze, A. Riccardi, M. Vasile, vol. 731, (Springer, Cham, 2018). https://doi.org/10.1007/978-3-319-64063-1_4
2. A.A. Abd El-Latif, B. Abd-El-Atty, M.S. Hossain, S. Elmougy, A. Ghoneim, Secure quantum steganography protocol for fog cloud internet of things. IEEE Access **6**, 10332–10340 (2018)
3. https://www.designworldonline.com/part-1-connectivity-and-iot-in-motion-and-general-automation/
4. A. Behura, S.B.B. Priyadarshini, Assessment of load in cloud computing environment using C-means clustering algorithm, in *Intelligent and cloud computing*, (Springer, Singapore, 2019), pp. 207–215
5. A. Behura, M.R. Kabat, Energy-efficient optimization-based routing technique for wireless sensor network using machine learning, in *Progress in computing, analytics and networking*, (Springer, Singapore, 2020), pp. 555–565
6. M. Buvana, K. Loheswaran, K. Madhavi, S. Ponnusamy, A. Behura, R. Jayavadivel, Improved resource management and utilization based on a fog-cloud computing system with IOT incorporated with classifier systems. Microprocessors and Microsystems **103815**
7. S. Sahoo, R. Halder, Blockchain-based forward and reverse supply chains for E-waste management, in *International Conference on Future Data and Security Engineering*, (Springer, Cham, 2020, November), pp. 201–220

8. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials **22**(2), 1191–1221 (2020)
9. A. Alenezi, N.H.N. Zulkipli, H.F. Atlam, R.J. Walters, G.B. Wills, The impact of cloud forensic readiness on security, in *Proceedings of the 7th International Conference on Cloud Computing and Services Science*, (2017), pp. 539–545
10. A. Cook et al., *Internet of Cloud: Security and Privacy Issues* (Springer, Cham, 2018), pp. 271–301
11. G. Ramachandra, M. Iftikhar, F.A. Khan, A comprehensive survey on security in cloud computing. Procedia Computer Science **110**(2012), 465–472 (2017)
12. M. Hossain, R. Hasan, A. Skjellum, Securing the Internet of Things: A meta-study of challenges, approaches, and open problems, in *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, (2017), pp. 220–225
13. M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open issues. Future Gener. Comput. Syst. **82**, 395–411 (May 2018)
14. M. Ammar, G. Russello, B. Crispo, Internet of things: A survey on the security of IoT frameworks. J. Inf. Security Appl. **38**, 8–27 (Feb. 2018)
15. M. Aly, F. Khomh, M. Haoues, A. Quintero, and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review, " *Internet Things*, vol. 6, 2019., Art no. 100050
16. J. Gubbi, R. Buyya, S. Marusic, Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(1), 1–19 (2013)
17. Y. Lu, L.D. Xu, Internet of things (IoT) cyber security research: A review of current research topics. IEEE Internet Things J. **6**(2), 2103–2115 (Apr. 2019)
18. S. Balaji, K. Nathani, R. Santhakumar, IoT technology, applications and challenges: A contemporary survey. Wireless Pers. Commun. **108**, 363–388 (Apr. 2019)
19. A. Colakovi'c, M. Hadžiali'c, Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Comput. Netw.* **144**, 17–39 (2018)
20. M.Z. Hasan, H. Al-Rizzo, F. Al-Turjman, A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks. IEEE Commun. Surveys Tuts. **19**(3), 1424–1456. , 3rd Quart. (2017)
21. A. Adeel et al., *A Survey on the Role of Wireless Sensor Networks and IoT in Disaster Management* (Springer, Singapore, 2019), pp. 57–66
22. R. Ahmed, A.K. Malviya, M.J. Kaur, V.P. Mishra, Comprehensive Survey of Key Technologies Enabling 5G-IoT. SSRN Electron. J., 488–492 (2019)
23. J. Yin, Z. Yang, H. Cao, T. Liu, Z. Zhou, C. Wu, A survey on Bluetooth 5.0 and mesh. ACM Trans. Sens. Netw. **15**(3), 1–29 (2019)
24. M. Bembe, A. Abu-Mahfouz, M. Masonta, T. Ngqondi, A survey on low-power wide area networks for IoT applications. Telecommun. Syst. **71**(2), 249–274 (2019)
25. F. Al-Turjman, E. Ever, H. Zahmatkesh, Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview. IEEE Commun. Surveys Tuts. **21**(1), 28–65 (2019)
26. J.G. Andrews et al., What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014)
27. M. Agiwal, N. Saxena, A. Roy, Towards connected living: 5G enabled internet of things (IoT). IETE Tech. Rev. **36**(2), 190–202 (2019)
28. H. Ullah, N.G. Nair, A. Moore, C. Nugent, P. Mus-champ, M. Cuevas, 5G communication: An overview of vehicle-to everything, drones, and healthcare use-cases. IEEE Access **7**, 37251–37268 (2019)
29. M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. **78**, 544–546 (018)
30. Á. MacDermott, T. Baker, Q. Shi, IoT Forensics: Challenges for the Ioa era, in *Proc. 9th IFIP Int. Conf. New Technol. Mobile Security (NTMS)*, (2018), pp. 1–5

31. A. Alenezi, H.F. Atlam, R. Alsagri, M.O. Alassafi, G.B. Wills, IoT forensics: A state-of-the-art review, challenges and future directions, in *Proc. 4th Int. Conf. Complexity Future Inf. Syst. Risk (COMPLEXIS)*, (2019), pp. 106–115
32. D. Lillis, B. Becker, T. O'Sullivan, M. Scanlon, Current challenges and future research areas for digital forensic investigation, in *Proc. 11th ADFSL Conf. Digit. Forensics Security Law (CDFSL), Daytona Beach, FL, USA*, (2016)
33. M.Y. Arafat, B. Mondal, S. Rani, Technical challenges of cloud forensics and suggested solutions. Int. J. Sci. Eng. Res. **8**(8), 1142–1149 (2017)
34. S. Zawoad, R. Hasan, Digital forensics in the age of big data: Challenges, approaches, and opportunities, in *Proc. IEEE 17th Int. Conf. High Perform. Comput. Commun. IEEE 7th Int. Symp. Cyberspace Safty Security IEEE 12th Int. Conf. Embedded Softw. Syst.*, (2015), pp. 1320–1325
35. I. Yaqoob, I.A.T. Hashem, A. Ahmed, S.M.A. Kazmi, C.S. Hong, Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Gener. Comput. Syst. **92**, 265–275 (2019)
36. L. Sadineni, E. Pilli, R.B. Battula, *A Holistic Forensic Model for the Internet of Things* (Springer, Cham, 2019)
37. M. Hossain, Towards a holistic framework for secure, privacy-aware, and trustworthy Internet of Things using resource efficient cryptographic schemes. Ph.D. dissertation (2018). https://doi.org/10.13140/RG.2.2.33117.72165
38. H. Chung, J. Park, S. Lee, Digital forensic approaches for Amazon Alexa ecosystem, in *Proc. 17th Annu. DFRWS USA*, (2017), pp. S15–S25
39. M. Al-Sharrah, A. Salman, I. Ahmad, Watch your smart watch, in *Proc. Int. Conf. Comput. Sci. Eng. (ICCSE)*, (2018), pp. 1–5
40. C.M. Rondeau, M.A. Temple, J. Lopez, Industrial IoT cross-layer forensic investigation. Wiley Interdiscip. Rev. Forensic Sci. **1**(1), Art. no. e1322 (2019)
41. K. Wang, M. Du, Y. Sun, A. Vinel, Y. Zhang, Attack detection and distributed forensics in machine-to-machine networks. *IEEE Netw.* **30**(6), 49–55 (2016)
42. A. Tekeoglu, A. Tosun, Investigating security and privacy of a cloud-based wireless IP camera: NetCam, in *Proc. 24th Int. Conf. Comput. Commun. Netw. (ICCCN)*, (2015), pp. 1–6
43. E. Knight, S. Lord, B. Arief, Lock picking in the era of Internet of Things, in *Proc. IEEE CPS Workshop Data Security Privacy Forensics Trust (DSPFT)*, (2019), pp. 835–842
44. F. Al-Turjman, M. Abujubbeh, IoT-enabled smart grid via SM: An overview. Future Gener. Comput. Syst. **96**, 579–590 (2019)
45. V. Bhoopathy, A. Behura, V.L. Reddy, S. Abidin, D.V. Babu, A.J. Albert, IOT-HARPSECA: A secure design and development system of roadmap for devices and technologies in IOT space. Microprocess. Microsyst. **104044** (2021)
46. R. Abassi, VANET security and forensics: Challenges and opportunities. Wiley Interdiscip. Rev. Forensics Sci. **1**(2), Art. no. e1324 (2019)
47. M. Hossain, R. Hasan, S. Zawoad, Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV), in *Proc. IEEE 2nd Int. Congr. Internet Things (ICIOT)*, (2017), pp. 25–32
48. E.K. Lee, M. Gerla, G. Pau, U. Lee, J.H. Lim, Internet of vehicles: From intelligent grid to autonomous cars and vehicular fogs. Int. J. Distrib. Sens. Netw. **12**(9), 1–14 (2016)
49. F. Al-Turjman, J.P. Lemayian, S. Alturjman, L. Mostarda, Enhanced deployment strategy for the 5G drone-BS using artificial intelligence. IEEE Access **7**, 75999–76008 (2019)
50. A. Renduchintala, F. Jahan, R. Khanna, A.Y. Javaid, A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework. Digit. Invest. **30**, 52–72 (2019)
51. U. Jain, M. Rogers, E.T. Matson, Drone forensic framework: Sensor and data identification and verification, in *Proc. IEEE Sensors Appl. Symp. (SAS)*, (2017), pp. 1–6
52. M.A. Ferrag, L. Maglaras, DeliveryCoin: An IDS and block chain based delivery framework for drone-delivered services. Computers **8**(3), 58 (2019)

53. N.M. Karie, V.R. Kebande, H.S. Venter, K.-K.R. Choo, On the importance of standardising the process of generating digital forensic reports. Forensics Sci. Int. Rep. **1**, Art no. 100008 (2019)
54. E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, Internet of Things forensics: Challenges and approaches, in *Proc. 9th IEEE Int. Conf. Collaborative Comput. Netw. Appl. Worksharing*, (2013), pp. 608–615
55. K. Hasan, K. Biswas, K. Ahmed, N.S. Nafi, M.S. Islam, A comprehensive review of wireless body area network. J. Netw. Comput. Appl. **143**, 178–198 (2019)
56. A. Nieto, R. Rios, J. Lopez, A methodology for privacy-aware IoT-forensics, in *Proc. 16th IEEE Int. Conf. Trust Security Privacy Comput. Commun. 11th IEEE Int. Conf. Big Data Sci. Eng. 14th IEEE Int. Conf. Embedded Softw. Syst.*, (2017), pp. 626–633
57. S.M. Tahsien, H. Karimipour, P. Spachos, Machine learning based solutions for security of Internet of Things (IoT): A survey. J. Netw. Comput. Appl. **161**, 102630 (2020)
58. M. Whaiduzzaman, M.R. Hossain, A.R. Shovon, S. Roy, A. Laszka, R. Buyya, A. Barros, A privacy-preserving mobile and fog computing framework to trace and prevent covid-19 community transmission. IEEE J. Biomed. Health Inform. **24**(12), 3564–3575 (2020)
59. S.K. Bhoi, K.K. Jena, S.K. Panda, H.V. Long, R. Kumar, P. Subbulakshmi, H.B. Jebreen, An Internet of Things assisted Unmanned Aerial Vehicle based artificial intelligence model for rice pest detection. Microprocess. Microsyst. **80**, 103607