Wireless Personal Communications (2020) 115:1667–1693
https://doi.org/10.1007/s11277-020-07649-9

Security and Privacy in IoT: A Survey

Poornima M. Chanal[1] · **Mahabaleshwar S. Kakkasageri**[1]

Published online: 29 July 2020

Abstract
The Internet of Things (IoT) is a network of globally connected physical objects, which are associated with each other via Internet. The IoT foresees the interconnection of few trillions of intelligent objects around us, uniquely and addressable every day, these objects have the ability to accumulate process and communicate data about themselves and their surrounding environment. The best examples of IoT systems are health care, building smart city with advance construction management system, public and defense surveillance and data acquisition. Recent advancement in the technology has developed smart and intelligent sensor nodes and RFIDs lead to a large number of wireless networks with smart and intelligent devices (object, or things) connected to the Internet continuously transmit the data. So to provide security and privacy to this data in IoT is a very challenging task, which is to be concerned at highest priority for several current and future applications of IoT. Devices such as smart phone, WSNs and RFIDs etc., are the major components of IoT network which are basically resource constrained devices. Design and development of security and privacy management schemes for these devices is guided by factors like good performance, low power consumption, robustness to attacks, tampering of the data and end to end security. Security schemes in IoT provide unauthorized access to information or other objects by protecting against alterations or destruction. Privacy schemes maintain the right to control about the collected information for its usage and purpose. In this paper, we have surveyed major challenges such as Confidentiality, Integrity, Authentication, and Availability for IoT in a brief manner.

Keywords Internet of things · Security · Privacy

1 Introduction

The Internet of Things (IoT) is the network of physical objects i.e., devices, vehicles, home appliances and other things embedded with computation and communication capability which enables these things to connect each other and exchange data via the existing global Internet infrastructure. Traditional fields of embedded systems

✉ Poornima M. Chanal
poornima.chanal@yahoo.com

[1] Electronics and Communication Engineering Department, Basaveshwar Engineering College (Autonomous), Bagalkot, Karnataka 587103, India

with Radio-frequency identification (RFID), Wireless Sensor Networks (WSNs), control systems, automation and others all contribute to enable and empower the IoT. IoT offers individual objects or things identification, sensor and connection capability as the basis for the development of independent complaisant services and applications. These objects are characterized by a high degree of autonomous data capture, event transfer, network connectivity and interoperability. The overall IoT context will consist of few trillions of different devices and their services that connect to each other to exchange valuable information [1]. Rapid advancements in mobile communication and networking, VLSI design and MEMS technologies lead to design and development of smart networks with cell phones, WSNs and RFIDs, things and mechanisms in IoT can team up with one another anytime, anywhere and in any form [2, 3]. The major goal of IoT is to create smart environments and self-conscious/autonomous devices used in the construction of smart cities, smart hospitals, intelligent transportation system and so on [4, 5]. In business, IoT presents good vision for different types of organizations, including IoT applications, different service providers, IoT integrators, telecom operators and software vendors [6]. According to estimation, more than 30 billion connected device to Internet with more than 200 billion intermittent connections [7] will generate approximately 714 billion EUR in revenue by 2020 [8]. Many of the vertical segments are expected to grow in double digit in future. Among the most upcoming vertical application domains are automotive industries, smart transport, smart items, smart health care, smart cities and so on.

With the rapid increase in IoT applications a huge amount of data is generated where several security and privacy issues are observed. When devices will be connected to each other, security and privacy issues will only become more pronounced, and continuously exposes additional security flaws and weaknesses. In statistical senses all exposed errors and weaknesses may be abused in an environment with many billions of devices [9]. In the absence of security and privacy, attacks and malfunctions in the IoT may outweigh its advantages and applications [10]. An analysis of recent research in IoT security from 2016 to 2018, its trends, open issues and current state of IoT security research discussed in [11]. The relevant tools, IoT modelers and simulators are also presented. Scalability parameters and other restrictions on IoT device capabilities also mean that traditional cryptography protocols, protection algorithms, and security schemes are insufficient [12–14]. The security and privacy platform must be robust and the security architecture designed should be of life span of 20+ years. When dealing with large population of devices some of the devices will be comprised with security and privacy aspects. Therefore new design and development methodologies should be adapted to meet IoT requirements in terms of security and privacy issues [15–18]. The IoT have gained more popularity and becoming more common in people lives, so prolonging the privacy and security in intelligent manner is very crucial. These things are restricted in size, battery life and computational techniques so they may not support the same of security and privacy as traditional Internet connected devices [19–21]. Security problems and solutions of each layer and comparison of existing trust models with respect to Trust Related Attacks (TRA) and Function Requirements (FR) of IoT [22, 23]. Total number of existing IoT devices and new devices connecting to Internet will create new challenges and requires new approaches to solve the privacy and security issues.

Rest of the paper is organized as follows. The Sect. 2 reviews IoT architecture and applications. Section 3 presents research challenges in IoT. Security and privacy issues along with on-going research works in IoT are discussed in Sect. 4. The survey is summarized in final Sect. 5.

2 Internet of Things Overview

IoT allow people and objects/things to be connected anywhere, anytime, anything and anyone. Internet has turned into more common in our life in very short period than any other technology in the history. It revolutionized the communicate way of people. Mainly IoT involves in the process of connecting machines, equipment, software, and objects/things. This will be through the usage of the unique Internet protocol address that permits things for communicating to each other without human intervention [24]. The term IoT is mentioned by Massachusetts Institute of Technology (MIT) Auto-ID center [25].

2.1 Architectures

IoT architectures can be classified as follows: (i) Three layer architecture, (ii) Middle-ware based architecture, (iii) SOA based architecture, (iv) Five layer architecture, (v) Cloud and Fog based architecture and (vi) Social IoT (SIoT) [26–29]. In the following sections, we present these architectures.

2.1.1 Three Layer Architecture

Three layer architecture is the basic IoT architecture [30–32] (as shown in Fig. 1). This layer defines the concept of IoT, but it is not adequate for emerging IoT applications. It has three layers: perception layer, network layer and application layer. The function of

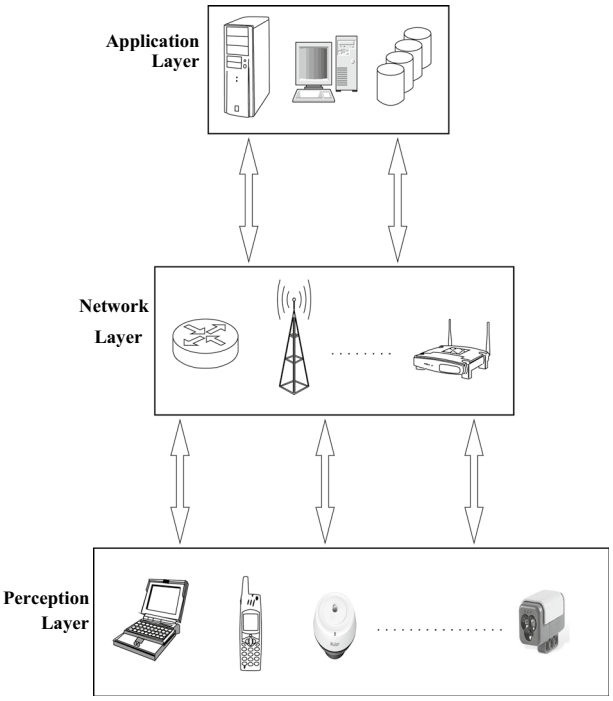

Fig. 1 Three layer IoT architecture

perception layer is to recognize each thing in the IoT system. This is done by gathering data about each entity. The perception layer contains RFID tags, sensors, cameras, etc. This is the physical layer responsible to identify each object/thing in IoT. This is achieved with the help of sensors for sensing and gathering data about each thing. The network layer is the core of IoT and it is responsible for connecting to other smart objects, network devices, and servers. It is also responsible to transmit the information gathered by the perception layer. The application layer is responsible for converging IoT application services to the user. It defines various applications such as smart homes, smart cities, smart health, intelligent automation etc., in which the IoT can be deployed.

2.1.2 Middle-Ware Based Architecture

This architecture connects to different, often complex and already existing programs. The fundamental nature of the IoT is making it possible for just about anything (any thing) to be connected and to communicate information over a network. Middle-ware is part of the IoT system to enable connectivity for large numbers of various things by providing a connectivity layer for sensors and also for the application layers that give services that ensure effective communications among software. Middle-ware based IoT architecture (as shown in Fig. 2) consists of following layers: Edge technology layer, Access gateway layer, Network layer, Middle-ware layer and Application layer.

Edge technology layer is also called as hardware layer that consists of embedded systems, RFID tags, sensor and other sensors in different forms. This layer is responsible for collecting data from a system, or an environment, processing information and supporting communication. Data handling process is done by access gateway layer, and is accountable for publishing and subscribing the services that are provided by the objects, message routing, and hoveling the communication between platforms. Middle-ware layer include some critical functions such as gathering and removal of unwanted data received from the hardware devices, discovery of information and permitting access control to the devices for applications.

Interface protocols component present in middle-ware layer has the ability to provide technical interoperability between two systems by using the same communication protocols. Device abstraction component provides syntactic and semantic interoperability with other devices. Syntactic interoperability is associated with data formats. Semantic interoperability is associated with the meaning of the content of message which is understandable for human. Control and management component is responsible to support computational style that takes to account the context of the entities that interact with the system. Application idea component provides an interface for both high level applications and end users to interact with devices. Some of the IoT middle-ware are HYDRA (Link Smart), AURA, Tiny DB, Wise MID, ISMB, ASPIRE, UBIWARE, UBISOAP, UBIOAD, GSN, SMEPP, SOCRADES, SIRENA and WHEREX[33].

2.1.3 SOA Based Architecture

Service Oriented Architecture (SOA) based IoT is as shown in Fig. 3. IoT is consists of heterogeneous set of objects and each object provides one particular functions with respect to its language. Abstraction layer is capable of providing the access to the various objects with a common language. Service management layer provides the key functions that are expected to be available for each object and that allow for their

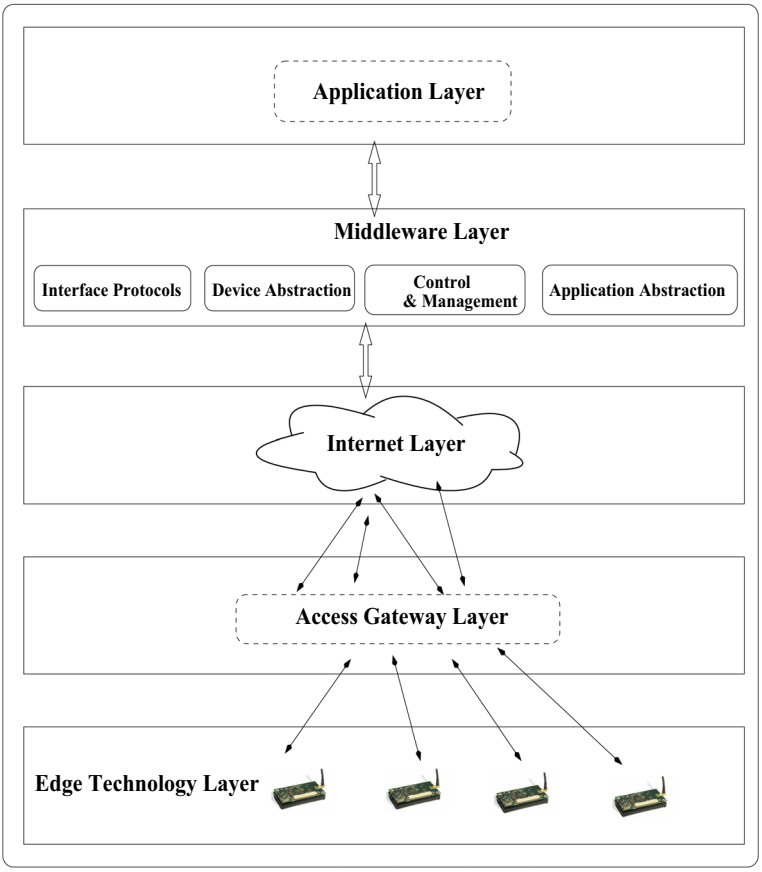

Fig. 2 Middle-ware based IoT architecture

management in the IoT scenario. Both service management and composition layer present the functionalities for the composition of single services offered by networked objects to build specific applications. Applications are on the top of the architecture, exporting all the functionalities to the end user.

2.1.4 Five Layer Architecture

Five layer IoT (as shown in Fig. 4) consists of following layers: Perception layer, Network layer, Middle-ware layer, Application layer and Business layer. Perception layer is meant to define the physical meaning of each object in the IoT system. Network layer acts as a intermediate layer in between perception layer and middle-ware layer. Middle-ware layer is responsible for information gathering, storing and analyzing. Application layer is responsible to execute various applications. Business layer defines the IoT applications charge and management. Privacy and security is the integral part of all five layers.

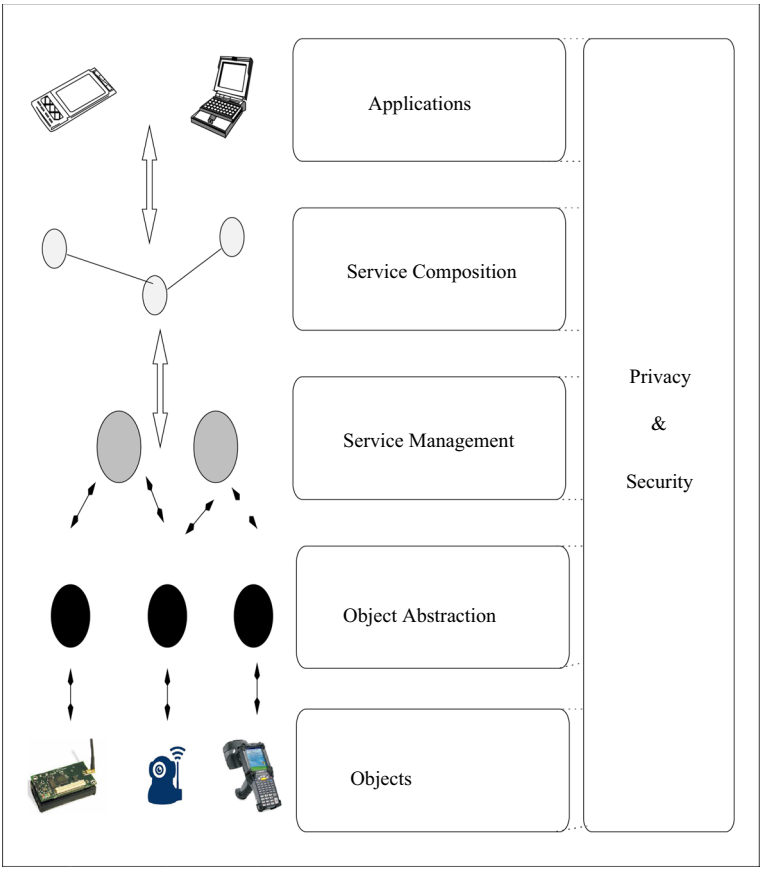

Fig. 3 SOA based IoT architecture

2.1.5 Cloud and Fog Based Architecture

Storage of information in large quantity service is offered by cloud computing infrastructure, platform and software. Fog computing is next level of computing mechanism where sensors and gateways perform information processing and analysis. Monitoring, pre-processing, storage, and security layers exist in between the perception and application layers. The monitoring layer monitors power, resources, responses, and services. Monitoring and pre-processing are done on the edge of the network before sending information to the cloud. Data replication, distribution, and storage functions are performed by temporary storage layer. Data security and privacy is given by security layer using different types of encryption/decryption mechanism. Recently edge computing and fog computing are gaining popularity. Fog computing originally termed by Cisco refers to smart gateways and smart sensors, whereas edge computing provides smart data pre-processing capabilities to physical devices. Generic block diagram for cloud and fog based architecture is as shown in Fig. 5.

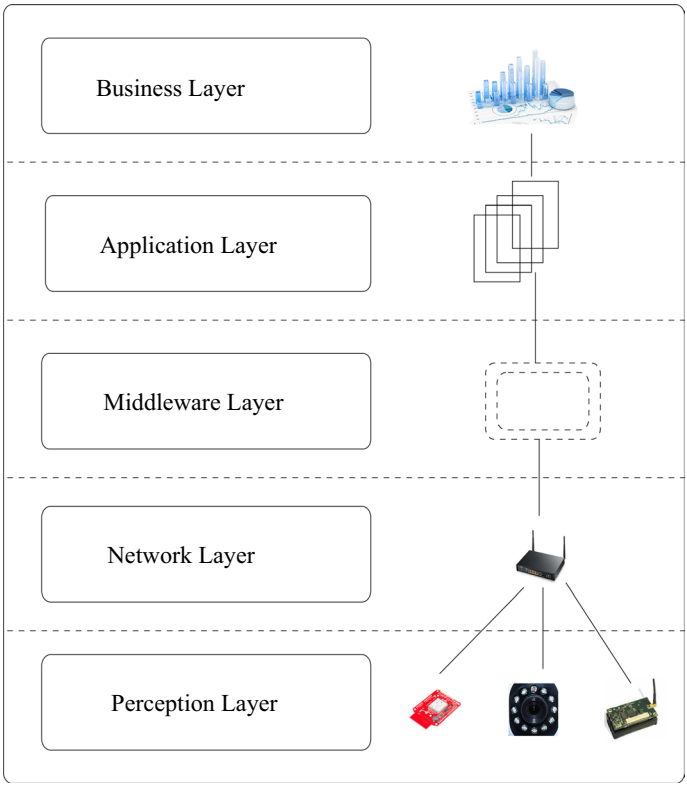

Fig. 4 Five layer IoT architecture

2.1.6 Social IoT (SIoT)

Social relationships between objects are existing in Social IoT (SIoT) as the same way as humans form social relationships. In SIoT, objects and services are considered as bots where they can place relationships between them and modify them over time. This will allow the objects to operate seamlessly each other and achieve a complex task. Some of the important components in SIoT are ID, Meta information, Security controls, Service discovery, Relationship management, and Service composition. Generic architecture for SIoT is as shown in Fig. 6. The perception layer of SIoT is accountable for sensing and gathering data from IoT devices. After gathering the data, IoT objects are set up social relationships and friendship circles among themselves using SIoT technique. Gathered sensing and friendship circles data are forwarded to network layer in order to use this data by IoT applications. The SIoT recommendation system requires data sharing among IoT applications; providing proposal services based on this shared data.

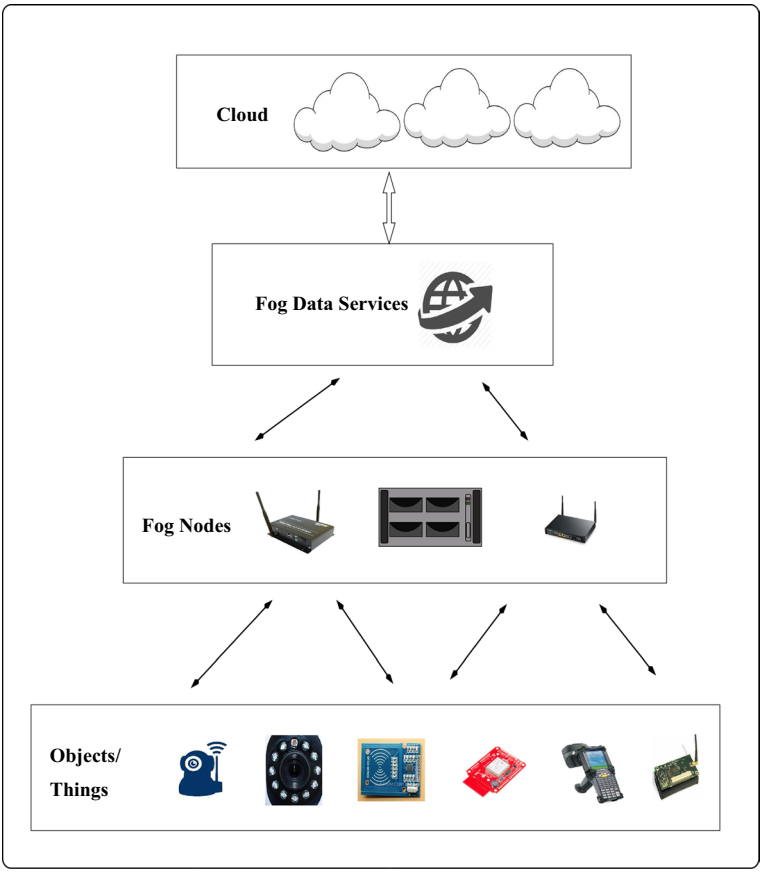

Fig. 5 Cloud and Fog based IoT architecture

2.2 IoT Applications

IoT offers several potential services, out of which very few are popular. Many applications improve the quality of life. Applications of IoT can be grouped into the following main domains (see Fig. 7): Medical, Military, Industrial, Automotive, Environmental, Agriculture, Retail and Consumer. Transportation and logistics domain, Health-care domain, Smart environment [34] (Smart home, Smart office) domain, Personal and social domain.

2.2.1 Medical Applications

The market for the IoT in medical field is growing steadily, with applications ranging from remote monitoring system to smart sensors and medical objects integration. IoT in health care can also boost patient appointment and fulfillment by allowing patients to spend extra time interacting with their doctors. But the number of connected objects and great amount of information collection can be a challenge to manage by providing security

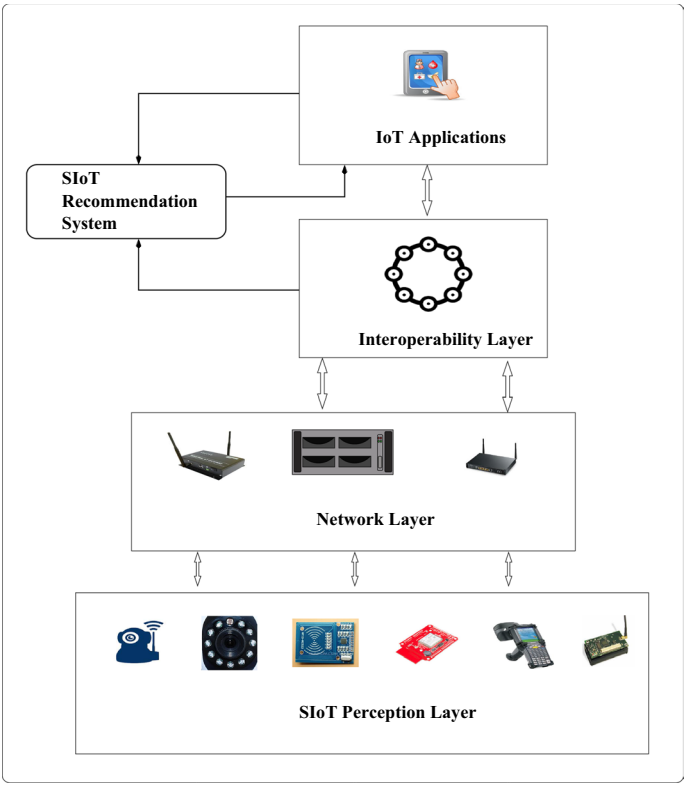

Fig. 6 SIoT architecture

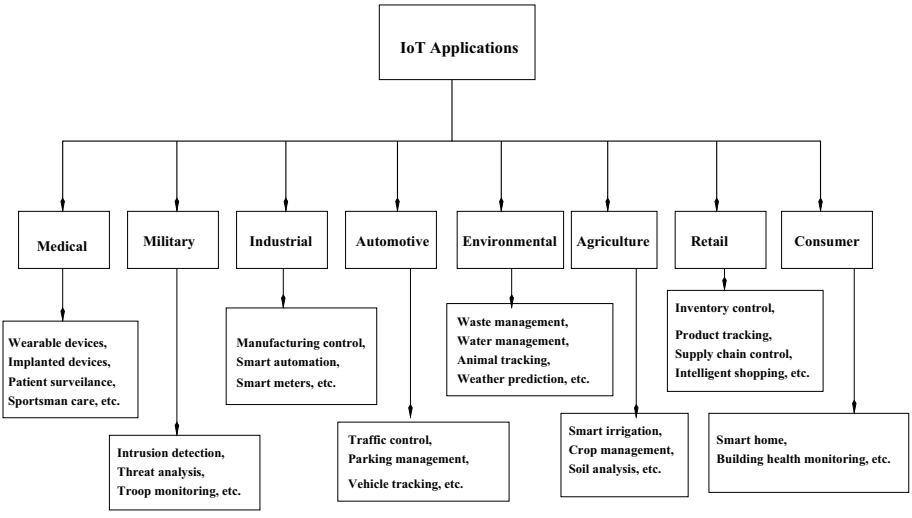

Fig. 7 IoT applications

and privacy. Some of the emerging IoT medical applications are Open Artificial Pancreas System (OpenAPS), Continuous Glucose Monitoring (CGM) system, Connected inhalers, Connected contact lenses, Depression-fighting Apple Watch app, Arthritis - Apples ResearchKit, etc., [35].

The most significant challenges faced by IoT in medical field is data security and privacy. IoT enabled mobile devices capture data in real-time, but most of them lack adherence to data protocols and standards. Due to the heterogeneity of data and communication protocols, it is difficult to aggregate data for vital insights and analysis. IoT collects data in bulk for proper data analysis, the data need to be segregated in chunks without overloading with precise accuracy for better results. Overloading of data might affect the decision making process in the hospital sectors in the longer run and costs are one of the greater challenge when planning to consider IoT app development for health-care mobility solutions.

IoT devices exhibit significant challenges w.r.t. security and privacy. Unauthorized access, Denial of Service (DoS) attacks, tag cloning, spoofing, RF jamming, and cloud polling are the major concerns for IoT applications in medical field. Security protection of wireless and sensor technologies such as WiFi, Bluetooth, ZigBee, UWB, etc., against eavesdropping, sybil attacks, sinkhole attacks, and sleep deprivation attacks must be enforced before deploying the IoT devices for the medical applications. Confidentiality and privacy are important concerns for patients and as well as physicians. Patients may not be interested in disclosing their medical records to the third party because of the data sensitiveness. Major concerns is that the integration of connected technology into medical information systems may compromise the confidentiality of health data [36].

An ECG monitoring based on IoT techniques is presented in [37]. Electrocardiogram (ECG) data are gathered using a wearable monitoring node and are transmitted directly to the IoT cloud using Wi-Fi. Both the Hypertext Transfer Protocol (HTTP) and Message Queuing Telemetry Transport (MQTT) protocols are employed in the IoT cloud in order to provide visual and timely ECG data to users. All smart terminals with a web browser can acquire ECG data conveniently, which has alleviated the cross-platform issue. Results shown that the proposed system is reliable in collecting and displaying real-time ECG data, which can aid in the primary diagnosis of certain heart diseases. A distributed framework based on IoT paradigm for monitoring human biomedical signals in activities involving physical exertion is discussed in [38]. The system is the flexible in computing the health application by using resources from available devices inside the body area network of the user. It can be applied to other mobile environments where intensive data acquisition and high processing is required.

2.2.2 Military Applications

Current military activities are led in a complex, multidimensional, exceedingly unique and problematic condition now and then with unexpected accomplices and irregular adversaries. Military officers have progressively restricted time to get an exact appraisal of the circumstance to survey potential game-plans and decide. Besides, they have to draw from every possible sources to guarantee that the most total and pertinent picture can be made of the circumstance in real time, and understand the implications of their choices and courses of action. And these challenges are to present the idea of IoT into the military domain.

Present day military equipment is relied upon progressively furnished with handling and correspondence capacities, which can be utilized to examine or alter the status of the equipment. To some degree, the equipment could be viewed as sensors or actuators and

integrated into whatever remains of the military data infrastructure. Physical and virtual military things have characters, physical attributes, and virtual identities, use intelligent interfaces, and should be seamlessly integrated into the military data network. In order to accomplish full integration, the relevant security mechanisms, protocol adoptions, and scalability properties must be provided. The possible result of this integration is a more extensive arrangement of sensors and data for use in awareness applications, medical applications, transportation and logistics applications, and so on.

However to provide an efficient IoT applications for military, specific requirements are as follows: decentralized infrastructures, network utilization, interoperability, trust, and security. Some of the prominent IoT applications are disaster relief, battlefield communications, mission critical voice, equipment tracking (such as cars, jeeps, ambulances, tanks, fighter jets, etc.), intrusion detection, threat analysis, workforce training etc., [39].

Security and dependability are the most crucial challenges for the IoT implementation into the military domain. Insufficiently secured military IoT can provide adversary possibility of manipulation or disruption of data transmitted between units or even taking control of or disabling automated systems. The defense mechanisms in traditional computer networks are insufficient due to the high complexity of systems, limited resources of sensors, non reliable communication links and remote management.

Securing the military IoT network ensure strong nodes authentication within network clusters is presented in [40]. To secure data transmission between sensor nodes (SN) and gateways Commercial Off The Shelf (COTS) are used in IoT platforms. These platforms are equipped with Trusted Platform Module (TPM). Cryptomechanism concept is used in the TPM module for strong authentication and protection of the data transmission between sensor nodes.

Wireless Ad-hoc and Sensor Networks (WASN) or opportunistic sensor networks (Oppnets) provide secure communication for military applications. To provide security and privacy in military IoT network, secure route selection and three different encryption algorithms i.e., Commando-Commando (CC), Soldier-Soldier (SS) and Commando-Soldier (CS) communication are discussed in [41]. Routing is based on Path Protected Hop-by-Hop routing protocol (PPHH) by which a secure path is selected with authentication by certificate authority (CA). The code-based cryptography, hyper elliptic curve cryptography, and design-based cryptography algorithms are used for secure and reliable communication and protect the valuable data.

2.2.3 Industrial Applications

Industrial applications integrated with IoT are called as Industrial Internet of Things (IIoT). The IIoT enables companies to gather, aggregate, and analyze information from sensors to maximize the effectiveness of machines and throughput of an entire operation. Applications include manufacturing control, smart meters, smart automation, motion control, machine-to-machine, predictive maintenance, smart grid [42].

Some of the major challenges faced by industry in integrating IoT are interoperability, security, data analysis and transfer, information technology and operational technology convergence. Industrial Block chain Tokenizer (IBT) based on an industrial data acquisition system to gather data from both modern and legacy machines interfaced with sensors is presented in [43]. Acquired data is processed locally by enabling an edge filtering paradigm to any blockchain platform. The system is tested on two supply chain scenarios. Tests reveal that the system has capability to act as a bridge between

industrial assets and blockchain platforms. This leads to the generation of immutable and trust-less "digital twins" for industrial IoT applications.

Implementation of task allocation and secure deduplication mechanisms over four layers of fog assisted cluster-based industrial IoT is discussed in [44]. IoT device layer is used to sense data and mitigate security threats. Devices are registered to the cloud server using Elliptic Curve Cryptography based Hybrid Multiplier (ECC HM). Multi-Objective based Whale Optimization algorithm is used for clustering. SHA-3 is used for secure data deduplication. ECC HM private key is used for data encryption. In cloud, layer indexing is constructed using Merkle Hash Tree. This provides query search results for IoT users at the service layer. The results show the enhancement in average latency, user satisfaction, network lifetime, energy consumption, and security strength. An IIoT gateway can help the existing device infrastructure to securely connect any industrial infrastructure [45]. Distributed edge computing helps in fast data transfer and real-time data analysis, enabling faster fault response time. IoT gateway clustering helps in ensuring the continuity of cloud communication and storage of data to resolve the problem of information technology and operational technology.

2.2.4 Automotive Applications

Daily traffic in cities can be managed using sensors and intelligent transportation systems. The most important goal of the intelligent transportation systems is to decrease traffic jam, free parking and avoid accidents by traffic and spotting drunk drivers. The sensor advancements overseeing these types of applications are GPS sensors for area, accelerometers for speed, gyrators for heading, RFIDs for vehicle identification, infrared sensors for tallying travelers and vehicles, and cameras for recording vehicle development and traffic [46, 47]. Vehicles are associated with each other by the cloud and a large group of IoT gadgets. These gadgets can assess traffic conditions in various parts of the city, urban and highway scenario. Custom applications can examine traffic designs with the goal that future traffic conditions can be assessed. Some of the emerging automotive IoT applications are parking management, crash response, car problem diagnosis, integrated navigation, infotainment and critical information assistance etc. The unprecedented demand of vehicle monitoring sensors can lead to packet collisions, severe network congestion and lost of time-critical data. As the number of sensors in vehicles increase rapidly, there is a risk of hackers who steal Personally Identifiable Information (PII) from the vehicle's systems. Information may be personal trip, location data, entertainment preferences, financial information, etc.

Vehicle Telematics is one important solution of IoT automotive. Telematics refers to the long transmission of computerized data. By using vehicular telematics a car owner can keep an eagle eye view on vehicle even from remote locations. Connected cars facilitate fast transmission of data and increase drivers' response time through enhanced vehicle communication [48]. An enhanced MAC scheme scalable for diversed sensor-traffic quality of services is presented in [49]. The hybrid scheme combine two procedures, namely history and priority based MAC to allocate appropriate network resources for smooth transmission flow from multiple sensors. History based MAC exploits historical contention of data to optimize a near future contention window. This minimizes packet collision and expedite the average of data delivery. Priority based MAC assigns the time-criticality of the sensing data, which is subsequently used to schedule network resources.

2.2.5 Environmental Applications

The applications of IoT in environmental monitoring include waste management, water management, animal tracking, weather monitoring and prediction, environmental protection, endangered species protection, commercial farming, etc. Things detect and measure every type of environmental change in these applications [50]. The term smart environment is defined as a technology that provides many facilities and solutions for many environmental application issues related to water quality and health, air pollution, weather, radiation monitoring, waste management, natural disaster, and many other environment indicators.

A Conservative Data Analytical Model (CDAM) for real time data evaluation and remittance is discussed in [51]. This model is based on the factors of correlation and conditional similarity verification for remitting reliable information across the reporting system. The correlation analysis model is preceded using fuzzy derivatives for deriving possible solutions. The CDAM is tested with the available real-time weather information for predicting dynamic climatic changes and shows improvement in correlation accuracy and data analysis rate by reducing the error rate. A bio-inspired IoT architecture allows flexible creation and discovery of sensor-based services offering self-organization and self-optimization properties to the dynamic network [52]. This technique is also known as Hot–Cold, to ensure proximity maintenance by the tracking robotic device solely based on the strength of the radio frequency signal broadcasted by the target to communicate sensor data.

Smart environment sensors such as AirBot, WaterBot, Sensordrone, Air Quality Egg, Lapka, and wearable sensor integrated with IoT provide a new concept in tracking, sensing and monitoring objects of environment. This provides benefits leading up to the possibility of achieving a green world and a sustainable lifestyle. IoT allows environmental sensors to connect with other systems such as smart phones through Bluetooth or WiFi to send enormous amounts of data to the network. This allows a better understanding of surroundings and find suitable solutions for environmental problems [53].

2.2.6 Agriculture Applications

IoT technologies in smart forming will empower growers and farmers to diminish waste and upgrade efficiency ranging from the amount of fertilizer used to the quantity of journeys the farm vehicles have made. Some of the applications of IoT in agriculture are soil analysis, precision farming, agricultural drones, livestock monitoring, smart greenhouses, etc., [54]. Monitoring the climatic parameters such as (temperature, humidity, light, carbon dioxide, soil moisture, acidity, etc.) in an agriculture field is a challenging task. The climatic parameters are very important in terms of growth, quality and productivity of crops. But any kind of interception, modification, insertion, and deletion on these parameters can have negative effect on crop. Therefore, security and privacy are important issues in agriculture field.

Agricultural products need security and protection at very initial stage, like protection from attacks of rodents or insects, in fields or grain stores. An intelligent security systems Internet Protocol (IP) based Closed Circuit Television (CCTV) cameras used to identify motion of rodents and distance of rodents using heat sensor [55]. Based on the distance calculated by ultrasonic ranging device, repeller will be activated with a particular frequency within range (30kHz to 65kHz) which is aversive to rodents. Simultaneously webcam daemon is activated to capture a snap of area. Further, a Short Message Service (SMS)

will be sent to user through IP address of the server to access webcam daemon lively. IoT monitoring modules for agriculture applications using various sensors for which the inputs are fed from Knowledge base are demonstrated in [56]. A prototype of the mechanism is exhibited using TI CC3200 Launchpad with interconnected sensor modules with other necessary electronic devices. The system overcomes limitations of traditional agricultural procedures by utilizing water resource efficiently and also reducing labor cost.

2.2.7 Retail Applications

With the fast improvement of online shopping, retailers rush to bring the frictionless customer experience of online shopping into the store wherever they can. They require access to a similar type of rich data and best performance analytics that retailers use to drive websites and mobile shopping trips. Their aim is to have that same boundless control to make a client experience and gather detailed information to enable them to predict how customers will shop. Supply chain connected consumer and smart-store applications are the key applications of IoT for retail [57]. Some challenges for retail IoT applications are infrastructure, security and privacy of users. Most retailers lack the infrastructure and network components that huge volumes of IoT data require. Carrying out IoT data analysis in a timely and relevant manner represents a major challenge for retail businesses due to a lack of relevant qualifications and expertise.

A Blockchain enabled Logistics Finance Execution Platform (BcLFEP) is integrated to facilitate Logistics Finance (LF) for E-commerce retail applications are presented in [58]. A cross-layered architecture is involved in resources, workflows and decisions based on the Object-Oriented Methodology (OOM). A Hybrid Finite State Machine-based Smart Contract (HFSM-SC) is designed to associate and coordinate with all kinds of agents for LF operations throughout its life cycle. Blockchain is integrated with agent technology to construct a Blockchain enabled Multi-Agent System (BcMAS), providing a trusted runtime environment to autonomously and efficiently execute smart contract. To protect customers data, Markovian game technique is used with detailed states, actions, strategies and transitions available for data holder to achieve a compromise between privacy concessions and incentive motivation offered by data requester [59].

Retailers should work closely with IoT software developers to make sure that the devices and sensors are designed with strong security mechanisms in mind, including secure passwords, end-to-end encryption, regular software updates and an IT infrastructure that actively scans for bugs and vulnerabilities. Encryption can be used to protect the data produced by IoT at the application level protecting sensitive data. Access to this data using Payment Card Industry Data Security Standard (PCIDSS) is ideal for retail businesses [60].

2.2.8 Consumer Applications

IoT creates new possibilities for both businesses and consumers. The IoT allows users armed with hand-held computers to access and control devices remotely. As Internet access becomes ubiquitous, any device with a power switch is being enabled for remote control via the Internet. There are innumerable consumer applications for IoT technology such as automated home, connected cars, building health monitoring, etc., [61]. Some challenges for consumer IoT applications are machines actions in unpredictable situations, information security and privacy, machine interoperability, mean reverting human behaviors and slow adoption of new technologies.

Content Centric Networking (CCN) protocol and a novel consumer driven information freshness approach is discussed in [62] to satisfy the consumers needs while mitigating the negative effect of the freshness requirements in the overall network performance. The prototype of home automation provides users to remotely switch on and off home appliances using IoT concept with the option of solar charger [63]. The prototype uses four types of sensors i.e., PIR sensor, temperature sensor, ultrasonic sensor and smoke gas sensor for automatic environmental control and intrusion detection.

A cloud-centric IoT application store that serves a purpose for hosting virtual objects of different IoT domains to build IoT applications is discussed in [64]. The proposed system provide full-fledged IoT applications which include software and hardware that users can plug and play. The application store is decoupled and can expose virtual objects of different IoT domains. The system is modular, scalable, secure and support heterogeneity, which are considered vital attributes of IoT applications. An IoT testbed client application is mentioned in the system to reuse some of the virtual objects from the application store and to share specialized virtual objects for the use of other clients applications.

3 Research Challenges in IoT

Internet of Things attracted the scientists and researchers for its wide range of applications [65]. In IoT, still much more research works need to be done to make this concept in realization. Figure 8 depicts the major research challenges in IoT.

3.1 Monitoring and Sensing

Monitoring and sensing technologies have achieved significant maturity level in IoT. But energy-efficiency and form factor efficient mechanisms are still need to be addressed. As RFID tags and sensors acquire real-time data, energy-efficient mechanisms are highly important for network lifetime extension. Recent developments in miniaturization have enabled the development of sensors at the nano-scale [66, 67].

3.2 M2M Communication

Machine-to-Machine (M2M) communication is a Point-to-Point communication usually embedded within the "Things" and Network. Some of the possible wireless technology are Bluetooth Low Energy and LoRa [68], ZigBee, and UWB. Recent IoT oriented

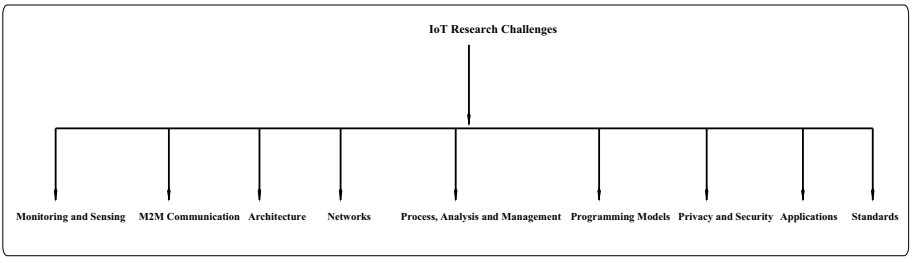

Fig. 8 IoT research challenges

communication protocols use MQTT [69], Constrained Application Protocol (CoAP) [70], Software Defined Networking (SDN) and Network Function Visualization (NFV) techniques [71, 72]. However still the visualization capabilities in things or objects, application fulfillment at lower costs are need to be addressed.

3.3 Architecture

There are several architectures for IoT have been proposed by researchers. But still lot of issues/challenges are limiting the effectiveness and performance of the IoT. Some of the major challenges related to the IoT architectures are communication, data management, scalability, real-time applications, security and privacy, interoperability, lack of standardization, etc.

3.4 Networks

IoT networking technologies have an impact on the design of IoT devices. In IoT devices (things/objects) network range, data rate and power consumption are directly related to networking technologies. For example, if network range and volume of data that is transmitted is increased, IoT devices will require additional power to transmit the data under those conditions. If the devices are directly powered (e.g., in home automation applications), power consideration criteria is of low importance. Effective bandwidth usage and connection stability are also important issues in IoT networking technologies.

3.5 Process, Analysis and Management

Managing, processing, analyzing information is truly difficult task due to the heterogeneity and the scale of collected data. The current tendency is to use centralized solutions to offload information and execute computationally concentrated task on a worldwide cloud platform. However, there is an increasing concern that traditional cloud designs will be unable to exchange the massive volume of information formed and consumed by IoT objects and to maintain the related computational load while gathering timing constraints. Emerging computing techniques such as fog computing and mobile cloud computing rely on edge processing to address this challenge [73–75].

3.6 Programming Models

Due to the different nature of IoT, different approaches to programming IoT applications are needed. For IoT applications and services that are focused on edge gadgets and work within a single domain e.g., a manufacturing plant or machine, programming models have a tends to use the standards of real time and embedded computing. For Smart buildings or smart cities [76] applications the utilization of cloud based programming models with synchronous and asynchronous APIs are explored in [77]. One promising method is the utilization of information flow programming models to process streams of procedures from IoT objects asynchronously is recently explored by research community. To accommodate the dispersed nature of IoT applications, Distributed Data Flow (DDF) proposed as a potential answer and is now an active research area [78]. Responsive programming also built on

an information flow model has newly gained footing in the IoT community with different research groups to explore dynamic and functional variants in IoT programme model.

3.7 Privacy and Security

Researchers have more information about the vulnerabilities existing in various IoT devices [79]. New attacks on IoT structure present the complete security system to protect system and information from end to end. The threat attack exploit weakness in individual device to enter a structure and access gadgets that are more secure from the outside is a driving inspiration for complete security solutions. This includes research in good cryptography technique for both system and data security [80], non-cryptographic techniques for security [81] and frameworks help developers to develop secure systems on heterogeneous devices more easily [82]. Cryptographic security solutions that fit for running on resource constrained IoT devices, we need research to activate users of all ability levels to safely transmit and use IoT system in spite of the limited user interface accessible with most IoT gadgets.

3.8 Applications

To make IoT applications work easily as an independent arrangement or part of existing system, there are numerous technological challenges such as security, privacy, connectivity, compatibility, longevity, standards and intelligent analysis and actions are need to be addressed.

3.9 Standards

Dynamic evolution of IoT business has created an opportunity for variety of IoT solutions. As the business develops, necessitate for a standard model to execute basic IoT back-end tasks are critically required. For example processing, storage, and firmware updates are becoming more popular IoT applications. Upcoming IoT standards should guarantee levels of interoperability, portability and manageability.

4 Security and Privacy Issues in IoT

Security is one important issue in IoT and plays vital role in the successful deployment of IoT at the root level [83]. The security solutions must be lightweight, means security solutions are able to operate in low memory, low computation power, and low cost devices/objects. There are many security solutions available, even so for the constrained objects, but these are considered only for single constrained devices and not for the integration into the IoT. The heterogeneity of devices, their varied computational specifications and complexity of the network points to the need for security solutions should be lightweight and operated with global standards [84].

Privacy is the privilege of an element (individual) to confirm the amount of data it will impart to other people [85]. Because privacy will become a serious matter in IoT system. A set of allocated data of a man can be composed without the awareness of the individual. It is impossible to control on the diffusion of all such data is in current situation. So the

clients of the IoT scheme need to deal their own particular data. The owner should know who are utilizing their data and when it is utilized. A general framework for privacy in IoT and inventive enforcement method which will support scalability in heterogeneity of the IoT condition should be produced by the researchers [86]. This section presents the ongoing research works and research challenges still exist to provide privacy and security in IoT.

4.1 Security in IOT

IoT security is the area of undertaking worried about protecting associated devices and systems in IoT. The security hierarchy structure of the IoT shows different security technologies can be adopted in different layers. The sensation layer is extremely vulnerable to suffer security attacks, it mainly uses attack detection and intrusion response techniques to resist illegal attacks effectively; the network layer mainly aims at security technologies of the network environment, such as wireless network security, secure routing, firewall and so on, to realize safe network interconnection; the application layer guarantees the security of application system through user authentication and access control. Some of the important issues of IoT security are Authentication, Confidentiality, Integrity and Availability.

4.1.1 Authentication

In Internet, users authenticate by providing a secret key and browsers authenticate web sites by the Secure Sockets Layer (SSL) protocol. Now a day's passwords are also not good for Internet-scale authentication. So password mechanism is still worse for IoT scale authentication. Authentication is very important security issue and is sorely needed in IoT to secure the information from unauthorized people. In IoT, heterogeneous devices must confirm to the local gateway when transferring the information. Then the local gateway should confirm (authenticate) to the cloud endpoint when transferring this information. The applications should authenticate to the cloud when requesting the information. Allowing any user or gadget to avail the data from the IoT condition is called authorization. With proper identity, anyone can get to the data from the IoT condition. Without authorization, nobody can get to any information or administration from this condition.

Authentication will be the procedure from claiming checking those innovations of the user or substance taking an interest in the communication [87]. A significant number of gadgets utilize the sensors and actuators to take after specific intermediatary authentication to authorize to public their information. Meanwhile, minimal effort arrangements in this field have not been given as much as required [88]. Currently, we need to give the security for the sensors and we need to utilize expense solutions which are a conflict with the principle objective of IoT to give lightweight protocols [89]. Existing IoT authentication literature for secure transmission of data is presented in [90]. The authentication and access control technique described in [91] goes for shaping the session key on the source of lightweight encryption component and Elliptic Curve Cryptography (ECC). This plan defines attribute based access control arrangements, overseen by a quality specialist, upgrading common authentication among the user and the sensor nodes, and in addition settling the resource-constrained issue at application level in IoT. Efficient device authentication protocol without certification specialist for the IoT is introduced in [92]. An object authentication structure is proposed to abuse device specific data called as fingerprints to authenticate objects in IoT utilizing an exchange learning tools adequately track the impacts of physical

condition on objects fingerprints [93]. Authentication mechanisms requirements for IoT are presented in [94].

IoT challenges and authorization mechanisms in IoT are mentioned in [95]. A delegation structure that off-loads the connection establishment to a delegation server and solution for authorization, authentication and secure information transmission in the IP-based IoT is mentioned in [96]. A safe and dispersed configuration, authorization and organization across network borders in cloud based IoT is mentioned in [97]. Reliable network control across network borders and solid security ensures are accomplished. A preparation of lightweight authentication and authorization mechanisms with a specific end goal to support smart objects during their life cycle is discussed in [98]. A privacy-preserving authentication protocol using code-based cryptosystem for IoT environments is presented in [99]. The code-based cryptography is an important post-quantum cryptography that can resist quantum attacks.

4.1.2 Confidentiality

In IoT, billions of objects are part of the Internet. A large amount of private data generated by these objects need to be processed, transferred with confidentiality and stored. Traditional confidentiality algorithms exhibit many challenges for this task. For IoT confidentiality, solutions have to deal with high scalability requirements, heterogeneity of the involved building blocks, in addition to resources scarcity of the embedded devices such as energy and computational limitations. Data confidentiality in IoT is a main constraint that guarantees access and alteration to certify entities via an access control system and object authentication practice with a related identity supervision system. Defining an object authentication method and an access control system are two important concepts in the confidentiality.

Explanation of an appropriate query language for permitting applications to improve the desired information identified with confidentiality in an IoT scenario is described in [100]. Security architecture with reference to the confidentiality, security issues and privacy of the user are proposed in [101]. Author gave higher priority to the security of IoT and addresses the difficulties of scalability, availability and security of IoT.

4.1.3 Integrity

Integrity in IoT means data from devices/objects or platforms need to be checked for being processed to ensure that the data and its flow can be trusted. If proper integrity measurements cannot be taken in IoT, gadget can't work accurately, gadgets turn to be abused and a traded off stage from which different attacks can be launched. Integrity as the guarantee of the received information that has not been altered in transit [102]. A characteristic of the objects is unpredictable and it is extremely difficult to decide the first source of the information. There is a mess in utilize of trusted devices and data. Information protections with passwords are too short in IoT technologies and trusted computing solutions are to be established to maintain integrity of information and devices.

Integrity solutions for IoT involves in the data being generated or used by its own programming data. This includes all aspects of program software, configuration parameters and operating system software. To give the integrity solutions for IoT, it is useful to consider three distinct states that information can exist: in-motion, at rest and in process. Information in-motion requires that information be protected from modification while on its journey from sensor to cloud application. For information at rest stored programme

information will be verified and that will be done at boot time. In process, periodic integrity checks can be made during operation and always at start-up and shutdown.

Integrity refers to the protection of helpful data from the cyber criminals or the outer physical interference during communication with some normal tracking techniques, so the information altering is impossible without the system getting the threats [103]. This ensures the uniqueness of message including some technique like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. The traditional method of verifying the integrity of information is by a mathematical algorithm called as a hash of which the Secure Hash Algorithm (SHA) is most regularly utilized [104]. A hash technique may be used by an attacker to make a change to the message and recalculate the hash. Data integrity prevents any man-in-the middle modification to data by guarantee that data arriving at the receiver node is in unaltered shape and stays as transmitted by the sender. The framework for integrity protection well suited for IoT environment is described in [105]. Different integrity detection methods are examined and thought about and some promising and potential research directions on integrity detection are mentioned in [106].

4.1.4 Availability

In IoT, data gathered should be available at the back-end of the service may be on the private cloud or a public cloud. It is important to realize that the service and its data should be always available. Data availability ensures the immediate access of authorized party to their information resources. In IoT, many objects are connected to the Internet with full or limited connectivity. These objects may be exposed to attackers if not secured-by-design. Hence it is required to update them periodically or frequently to patch their vulnerabilities and to prevent hackers.

Availability involves recoverability and reliability [107]. Availability of IoT includes programming and hardware levels being given at whenever and anyplace to benefit supporters. Software availability means that the service is given to any individual who is authorized to have it. Hardware availability means that existing gadgets are easy to access and are compatibility with IoT functionality and protocols [108]. IoT challenges as well as the security challenges of various layers based on the security principles of data confidentiality, integrity and availability are presented in [109]. Different IoT layers with security problems are mentioned in [110]. IoT vulnerabilities facilitating the attacks are key considerations in ensuring information security.

4.2 Privacy

IoT privacy is the greater considerations required to keep information safe of individuals from exposure in IoT environment [111]. It is desired to provide unique identifier and the capability to communicate autonomously over the Internet to give physical or logical entity. As objects in the IoT environment transmit data autonomously, privacy is critically required. Interoperability of things is also essential to the IoT functioning. The information transmitted by a given endpoint probably won't cause any privacy issues on its own. However, when even fragmented information from different endpoints is assembled, grouped and analyzed, it can yield sensitive information. It is the right of an entity (person) to verify the quantity of information it is willing to share with others. Set of data of a person can be made without the awareness of the person. Control

on the dissemination of all such data is impossible in current scenario. So, the users of the IoT scheme need to deal their own information. The owners should know who are using their information and when it is used. A general system for protection in IoT and inventive authorization procedures which will bolster versatility in heterogeneity of the IoT condition is presented in [112]. Future opportunities, trends and recommendations about the privacy for IoT based applications and services are discussed in [113].

Three main axes of research activities in data privacy i.e., collection, sharing and management, and security issues are discussed in [114]. Privacy in data collection involves in different technologies for different qualities for energy, connectivity, ability etc. Specially in IoT, information are collected from various components including RFID tags and readers, wireless sensor networks, mobiles phones with 3G and WiFi connectivity, GPS terminals, etc. This openness might lead an immediate impact with respect to information privacy also might infer certain dangers. Privacy in data sharing and management is a critical issue for IoT. Because a big amount of information is replaced over the network between IoT modules. These data are frequently human centric and need to be correctly protected. From a practical point of view, infrastructures passing on this information might a chance to be imparted between large portions substances or networks with diverse security practices and policies. Also, the frequent utilization of wireless communication and other diffusion based networks might prompt information revelation assuming that sufficient precautions have not been made. Information security issues concerned, information might be put away and handled in the collection nodes. Lasting for a variable time in channels may lead to data integrity and confidentiality issues. Hence sufficient components necessity on be tended to should stay away from these dangers.

5 Conclusion

In this survey paper, IoT architectures, applications and research challenges are highlighted. As per the literature survey, there is a lack of a efficient privacy and security algorithms for IoT. Most of the privacy and security algorithms for IoT are still in implementation stage under several assumptions. However, those algorithms are known to be extremely demanding in terms of CPU, energy and memory resources. Their usage in the setting of the IoT might a chance to be really going a greater amount complicated. Therefore, new lightweight strategies would require to guarantee information minimization. However, the feasibility and optimization of this kind of design is still an open issue. In IoT, objects and platforms are required to share their personal or confidential information. In this case, how to balance the privacy and security is still an open issue. Moreover to detect the malicious objects is also very important during the communication process. Detection of a malicious object may cause increase in latency. Therefore, how to balance the algorithm performance and security is still an open challenge.

In IoT, it is important to implement applications with privacy and security features that respect the data minimization principle and give priority to data control rather than data collection. Hence, there will be a compelling reason for creating IoT standard to meet an addition level of security and privacy in practice. Finally, security mechanism must be expounded to permit users ensuring their private information as opposed to expecting actualized components in IoT frameworks to regard their privacy.

References

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements and future directions. *Journal of Future Generation Computer Systems*, *29*(7), 1645–1660.
2. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Journal of Computer Network*, *54*(15), 2787–2805.
3. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Journal of Wireless Personal Communications*, *58*(1), 49–69.
4. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Journal of Ad Hoc Networks*, *10*(7), 1497–1516.
5. Yang, D., Liu, F., & Liang, Y. (2010). A survey of internet of things. In *Proceedings of The international conference on E-business intelligence (ICEBI2010)* (Vol. 978, pp. 78–99), Kunming, China.
6. Vision and challenges for realising the internet of things. *Cluster of European Research Projects on the Internet of Things*, European Commission Information Society and Media, 2010.
7. Internet of things: Converging technologies for smart environments and integrated ecosystems. *River Publishers*, 2013.
8. Internet of things market value networks and business models: State of the art report. *University of Jyvaskyla*, 2013.
9. Covington, M., & Carskadden, R. (2013). Threat implications of the internet of things. In *Proceedings of the 5th international conference on cyber conflict* (pp. 1–12), Estonia.
10. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Journal of Computer Network*, *44*(9), 51–58.
11. Mardiana, B., Mohamad, N., & Haslina, H. W. (2019). Current research on internet of things (IoT) security: A survey. *Journal of Computer Networks*, *148*, 283–294.
12. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the internet of things: A review. In *Proceedings of The IEEE international conference on computer science and electronics engineering* (Vol. 3. pp. 648–651), China.
13. Yang, G., Xu, J., Chen, W., Qi, Z. H., & Wang, H. Y. (2010). Security characteristic and technology in the internet of things. *Journal of Nanjing University of Posts and Telecommunications*, **30**(4).
14. Internet of things strategic research roadmap. http://www.internet-of-things-research.eu/pdf...pdf.
15. Pan, J., Paul, S., & Jain, R. (2011). A survey of the research on future internet architectures. *IEEE Communications Magazine*, *49*(7), 26–36.
16. Jala, A., Mohsen, G., Mehdi, M., Mohammed, A., & Moussa, A. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communication Surveys and Tutorials*, *17*(4), 2347–2376.
17. Farooq, M. U., Waseem, M., Mazhar, S., Khairi, A., & Kamal, T. (2015). A review on internet of things (IoT). *Journal of Computer Applications*, *113*(1), 1–7.
18. Sonar, K., & Upadhyay, H. (2014). A survey: DDOS attack on internet of things. *Journal of Engineering Research and Development*, *10*(11), 58–63.
19. Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. *Journal of Networking and Applications*, *6*(4), 2372–2378.
20. Akanksha, T., & Gupta, B. B. (2020). Security, privacy and trust of different layers in internet of things (IoTs) frameworks. *Journal of Future Generation Computer Systems*, *108*, 909–920.
21. Altaf, A., Abbas, H., Iqbal, F., & Derhab, A. (2019). Trust models of internet of smart things: A survey, open issues, and future directions. *Journal of Network and Computer Applications*, *137*, 93–111.
22. Yinghui, H., & Guanyu, L. (2010). Descriptive models for internet of things. In *Proceedings of the IEEE international conference on intelligent control and information processing* (pp. 483–486), China.
23. Mealling, M. (2003). Auto-ID object name service (ONS) v1.0. *Auto-ID Center Working Draft*.
24. Miao, W., Ting, L., Fei, L., Ling, S., & Hui D. (2010). Research on the architecture of internet of things. In *Proceedings of the IEEE international conference on advanced computer theory and engineering* (pp. 484–487), China.
25. Jinxin, Z., & Mangui, L. (2010). A new architecture for converged internet of things. In *Proceedings of the international conference on internet technology and applications* (pp. 1–4), Brazil.
26. Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. In *Proceedings of The 11th international conference on wireless communications, networking and mobile computing (WiCOM 2015)* (pp. 1–5), China.

27. Inge, G. (2008). Architecture for the internet of things (IoT): API and interconnect. In *Proceedings of the 2nd international conference on sensor technologies and applications* (pp. 802–807), Syria.
28. Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on internet and underlying issues. *Journal of Ad Hoc Networks*, *28*, 68–90.
29. Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *Journal of Computer Networks*, *5*(1), 1–17.
30. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of internet of things. In *Proceedings of the 3rd IEEE international conference on advanced computer theory and engineering*, China.
31. Chowdhury, S. N., Kuhikar, S. M., & Dhawan, S. (2015). IoT architecture: A survey. *Journal of Industrial Electronics and Electrical Engineering*, *3*(5), 88–92.
32. Sethi, P., & Sarang, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*, *17*, 1–25.
33. Mohmmad, S., Sirajuddin, M., & Shabana, (2016). IoT middleware for device privacy on big data. *Journal of Innovative Research in Science, Engineering and Technology*, *5*(6), 10266–10273.
34. Zaidan, A. A., & Zaidan, B. B. (2020). A review on intelligent process for smart home applications based on IoT: Coherent taxonomy, motivation, open challenges and recommendations. *Journal of Artificial Intelligence Review*, *53*, 141–165.
35. https://econsultancy.com/blog/68878-10-examples-of-the-internet-of-things-in-healthcare.
36. Zeadally, S., Siddiqui, F., Baig, Z., & Ibrahim, A. (2019). Smart health care challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Research Review*. https://www.emerald.com/insight/content/doi/10.1108/PRR-08-2019-0027/...-analytics.
37. Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud based wearable ECG monitoring system for smart health care. *Journal of Medical Systems*, *40*(12), 286–296.
38. Gil, D., Terol, R. M., Azor, J., & Szymanski, J. (2017). An IoT-based computational framework for healthcare monitoring in mobile environments. *Sensors*, *17*(10), 1–25.
39. Fraga-Lamas, P., Fernández-Caramás, T. M., Suárez-Albela, M., Castedo, L., & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, *16*, 1644.
40. Zielinski, Z., Chudzikiewicz, J., & FurtakAn, J. (2019). Approach to integrating security and fault tolerance mechanisms into the military IoT: Technology, communications and computing. In *Security and fault tolerance in internet of things* (pp. 111–128).
41. Arafath, M. S., Khan, R., Ur, K., & Sunitha, K. V. N. (2017). Incorporating privacy and security in military application based on opportunistic sensor network. *Journal of Internet Technology and Secured Transactions*, *7*(4), 295–316.
42. https://www.raconteur.net/technology/top-5-applications-for-the-industrial-internet-of-things.
43. Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., et al. (2020). A blockchain tokenizer for industrial IoT trustless applications. *Journal of Future Generation Computer Systems*, *105*, 432–445.
44. Sharma, S., & Sain, H. (2020). Fog assisted task allocation and secure deduplication using 2FBO and MoWo in cluster-based industrial IoT (IIoT). *Journal of Computer Communications*, *152*, 187–199.
45. Sisinni, E., Saifullah, A., Han, S., & Jennehag, U. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, *17*, 4724–4734.
46. https://www.tutorialspoint.com…monitoring.html.
47. Dimitrakopoulos, M. G. (2011). Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges. In *Proceedings of The 11th IEEE international conference on information technology and system telecommunications* (pp. 145–151), Cyprus.
48. Rukmini, M. S. S., & Usha Devi, Y. (2016). IoT in connected vehicles: Challenges and issues— A review. In *Proceedings of The IEEE international conference on signal processing, communication, power and embedded system (SCOPES)* (pp. 1864–1867), Paralakhemundi.
49. Rahmana, M. A., Asyharib, T., Kurniawan, I. F., Ali, M. J., Rahman, M. M., & Karima, M. (2020). A scalable hybrid MAC strategy for traffic-differentiated IoT-enabled intra vehicular networks. *Journal of Computer Communications*, *157*, 320–328.
50. Li, H., Wang, H., Tao, X., & Zhou, G. (2011). Application study on internet of things in environment protection field. *Journal of Informatics in Control, Automation and Robotics*, *2*, 99–106.
51. Ma, J., Yu, H., Xu, Y., & Deng, K. (2020). CDAM: Conservative data analytical model for dynamic climate information evaluation using intelligent IoT environment–an application perspective. *Journal of Computer Communications*, *150*, 177–184.
52. Lagkas, T., Eleftherakis, G., Dimopoulos, K., & Zhang, J. (2020). Signal strength based scheme for following mobile IoT devices in dynamic environments. *Journal of Pervasive and Mobile Computing*, *65*, 1–24.

53. Elmustafa, S. A. A., & Mujtaba, E. Y. (2019). Internet of things in smart environment: Concept, applications, challenges, and future directions. *International Scientific Journal*, *134*, 1–51.
54. https://www.iotforall.com/iot-applications-in-agriculture.
55. Punitha, A., & Geetha, V. (2018). Review on challenges and opportunities of IoT in agriculture. *Journalof Advanced Research in Applied Science*, *5*(11), 25–31.
56. Mohanraj, I., Ashokumar, K., & Naren, J. (2016). Field monitoring and automation using IoT in agriculture domain. *Journal of Procedia Computer Science*, *93*, 931–939.
57. https://www.sas.com/en_us/insights/articles/big-data/five-iot-applications-retailers-are-using-today.html.
58. Li, M., Shao, S., Ye, Q., Gangyan, X., & Huangg, G. Q. (2020). Blockchain enabled logistics finance execution platform for capital constrained e-commerce retail. *Journal of Robotics and Computer Integrated Manufacturing*, *65*, 1–14.
59. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2017). A Markov game privacy preserving model in retail applications. In *Proceedings of the international conference on selected topics in mobile and wireless networking (MoWNeT)* (pp. 1–14), Avignon.
60. Dlamini, N. N., & Johnston, K. (2016). The use, benefits and challenges of using the internet of things (IoT) in retail businesses—A literature review. In *Proceedings of the international conference on advances in computing and communication engineering (ICACCE)* (pp. 430–437), Durban.
61. http://www.ingrammicroadvisor.com/data-center/internet-of-things-examples-for-the-connected-consumer.
62. Quevedo, J., Corujo, D., & Aguiar, R. (2014). Consumer driven information freshness approach for content centric networking. In *Proceedings of the IEEE information centric networking to support disastar management workshop on name-oriented mobility* (pp. 482–487), Canada.
63. Gunawan, T. S., et al. (2017). Prototype design of smart home system using internet of things. *Indonesian Journal of Electrical Engineering and Computer Science*, *07*(07), 107–115.
64. Ahmad, S., Mehmood, F., Mehmood, A., & Kim, D. H. (2019). Design and implementation of decoupled IoT application store: A novel prototype for virtual objects sharing and discovery. *Electronics*, *08*(285), 1–31.
65. Borgia, E., Gomes, D. G., Lagesse, B., Lea, R., & Puccinelli, D. (2016). Special issue on internet of things: Research challenges and solutions. *Journal of Computer Communications*, *89*(4), 1–4.
66. Akyildiz, F., Pierobon, M., Balasubramaniam, S., & Koucheryavy, Y. (2015). The internet of bio-nano things. *Journal of IEEE Communication and Management*, *53*(3), 32–40.
67. Akyildiz, I., & Jornet, J. (2010). The internet of nano-things. *Journal of IEEE Wireless Communication*, *17*(6), 58–63.
68. Bor, M., Vidler, J., & Roedig, U. (2016). LoRa for the internet of things. In *Proceedings of the international conference on embedded wireless systems and networks* (pp. 361–366), Austria.
69. International Business Machines Corporation (IBM)—Eurotech, MQTT V3.1 Protocol Specification, 2010. http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt- v3r1.html.
70. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An application protocol for billions of tiny internet nodes. *Journal of IEEE Internet Computing*, *16*(2), 62–76.
71. Manzalini, A., Minerva, R., Callegati, F., Cerroni, W., & Campi, A. (2013). Clouds of virtual machines in edge networks. *Journal of IEEE Communication Magazine*, *51*(7), 63–70.
72. Ravindran, R., Liu , X., Chakraborti, A., Zhang, X., & Wang, G. (2013). Towards software defined ICN based edge-cloud services. In *Proceedings of The IEEE 2nd international conference on cloud networking* (pp. 22–235), Spain.
73. Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the mobile cloud computing* (pp. 13–16), Helsinki.
74. Shi , C., Ammar , M. H., Zegura, E. W., & Naik, M. (2012). Computing in cirrus clouds: The challenge of intermittent connectivity. In *Proceedings of the mobile cloud computing* (pp. 23–28), Helsinki.
75. Borgia, E., Bruno, R., Conti, M., Mascitti, D., & Passarella, A. (2016). Mobile edge clouds for information-centric IoT services. In *Proceedings of the IEEE symposium on computers and communications* (pp. 1–7), Italy.
76. Lea, R., & Blackstock, M. (2014). City hub: A cloud-based IoT platform for smart cities. In *Proceedings of the 6th IEEE conference on cloud computing technology and science* (pp. 799–804), Singapore.
77. Giang, N. K., Blackstock, M., Lea, R., & Leung, V. C. M. (2015). Developing IoT applications in the fog: A distributed dataflow approach. In *Proceedings of the 5th international conference on the internet of things* (pp. 155–162), China.

78. Cui, A., & Stolfo, S. J. (2010). A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. In *Proceedings of the conference on computer security applications* (pp. 97–106), Florida.
79. Andrea, L., Chrysostomou, C., & Hadjichristofi, G. C. (2017). Internet of things: Security vulnerabilities and challenges. In *IEEE international workshop on smart city and ubiquitous computing applications* (pp. 180–187), Larnaca, Cyprus.
80. Iqbal, M. A., Olaleye, O. G., & Bayoumi, M. A. (2016). A review on internet of things (IoT): Security and privacy requirements and the solution approaches. *Journal of Computer Science and Technology: E Network, Web and Security*, *16*(7), 1–11.
81. Dinu, D., Corre, Y. L., Khovratovich, D., Perrin, L., Groschłdl, J., & Biryukov, A. Triathlon of lightweight block ciphers for the internet of things. (Cryptology ePrint Archive, Report 2015/209). http://eprint.iacr.org/.
82. Sankaran, S. (2016). Lightweight security framework for IoTs using identity based cryptography. In *Proceedings of the international conference on advances in computing, communications and informatics (ICACCI)* (pp. 880–886), Jaipur.
83. Ammar, M., Russello, G., & Crispo, B. (2018). Internet of things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8–27.
84. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet of things. *Journal of IEEE Internet of Things*, *4*(5), 1250–1258.
85. Sathish Kumar, J., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *Journal of Computer Applications*, *90*(11), 20–26.
86. Newlin Rajkumar, M., Chatrapathi, C., & Venkatesa Kumar, V. (2014). Internet of things: A vision, technical issues, applications and security. *Journal of Computer Science*, *2*(8), 20–27.
87. Joshitta, S. M., & Arockiam, L. (2016). Authentication in IoT environment: A survey. *Journal of Advanced Research in Computer Science and Software Engineering*, *6*(10), 140–145.
88. Ye, N., Zhu, Y., Wang, R. C. B., Malekian, R., & Lin, Q. M. (2014). An efficient authentication and access control scheme for perception layer of internet of things. *Journal of Information Science*, *8*(4), 1617–1624.
89. Jang, S., Lim, D., Kang, J., & Joe, I. (2016). An efficient device authentication protocol without certification authority for internet of things. *Journal of Wireless Communication*, *91*(4), 1681–1695.
90. Sharaf-Dabbagh, Y., & Saad, W. (2016). Authentication of devices in the internet of things. In *Proceedings of the IEEE 17th international symposium on a world of wireless, mobile and multimedia networks* (Vol. 32, No. 6), Portugal.
91. Gupta, U. (2015). Application of multi factor authentication in internet of things domain. *Journal of Computer Applications*, *123*(1), 21–23.
92. Sengul, C. (2017). Privacy, consent and authorization in IoT. In *Proceedings of the 20th international conference on innovations in clouds, internet and networks* (pp. 319–321), Chicago.
93. Hummen, R., Shafagh, H., Razaz, S., Voigtzx, T., & Wehrle, K. (2014). Delegation-based authentication and authorization for the IP-based internet of things. In *Proceedings of the 11th international conference on sensing, communication, and networking* (pp. 284–292), Singapore.
94. Henze, M., Wolters, B., Matzutt, R., Zimmermann, T., & Wehrle, K. (2017). Distributed configuration, authorization and management in the cloud-based internet of things. In *Proceedings of The IEEE international conference on trust, security and privacy in computing and communications (IEEE TrustCom–17)* (pp. 185–192), Australia.
95. Hern, J. L., Ramos, A., Pawlowskixy, M. P., Jaray, A. J., Skarmeta, A. F., & Ladid, L. (2015). Towards a lightweight authentication and authorization framework for smart objects. *Journal of Selected Areas in Communications*, *33*(4), 690–702.
96. Muhammad, F., Anjum, W., & Mazhar, K. S. (2015). Critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications*, *111*(7), 1–6.
97. Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *15th IEEE world congress* (pp. 1–8), Chicago.
98. Shahid, R. Lightweight Security solutions for the internet of things. www.diva-portal.org/smash/get/diva2:619066/FULLTEXT02.
99. Chikouche, N., Cayrel, P. L., & Boidje, B. O. (2019). A privacy preserving code based authentication protocol for internet of things. *Journal of Supercomputing*, *75*, 8231–8261.
100. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Journal of Ad Hoc Networks*, *10*(7), 1497–1516.
101. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2017). SIT: A lightweight encryption algorithm for secure internet of things. *Journal of Advanced Computer Science and Applications*, *8*(1), 12–20.

102. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Journal of Computer and Telecommunications Networking*, *54*(15), 2787–2805.
103. Atzori, L., Iera, A., & Morabito, G. (2017). Preserving data integrity in IoT networks under opportunistic data manipulation. In *Proceedings of the international conference on big data intelligence and computing and cyber science and technology congress* (pp. 446–453), USA.
104. Zhang, G., Kou, L., Zhang, L., Liu, C., Da, Q., & Sun, J. (2017). A new digital watermarking method for data integrity protection in the perception layer of IoT. *Journal of Security and Communication Networks*, *2017*, 1–12.
105. Fongen, A. (2012). Identity management and integrity protection in the internet of things. In *Proceedings of The 3rd international conference on emerging security technologies* (Vol. 4, pp. 111–114), Portugal.
106. Li, C., Liu, Q., & Wang, G. (2014). Survey of integrity detection methods in internet of things. In *Proceedings of The 13th IEEE international conference on trust, security and privacy in computing and communications* (pp. 906–913), Finland.
107. Internet of Things: IoT Governance European Research Cluster on the Internet of Things, 2014.
108. Networking protocols and standards for internet of things. *Internet of Things and Data Analytics Handbook*, 2017.
109. Pokorni, S. (2018). Reliability and availability of the internet of things. *Military Technical Courier* (pp. 588–600).
110. Kolisnyk, M., Kharchenko, V., Piskachova, I., & Bardis, N. (2017). A Markov model of IoT system availability considering DDos attacks and energy modes of server and router. In *Proceedings of the international conference on ICT education, research and industrial applications* (pp. 1–14), Ukren.
111. Mendez, D., Papapanagiotou, I., & Yang, B. (2017). Internet of things: Survey on security and privacy IoT security. *Journal of IEEE Internet of Things*, *4*(5), 1250–1258.
112. Vignesh, R., & Samydura, A. (2017). Security on internet of things (IoT) with challenges and countermeasures. *Journal of Engineering Development and Research*, *5*(1), 417–423.
113. Usman, M., Ahmed, I., Aslam, M. I., Khan, S., & Shah, U. A. (2018). Preserving privacy in internet of things: A survey. *Journal of Information Technology*, *10*, 189–200.
114. Miloslavskaya, N., & Tolstoy, A. (2019). Internet of things: Information security challenges and solutions. *Journal of Cluster Computing*, *22*, 103–119.

Poornima M. Chanal received her B.E. degree in Electronics and Communication Engineering, M.Tech. degree in Digital Electronics and Communication from the Visvesvaraya Technological University, Belgaum, Karnataka, India. Presently she is pursuing her Ph.D. degree in Internet of Things. Her research interests are: Software Agent based Network Management, Wireless Networks, and Internet of Things. She has published 10 papers in national and international conferences. She is a member of ISTE.

Mahabaleshwar S. Kakkasageri received his B.E. Degree from Karnataka University, M.Tech. degree in Digital Communication and Ph.D. degree from the Visvesvaraya Technological University, Belgaum, Karnataka, India. He has experience of 15 years in teaching. His research interests are: Vehicular Ad hoc Networks, Software Agent based Network Management, Wireless Networks, and Internet of Things. He has published 50 papers in national and international conferences, 17 papers in national and international journals, and 03 publications/books/books chapters. He is a member of IETE. He is a reviewer and programme committee member for many journals (published by IEEE, Springer, Elsevier, etc.) and international conferences, respectively. He received "Seed Money to Young Scientist for Research" from VGST Karnataka in 2015.