Wireless Networks
https://doi.org/10.1007/s11276-020-02445-6

Unification of Blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions

Bharat Bhushan[1] · Chinmayee Sahoo[1] · Preeti Sinha[1] · Aditya Khamparia[2]

Abstract
The Internet of Things (IoTs) enables coupling of digital and physical objects using worthy communication technologies and introduces a future vision where computing systems, users and objects cooperate for convenience and economic benefits. Such a vision requires seamless security, data privacy, authentication and robustness against attacks. These attributes can be introduced by blockchain, a distributed ledger that maintains an immutable log of network transactions. In this paper, we present a comprehensive review on how to remodel blockchain to the specific IoT needs in order to develop Blockchain based IoT (BIoT) applications and aim to shape a coherent picture of the current state-of-the-art efforts in this direction. After describing the basic characteristics and requirements of IoT, evolution of blockchain is presented. In this regard, we start with the fundamental working principles of blockchain and how such systems achieve auditability, security and decentralization. Further, we describe the most relevant BIoT applications, its architecture design and security aspects. From there, we build our narrative on the centralized IoT challenges followed by recent advances towards solving them. Finally, some future directions are enumerated with the aim to guide future BIoT researchers on challenges that needs to be considered ahead of deploying the next generation of BIoT applications.

Keywords Internet of Things (IoT) · Blockchain · Security · Bitcoin · Consensus · Decentralized · Ledger

1 Introduction

A drastic increase in Internet of Things (IoT) devices in the market was reported in the past decade. Roughly the number of IoT devices introduced in market is approaching 25 billion and it is expected that this number may increase to 50 billion by the end of 2025. These devices have sensors to establish network connection and to enable collected information transmission to a remote node [1, 2]. With the emergence of numerous technologies including embedded computing, sensors, actuators, cloud computing and wireless devices, many things in our routine life is becoming wirelessly interoperable with low-powered wireless devices like Radio Frequency Identification (RFID) tags [3, 4]. By enabling easy interaction with a wide range of things (or physical devices) such as monitoring sensors, home appliances, surveillance cameras, actuators, vehicles and so on, the IoT helps in development of many different applications like industrial automation, home automation, medical aids, intelligent energy management, mobile healthcare and smart grids [5]. Enormous amount of data generated by objects are used by these applications to provide new services and serve citizens, public administration and companies [6, 7]. Huge number of events generated by these objects along with heterogeneous technologies of IoT throws light on new challenges in application development making the ubiquitous computing even more difficult [8]. The centralized IoT network architecture faces following challenges.

✉ Bharat Bhushan
bharat_bhushan1989@yahoo.com

Chinmayee Sahoo
chinmayee.sahoo92@gmail.com

Preeti Sinha
preetigunja5@gmail.com

Aditya Khamparia
aditya.khamparia88@gmail.com

[1] Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Jharkhand 835215, India

[2] School of Computer Science and Engineering, Lovely Professional University, Punjab 144411, India

Published online: 06 August 2020

- In case of failure of the centralized server, there is a risk for the entire network infrastructure to get paralyzed and disrupted [9].
- *Edward Snowden leaks* makes it difficult for the adopters of IoT to trust partners who provide control and access allowing them to analyse the collected data [10, 11].
- Accountability and traceability are not guaranteed for the data stored in centralized clouds as they rely on third party trust for storing and holding data [12].
- Owing to the exponential growth of IoT, the central server is no longer efficient enough for handling large amount of data as well as end to end communications. Moreover, due to existence of innumerable smart devices, maintenance is a problem as distributing regular software updates to all these devices is almost near to impossible [13].
- Closed source code also widens the lack of trust. Transparency is essential in order to foster security and trust therefore open source approaches needs to be considered for the development of next generation IoT solutions [14].
- Proposed IoT solutions are expensive owing to its high cost of maintenance and deployment of server farms and a centralized cloud. This cost becomes a burden for the middleman if the supplier does not create such an infrastructure [15].

These challenges make it necessary to rethink about the structuring of IoT. Currently, the most appropriate candidate technologies that can support a distributed IoT ecosystem is "blockchain". Blockchain technologies can carry out, coordinate and track transactions. These also enable creation of applications that possess no centralized cloud requirement and are able to store huge amount of information generated by several devices. Some companies such as IBM, labelled blockchain as technology that democratizes the future of IoT. Blockchain is a decentralized data management technology that had gained much significance in past few years when a group or anonymous user introduced Bitcoin—a blockchain-based digital currency application [16, 17]. A peer-to-peer self-sovereign blockchain system helps to achieve decentralization by chronologically time-stamping the transactions in a ledger [18, 19]. In [20], blockchain is recognised as the fifth disruptive computer paradigm innovation after internet, mobile networks, personal computers and mainframe. Blockchain based IoT (BIoT) have received enormous research interests and researchers are making efforts to decentralize IoT communications using blockchain. This is so because this integration has following benefits.

- This paradigm shift towards BIoT from the traditional centralized IoT systems enhances the fault tolerance and also prevents the inherent problem of bottleneck in centralized IoT servers [21].
- The end to end peer communications in a decentralized architecture need not utilize a centralized server for carrying out automation services thereby enabling the IoT device autonomy [22].
- The information transparency allows faster information exchange and transaction processing as the intermediate layer between the parties are eliminated.
- IoT event and data logs stored on blockchain are immutable and thereby guarantees traceability and accountability.
- Blockchain can treat IoT interactions as separate transactions as it offers programming logic functionality via use of smart contracts that helps to perform access control and enhance security, confidentiality and authentication in BIoT [23].
- Owing to tamper proof and secure storage, blockchains enable secure deployment of software updates to IoT devices.

1.1 Previous work

The blockchain mitigates the risk of network attacks, fraud via time stamping entries and single point of failure due to its distributed and decentralized nature. Further, the use of cryptographically linked chains enhances the security level and speed of transaction by manyfold. Owing to the widespread adoption of blockchain technology, there have been a number of previously published surveys that had focussed on blockchain and IoT. These surveys are summarized as follows.

Christidis et al. [24] presented an extensive description of smart contracts and blockchain, and also presented a good overview on the deployment and applications of BIoT solutions. Even though the paper brings forth some useful information, it does not consider the possible optimizations that needs to be considered for creation of BIoT application. Zheng et al. [25] provided an extensive review on various mechanisms and the architecture of blockchain. However, it did not focus on applications of blockchain to IoT. Khan et al. [26] discussed how blockchain technology can be a key enabler to solve the most prominent IoT security issues. However, the work did not provide the detailed description of the working model of blockchain technology, phases of operations involved and the architectural design of an optimized blockchain for IoT applications. Reyna et al. [27] investigated the challenges in blockchain IoT integration analysing the unique features of blockchain technology and evaluating the performance of different blockchain in an IoT device. However, the work did not focus on the architecture, requirements and threats

to the IoT systems. Yeow et al. [28] presented a state-of-the-art review on decentralized consensus systems for edge centric IoT. Similarly, Panarello et al. [29] analysed various blockchain based approaches in IoT context and introduced two usage patterns namely data management and data manipulation. However, the work did not explore various IoT requirements and the most prominent attacks that can be launched in an IoT system. Wang et al. [30] surveyed existing blockchain based solutions for IoT applications and identified potential enhancements on blockchain consensus protocols to suit the IoT applications. The work presented a comprehensive survey on characteristics of IoT, preliminaries on blockchain, industrial blockchain-based IoT applications and benefits of applying blockchain to IoT. Wu et al. [31] classified blockchain technology into four layers and presented a comprehensive survey on the consensus strategies, the network and the applications of blockchain. In another work, Makhdoom et al. [32] highlighted the most severe threats that can be launched at various layers of IoT architecture. Mohanta et al. [33] extensively surveyed blockchain along with its associated security issues. Similarly, Casino et al. [34] comprehensively classified blockchain-enabled applications across various sectors namely IoT, data management, healthcare, business and supply chain. However, the work presented a superficial description about the integration of blockchain and IoT without highlighting various blockchain based solutions for enhancing IoT security. Hamad et al. [35] reviewed various security and privacy services capable of supporting the resource constrained IoT devices. Similarly, Butun et al. [36] presented a detailed review on various types of attacks that can launched in an IoT system and WSNs. Even though, the work can serve as a perfect guide for assessing the possible threats and their proposed countermeasures, it fails to shed enough light on the realm of blockchain for realising IoT security. Lao et al. [37] attempts to survey the architectures of various IoT-blockchain systems and the associated communication protocols.

A comparative study of the existing work by different authors has been summarized in Table 1 by considering the following 12 criterias. 1: Layered IoT architecture; 2: Middleware requirements in IoT; 3: Threats to the IoT; 4: Blockchain basics and evolution; 5: Classification of Blockchain; 6: Working of blockchain; 7: Phases of Blockchain Operations; 8: Optimized BIoT architecture; 9: Blockchain based IoT security; 10: Applications of BIoT; 11: Challenges related to BIoT applications 12: Future research directions for blockchains in the IoT.

1.2 Research contribution of the work

However, although blockchain has been prevailing for several years, there are very few comprehensive studies that sheds light on research and application of blockchain for IoT. In contrast to the works discussed in Sect. 1.1, this paper brings forth a holistic approach for application of blockchain for IoT scenarios and compares the available literature proposals that have focussed on integrating blockchain and IoT using 12 different attributes that are capable of providing an insight into the current research status. To the best of our knowledge, this survey is the first that thoroughly covers the architecture, requirements and threats to the IoT systems, background and working of blockchain, optimized BIoT architecture, Blockchain based IoT security solutions, and focuses on applications and challenges related to BIoT applications. The major contribution of this work is a detailed comprehensive discussion on the recent advances in IoT systems, blockchain technologies and decentralization of IoT systems using blockchain. Apart from exploring the basics of BIoT applications, this work also presents an extensive analysis on its optimization, deployment and development. A summary of contribution of this work is enumerated as below.

- Characteristics and requirements of an IoT ecosystem is discussed along with the analysis and categorization of various security threats with respect to the layered IoT architecture.
- Evolution, basic functioning, classification and working models of blockchain is presented in detail.
- Motivation for blockchain integration with IoT systems is discussed along with BIoT applications and the architecture design of an optimized BIoT applications.
- Recently proposed blockchain based solutions for ensuring privacy and security in IoT is reviewed.
- Current research challenges in decentralization of IoT using blockchain is presented in detail along with future research directions in the field.

1.3 Organization of the paper

The remainder of the paper is organised as follows. Section 2 presents the overview of IoT highlighting its characteristics, architecture, middleware requirements and various threats to the IoT systems. Section 3 describes the basics of blockchain, its evolution and classifications. This section also reviews the various blockchain platforms for IoT. Section 4 elaborates the working model of blockchain, various phases of operations involved and the architectural design of an optimized blockchain for IoT applications. Section 5 reviews the various Blockchain based IoT security solutions. Section 6 presents the various BIoT applications and identifies the current challenges related to these applications. Section 7 enumerates future research

Table 1 A comparative summary of existing related surveys

References	Year	1	2	3	4	5	6	7	8	9	10	11	12
Christidis et al. [24]	2016	✘	✘	✘	✔	✔	✔	∼	✔	∼	∼	✔	✘
Zheng et al. [25]	2017	✘	✘	✘	✔	✔	∼	✘	✘	✘	✘	✔	✔
Khan et al. [26]	2018	✔	∼	✔	✔	✘	✘	✘	∼	✔	∼	∼	✔
Reyna et al. [27]	2018	✘	✘	∼	✔	✔	∼	✘	∼	✔	✔	✘	∼
Yeow et al. [28]	2018	✘	✘	✘	✔	✔	∼	✘	✘	∼	✘	✔	∼
Panarello et al. [29]	2018	✘	✘	✘	✔	✔	✔	∼	✘	∼	✔	✔	∼
Wang et al. [30]	2019	✘	∼	✔	∼	✘	✔	✘	∼	✔	✔	∼	✔
Wu et al. [31]	2019	✘	✘	∼	✔	✔	✔	✔	✘	∼	✔	✔	∼
Makhdoom et al. [32]	2019	✔	✔	✔	✘	✘	✘	✘	✘	✔	∼	∼	✘
Mohanta et al. [33]	2019	✘	✘	✘	✔	✘	✔	✔	✘	✘	✔	∼	✘
Casino et al. [34]	2019	✘	✘	✘	✔	✔	✘	✘	✘	∼	✔	∼	✔
Hamad et al. [35]	2020	✔	∼	✔	✘	✘	✘	✘	✘	∼	✔	∼	✔
Butun et al. [36]	2020	✔	✔	✔	✔	✘	∼	✘	✘	∼	✔	∼	✘
Lao et al. [37]	2020	✔	✘	✘	✔	✔	∼	✘	✔	✔	✔	∼	✘

✔ indicates that the topic has been covered in detail

∼ indicates that the topic has been partially covered

✘ indicates that the topic has not been covered

directions with the aim to guide future BIoT researchers followed by Sect. 8 which is devoted to conclusions.

2 IoT overview

Research and study in the field of IoT is in nascent stage as there is not even a single appropriate definition for IoT available yet. Three perspectives can broadly define IoT: Internet-oriented, Semantics-oriented, and Things-oriented [38]. These views can be used jointly to achieve the goals of IoT. The first standard definition for IoT was based on "Things-oriented" perspective that considered RFID tags as things. The IoT allows things and people to be connected anyplace, anytime, with anyone and anything using any service and any network. IoT is receiving special attention by leading companies and also significant investments are made for attaining industrial solutions. Each of these companies use different terms to describe IoT. IBM uses "Smarter planet" and Cisco uses "Internet of Everything" as a replacement term for IoT. Table 2 presents the definition of IoT.

Table 2 Definition of IOT

Definition of IoT
Anything any context
Any service any business
Any place anywhere
Anything any device
Anyone anybody
Any path any network

IoT focuses on optimizing and transforming manual processes to make them part of the digital era, thereby facilitating the development of huge range of smart applications. Innovations in IoT has the potential to impact huge range of services and applications, such as industrial IoT, smart cities, smart agriculture, smart transport, smart homes, and retail IoT. The subsections below present a brief description on the generalized IoT architecture and its protocol stack, characteristics of IoT, requirements of IoT and the possible threats that can be launched at various layers of the IoT protocol stack.

2.1 IoT architecture

Owing to the lack of standardization and consistency in IoT solutions across the globe, there are several emerging issues related to manageability, compatibility and interoperability. Non-uniformity in the presentation of layered protocol stack and IoT architecture have been observed in the literature. Kumar et al. [39] presented IoT layers along with only a meagre detail of the associated protocols and their functionalities. Similarly, Granjal et al. [40] focussed on communication protocols at different layers of IoT. Whereas, Fuqaha et al. [41] presented a tabular representation of the various technologies and elements that collectively form an IoT. Owing to the existence of this non-standardization, it is believed that there exists no single universally accepted IoT reference model. In order to mitigate this uniformity, this section presents a generalized IoT architecture and layered IoT protocol stack in Figs. 1 and 2 respectively.

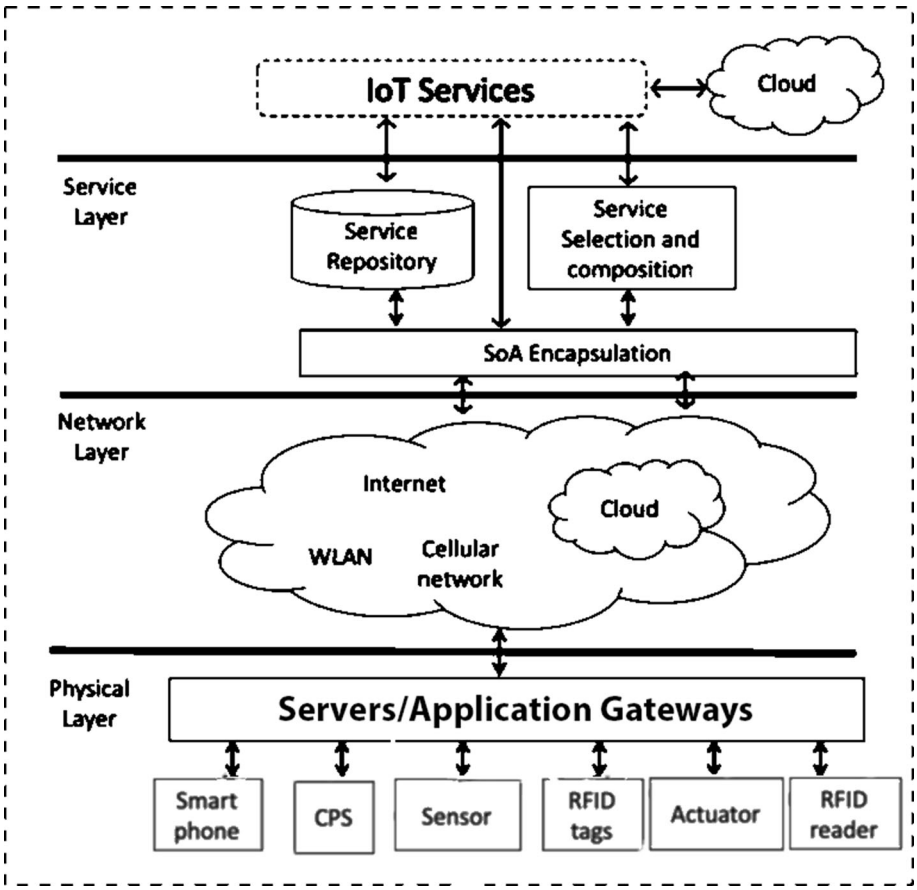

Fig. 1 Generalized IoT Architecture

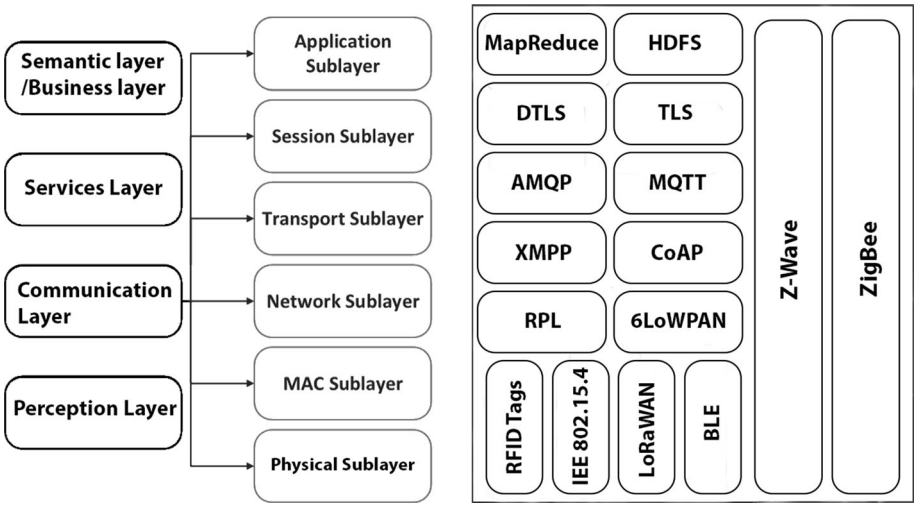

Fig. 2 IoT Protocol Stack

Numerous devices called "things" deployed in various topologies such as mesh, tree or clustered comprise an IoT ecosystem. "Things" are connected to gateways with the help of numerous IoT communication protocols such as RFID, BLE (Bluetooth Low Energy), WiFi, ZigBee, Sig-Fox, LoRaWAN and 802.15.4. Connection between these gateway devices and the network server is realized using satellite link, OFC (Optical, Fibre Cable), LTE (Long Term Evolution) and 3G/4G [42, 43]. These network servers facilitate data analytics services to the users and their associated third parties including private and government organizations. Useful information and services such as industrial automation, environment monitoring, business intelligence, smart home autonomous services, health statistics and smart city sharing services are obtained from these processed data [44]. As shown in Fig. 2, the IoT

protocol stack comprise of four different layers. These IoT layers are explored below.

2.1.1 Perception layer

The Perception/Physical layer is the first layer that comprise of computational hardware, actuators, sensors, identification and addressing of things. This layer is responsible for perceiving the environmental data, encryption-decryption, modulation-demodulation and frequency selection. Physical layer faces challenges related to interoperability, security and energy consumption. Some of the threats at the physical layer includes hardware failure, malicious data injection, node cloning, eavesdropping, timing attacks and hardware exploitation. the solutions proposed to prevent such threats includes the use of spread spectrum techniques such as direct sequence coding, frequency hopping, etc. [45, 46].

2.1.2 Communication layer

The second layer is Network/Adaptation/MAC (Medium Access Control) layer aimed to receive data from the sensors and relay them to the next layer for further analytics, processing and smart services. The major issues faced by the network layer is problems related to security, power consumption, network availability and scalability. MAC protocols play a vital role in prolonging the networks lifetime as it allows several nodes to access a common shared channel [47]. Recently, several works related to MAC protocols have been proposed. Bakshi et al. [48] proposed a multi user operation strategy based efficient MAC protocol aimed to support the short lived, high intensity demands of IoT network. Similarly, Cao et al. [49] presented a distributed, on-demand MAC protocol that permits connection among several backscatter devices (BDs) using ambient RF signal. Each BD is capable of switching itself among the receiving, transmitting and energy harvesting phases by making integrated use of dual-backoff mechanism and analog channel sensing strategy.

2.1.3 Services layer

The third layer is Services/Application layer aimed to feed the aggregated/processed data to the next layer and provide smart services to the users. The challenges faced at the application layer is related to the processing, storage as well as handling of data received from various sensors. Application layer performs data management, resource discovery and smart services provision to the customers. It is responsible for object tracking in supply chain, decision making in smart city and raw data processing in healthcare applications. Various protocols associated with this layer includes Advanced Message Queuing Protocol (AMQP), Constrained Application Prootocol (CoAP), light weight messaging protocol (MQTT), Extensible Message and Presence Protocol (XMPP), etc. [50, 51].

2.1.4 Semantic layer

The fourth layer is the Semantic layer/Business layer aimed to manage various activities of an IoT ecosystem. This layer employs cognitive technologies in order to provide numerous high-end services such as business modelling, business intelligence, data analysis, data fusion and decision making. Several works related to semantic layer have been proposed in the literature. Niu et al. [52] highlighted the need of distributed detection in WSNs and proposed a counting rule that uses the count of detections transmitted from the local sensors as a test statistic. Authors showed that the threshold at the local sensors is an important design parameter as it can significantly affect the overall system performance. Ciuonzo et al. [53] proposed a generalized locally optimum framework based fusion rules for distributed detection of a non-cooperative target.

Data fusion/data aggregation is the process of aggregating the sensory data in the form of a common representational format and send only the summarized and aggregated data [54]. The major objective of data fusion or decision fusion is to address problematic data (such as cooperative, complementary and redundant data), enhance data reliability and extract meaningful information from varied data sources [55, 56]. It is a key enabler for sustainable ubiquitous environments as it simplifies the decision-making process and contributes to the improvement of data quality [57]. In [58], authors proposed new fusion rules to address the issues of channel aware decision fusion in case the decision fusion centre have no prior knowledge of the sensor detection probability. In another work, Ciuonzo et al. [59] considered pilot-based channel estimation scheme for decision fusion. The work focussed on designing a low-complexity fusion rules that achieved enhanced spectral efficiency and extended battery lifetime. Zhu et al. [60] proposed a reliable and energy efficient direct transmission scheme aimed to achieve cooperative spectrum sharing in Industrial IoT. In another work, Zhang et al. [61] proposed evidence theory based collaborative weighted data fusion for distributed target classification in IoT scenarios. Mohammad et al. [62] proposed a mean-based blind hard decision fusion rules for resource constrained distributed networks. Instead of using the actual values, the proposed scheme considers the mean of the secondary user characteristics.

2.2 IoT characteristics

IoT is characterised by heterogeneous devices, resource constrained nature, spontaneous interaction, no infrastructure, context awareness and security attack surface. This section elaborates on aforementioned characteristics considering a general IoT system deployment.

2.2.1 Heterogeneous devices

The sensor computing and embedded nature of assorted IoT devices facilitates computing platforms that incurs low-cost. To minimize energy dissipation and IoT devices impact, low-power radios are used. WiFi or other cellular network technologies are not used by these low-power radios. IoT embrace high-order computational devices along with sensors and other embedded devices to execute tasks like switching, routing or data processing.

2.2.2 Resource constrained

Sensors and embedded computing require a device *form factor* that limits their communication, memory and processing capacity. Internet or cloud has higher memory and processing capacity followed by high-end computational devices. RFID aids machines to identify objects, control target and record metadata through radio waves. RFID tags enable the readers to automatically identify and monitor the objects in real time. Although RFID technology was discovered many years ago, it has evolved only during the last decade. In contrast to the earlier RFID tags that had limited processing capabilities, the newer RFID devices are semi-passive in nature and allows in-device processing operations [63, 64]. In another work, Yeh et al. [65] proposed an improvement of RFID scheme aiming to counter the security vulnerabilities such as replay attacks, eavesdropping and interception. Further, several energy saving technologies such as backscattering, energy harvesting and wireless power transfer have been proposed to power the resource constrained IoT devices [66–69]. Ambient backscatter supports battery free tags to use the wireless signals for both information transmission and energy harvesting. Zhao et al. [70] investigated the outage performance of an of an ambient backscatter system. Similarly, Ma et al. [71] proposed a distributed backscatter protocol for large scale IoT system. In another work, Nguyen et al. [72] proposed an energy harvesting aware routing protocol aimed to enhance the Quality of Service (QoS) and lifetime of the heterogeneous IoT networks. Khairy et al. [73] investigated the energy harvesting accomplishments of a Wi-Fi based IoT network that connects numerous IoT devices via Wi-Fi for both energy transfer and data communication. In order to maximize the network throughput and ensure prolonged energy sustainability, the charging period for different IoT devices are adaptively selected.

2.2.3 Spontaneous interaction

Sometimes in IoT applications, object move in and out of their communication range that causes unanticipated interaction leading to spontaneous event generation. For instance, whenever a smart phone user comes in contact with a TV/washing machine/fridge at home, it leads to event generation without user's involvement. Typically, in IoT, an event is generated upon interaction with an object and then is pushed into the system.

2.2.4 No infrastructure and dynamic network

IoT integrates many mobile, resource constrained and wirelessly connected devices. These mobile nodes can join or leave the network any moment. Battery shortage or poor wireless links may be a reason for the nodes to be disconnected. These factors make the IoT network highly dynamic. Maintaining a stable network for various IoT applications is difficult within such an environment which has limited connection to any fixed infrastructure. Thus, co-operation among the nodes is necessary to keep the network active and connected [74].

2.2.5 Context-aware and location-aware

Data is generated in prodigious amount by a huge number of sensors in the IoT. These data are useless until it is interpreted, analysed and understood. Context-awareness eases data interpretation and plays an important role in the autonomous and adaptive behaviour of various things in IoT. This eliminates human attention in IoT, making machine to machine communication easier. Spatial information about sensors, objects or things is critical in IoT. In context aware computing, location play an important role as interaction in large scale IoT depends heavily on their location and presence of varied entities or things.

2.2.6 Diverse real time applications

IoT purvey services to immense range of applications in many different domains and environments. These can be grouped as (1) logistics and transportation; (2) smart environment; (3) healthcare monitoring; (4) industrial; and (5) social and personal domain. Different deployment architectures are required for different applications having different requirements. There are two types of applications using IoT: first is real-time and second non-real-time.

Sometimes delayed data delivery can be useless for many services or applications. For instance, on-time data or service delivery is required in IoT for transportation or healthcare. In certain operation critical applications, delayed data delivery can even be more dangerous [75].

2.2.7 Security attack-surface

Apart from having huge range of applications and area of use, there are serious security concerns for applications and networks in different domains. IoT should be accessible to anyone, anywhere and anytime thus it requires global accessibility and connectivity. This increases the attack related to different IoT networks and applications. This complicates the deployment and design of coherent, scalable and interoperable security mechanisms.

2.3 Middleware requirements in IoT

Generally, a middleware obscures the hardware or system complexities, preventing application developers from being distracted by other hardware or software level orthogonal concerns so that they can focus directly on the main task [76, 77]. A middleware is a software layer that lies between the application, network communication layer and the operating system. It coordinates and facilitates the aspect of cooperative processing. Keeping computing perspective in mind, middleware is a layer between the system software and application software. In this section we present various types of requirements in IoT. These IoT requirements can be broadly categorised into two: Middleware service requirements and Middleware architectural requirements. These requirements are elaborated in the subsections below.

2.3.1 Middleware service requirements

The middleware service requirements in IoT can be broadly categorized as functional and non-functional IoT middleware requirements. Various functional IoT middleware requirements includes resource management, resource discovery, data management, code management and event management. Various non-functional IoT middleware requirements includes scalability, availability, security, reliability and ease of deployment. These functional and non-functional IoT middleware requirements are explored in the subsections below.

- *Resource management* This is an important requirement to deliver a desired level of Quality of Service (QoS). The resource usage needs to be monitored in a fair manner and conflicts related to resources needs to be resolved. In IoT architecture, the middleware is responsible for such resource management and for fulfilling the application needs.
- *Resource discovery* Resources of IoT comprises of heterogeneous hardware devices like sensors, sensor mote, RFID tags, and smart phones. Along with this, it also includes power devices, memory, the communication modules, and network level information. IoT's environment and infrastructure is dynamic resulting in an invalid, deterministic and global knowledge of these resources. Resource discovery mechanism should be well scaled and should incorporate efficient load distribution [78].
- *Data management* In IoT, any kind of sensed data or any information regarding the network infrastructure is referred to as data. An IoT middleware is responsible to provide the desired data management services including data acquisition, processing and storage. Data processing refers to data filtering, data aggregation and data compression.
- *Event management* Because of huge number of events being generated in IoT applications, event management is the core function of the IoT middleware. Simple observed events are transformed to meaningful events by the event management.
- *Scalability* To accommodate the growth of IoT's network, an IoT middleware must be scalable. IPv6 deals with stupendous number of things in IoT. As IoT's network is huge in size, IPv6 contribute a scalable solution for addressability. Virtualization or loose coupling can enhance the scalability by hiding the hardware complexity and implementation [79].
- *Availability* A middleware that supports a mission critical IoT application needs to be active always. In case of any system failure, the recovery time along with the failure frequency should be negligible to achieve the desired level of availability. To ensure better fault tolerance, the availability and reliability should work together.
- *Security and privacy* For every IoT operation, security is critical and it needs to be examined for all functional as well as non-functional blocks. Personal information may be disclosed by context-awareness in middleware. Owners privacy needs to be preserved as every middleware block uses personal information.
- *Reliability* A middleware should be operative for the entire lifetime even under failures. The middleware reliability helps in obtaining system level reliability. The overall reliability is achieved when every component of the IoT middleware is reliable. These components include data, communication devices and technologies from all the layers.
- *Ease of deployment* IoT middleware deployment should not desire expert support or knowledge since it is

deployed by the user. Complex installation and setup actions must be avoided.

2.3.2 Middleware architectural requirements

Various middleware architectural IoT requirements includes programming abstraction, interoperable, context-aware, adaptive, service-based and distributed. These requirements are explored in the subsections below.

- *Programming abstraction* For service or application developer, high level programming interface isolates the application development and their operations. While defining an Application Programming Interface (API) we need to consider the abstraction level, the interface type, and the programming paradigm. The abstraction level deals with the developer's view of the system. The interface type deals with the programming interface style and the programming paradigm defines the model for programming the services or applications [80].
- *Interoperable* A middleware must be capable of working with heterogenous applications or devices without involving any additional effort from the service or application developer. These heterogeneous devices must be capable of exchanging services and data. Interoperability in middleware is of utmost importance with syntactic or network or semantic perspectives. Syntactic interoperability must allow heterogeneous formatting of the exchanged service or information. Semantic interoperability must allow interchange between rapidly changing set of services and devices in IoT [81, 82].
- *Adaptive* Middleware to fit itself into environmental changes needs to be adaptive. Network and its environment changes in an IoT vary frequently. Also, the application level demands the change frequently. Thus, for ensuring user satisfaction, the middleware needs to adjust or adapt dynamically to fit in all such deviations or variations.
- *Service-based* IoTs middleware must be service-based for offering higher degree of flexibility every time a new function is to be aggregated with the IoT middleware. Such service-based middleware is responsible for providing abstraction of complex hardware needed by the applications. Other advanced services like data management, security and reliability can be designed, integrated and implemented in a service-based framework to guarantee flexibility for application development.
- *Distributed* In a large scale IoT, devices or users are geographically distributed thus a middleware implementation or a centralized view may not be sufficient for supporting many distributed applications or services. Thus, the middleware implementation must support distributed functions across the physical IoT's infrastructure [83].

2.4 IoT versus traditional networks

Prior to the discussion on IoT threats, the difference between the traditional networks and IoT needs to be outlined as these directly or indirectly relates to the development of requisite privacy and security solutions for IoT systems.

Resourcefulness level of the end devices is the primary difference between the IoT and the conventional networks [84]. IoT systems comprise of embedded devices such as sensor nodes (SNs) and RFID that are resource constraint in terms of disk space, computing power and memory [85]. In contrast, the traditional internet is composed of smartphones, servers and computers powered by plentiful resources. This enables the traditional networks to reap the support of multi-factor and complex security protocols without any specific resource considerations. Whereas, lightweight security algorithms are required by the IoT systems in order to maintain a proper balance between resource consumption issues such as battery life and security [86].

IoT devices and the internet or gateway devices are connected mostly via less secure and slower wireless communication media such as SigFox, NB-IoT, ZigBee, LoRa, 802.11a/b/g/n/p and 802.15.4. These result in IoT systems being prone to various privacy and data leakage issues. Whereas, the end devices in traditional internet communicate via relatively faster and secure wireless/wired media such as LTE, 4G, WiFi, DSL/ADSL and fibre optics. Moreover, the traditional network devices use the same data format as well as operating system whereas IoT use varying data contents and formats owing to the lack of OS and its application-specific functionality.

Owing to this huge diversity, development of a single standard security protocol capable of incorporating the requirements of every IoT systems and devices is a challenging task. As a result, there exists huge range of IoT threats capable of compromising the privacy and security of the users. Security design for traditional networks use an effective blend of host-based security approaches such as software patches and anti-viruses, and the static network perimeter defence schemes such as IDS (Intrusion Detection Systems) and firewalls. However, these host-based security schemes are not feasible for such resource constrained IoT devices. Moreover, the conventional perimeter defence schemes are incapable of protecting IoT devices from physical compromise and insider attacks due to the inherent IoT vulnerabilities such as lack of IoT-specific

attack signatures, cross-device dependencies, lack of access control schemes, mitigated security patches and absence of physical security schemes [87].

2.5 Threats to the IoT

The potential vulnerabilities associated with the IoT systems increase with drastic increase in number of things or devices connected together. This leads to various security incidents in the IoT systems. Smart devices in an IoT ecosystem aims to gather personal user information in some form or the other which might be vulnerable to data integrity, privacy and security attacks [88–90]. Furthermore, the lack of network access control schemes and data encryption measures enables the adversaries to launch real threat to networks user privacy through traffic analysis and eavesdropping [91]. The deployment of IoT and its affluent operation in several critical scenarios such as smart homes, smart vehicles, intelligent traffic systems, healthcare and smart grids is dependent on the reliability of the data being transmitted between these IoT devices. In the absence of any physical security standards in a trust less environment, these IoT devices are subject to numerous physical attacks including reverse engineering attacks, side channel attacks and invasive hardware attacks [92]. The most severe threats launched at various layers of IoT architecture is discussed in the following subsections.

2.5.1 Threats at the perception layer

- *Eavesdropping attack* The most commonly launched attack at the perception layer is the eavesdropping attack in which the adversary sniffs the wireless traffic in order to gain insight of the valuable user information by utilizing similar devices as the end nodes [93, 94].
- *Hardware failure* The launch of a cyber-attack or even some manufacturing fault may lead to substantial damage or physical impairments thereby causing the hardware failure. In some devices such as iBaby M6, guessing the user ID, camera type and the serial number of the device is possible which can be exploited to launch an authentication bypass in order to gain legitimate access to the device [95].
- *Data injection* Adversary can render the system unavailable to genuine users by compromising a device or even introducing a forged device in order to inject fabricated messages, eavesdrop on the radio traffic or flood the radio channels with numerous fake messages [96].
- *Sybil attack* An adversary may take up numerous identities by generating new fake identities or impersonating other legitimate nodes. The most severely launched sybil attack involves numerous identities that is generated using only a single device. Adversaries may present these identities either one by one or simultaneously at a single instance. This type of attacks can bring about a significant impact on the outcome of a voting-based system. Mishra et al. [97] classified the sybil attack into three different phases namely launching phase, deployment phase and compromise phase by considering the nature of task being performed during the attack operation.
- *Side-channel attacks* In this attack, the adversary exploits the side channel information about the encryption device and gains partial access to the secret values. Wu et al. [98] proposed a leakage resistant certificate-based signature scheme with unbounded leakage property. This scheme permits the adversaries with only the partial information about private keys thereby preventing the successful launch of side channel attack. In another work, Tseng et al. [99] proposed an ID-based authentication and key exchange (ID-AKE) protocol capable of securing the mobile devices against the ephemeral secret leakage attacks. The proposed scheme enhances the security without compromising the computational performance. Similarly, Tseng et al. [100] proposed a leakage resilient certificate-based cryptography scheme resilent against side channel attacks.
- *Device compromise* Wurm et al. [101] presented a practical manifestation of device compromise attack in a home automation system by compromising a smart controller via open Universal Asynchronous Receiver/Transmitter (UART) interface. After gaining access to the device, it was possible to modify the boot parameters as well as view the start-up sequence. Moreover, the adversary could launch several network layer attacks including the network traffic analysis and port scanning. Arias et al. [102] successfully executed a similar attack on Nike + Fuelband SE fitness tracker and Google Nest Learning Thermostat. They exploited weaknesses in the physical design and boot process vulnerabilities in the Nest Thermostat OS.
- *Node cloning* IoT devices such as CCTV cameras and Sensor Nodes (SNs) are deployed in absence of any tamper-proof hardware owing to the declined standardization of IoT device design. This enables these devices to be replicated or forged easily in order to launch malicious activities during both operational as well as manufacturing phase. A node can be captured and cloned in order to extract the security parameters and launch firmware replacement attacks during the operational phase. Whereas, during the manufacturing phase, an internal adversary launches malicious activities by substituting the original device by some pre-programmed thing [103, 104].

2.5.2 Threats at the adaptation layer

Security at the Adaptation/MAC/Network layer is affected by numerous threats such as sybil attacks [97], impersonation [105], interrogation and unfairness. Some of the DoS attacks launched at this layer include battery exhaustion attack, channel congestion attack [106] and collision attack [107]. Most of the attacks are launched at the network layer as it provides an interface to internet and connects multiple private LANs. These attacks include node replication [108], unauthorized network access, message fabrication attack, eavesdropping attack, insertion of rogue devices and Man In The Middle (MITM) attack [109]. Similarly, network services availability threats include blackhole attack, wormhole attack [110], sybil attack and selective forwarding attack.

2.5.3 Threats at the application layer

Application developers focus majorly on service delivery and efficiency rather than security aspect. This results in easy compromise of applications thereby leading to denied services. The most commonly launched threat at the application layers include the following.

- *Malicious code* The malicious codes that is spread over the targeted malware or internet may exploit the unique vulnerabilities of the IoT devices such as lack of application security and weaknesses in authorization mechanism in order to compromise these devices. These devices can be utilized in the form of "bots" to enable various attacks on other network/end devices applications.
- *Weak application security* Any kind of possible weakness in the authorization and authentication mechanism may facilitate unwanted disclosure of information, brute force attack, dictionary attack, data tampering and elevation of privileges. Open Web Application Security Project (OWASP) ranks the most sever application security risks that pose valid threat to IoT systems that relies on applications and websites to provide the desired user services [111]. Incorrect implementation of authentication, insecure web applications leading to exposure of sensitive data, security misconfiguration and XSS (Cross Site Scripting) are some of these application risks.
- *SQL injection attacks* IoT application and database servers face a major risk due to injection flaws that threaten LDAP (Lightweight Directory Access Protocol) and SQL/noSQL database. In Belkin's smart home products, security researchers successfully exploited an SQL injection vulnerability that allows them to gain root control of the connected device by malicious code injection into the paired Android WeMo smartphone app [111, 112].
- *Data exposure attacks* Insecure APIs and web applications leads to exposure of sensitive data thereby posing a threat to the confidentiality of collected user data from devices such as smart watches, wearable health monitors and smartphones. Philips Hue Smart Bulb is a classic example of such vulnerability where the users are able to wirelessly control the lighting system via mobile app [111]. Any eavesdropper or MITM attacker can sniff the ongoing communication between the smart bulb and the user. Furthermore, adversary can also masquerade as a legitimate user after gaining access to the authorized user's list from the bridge.
- *XSS (cross site scripting)* It is one of the most prominent attacks in both IoT and web-based applications. This XSS vulnerability was successfully exploited by the security researchers in Belkin's smart home products [112]. Utilizing these vulnerabilities, adversary can run an arbitrary JavaScript code in the victim' browser thereby causing theft of private data and hacking into the phone.

2.5.4 Threats at the semantics layer

The transformation of web into machine processable form from human readable form is powered by the creation of semantic web. The machine processing has augmented decision making, interpreting and human reasoning abilities on the basis of automated big data analytics. However, this extraction of application specific information or intelligence from Big Data brings forth numerous privacy issues [113, 114]. For an instance, unauthorized disclosure of sensitive health related data or personal information stored on social media may result in compromised user privacy. Table 3 presents various threats to the IoT along with the vulnerabilities exploited by the adversary in the launch of these attacks.

3 Blockchain basics, evolution and classification

3.1 Integration of blockchain and IoT

Brody et al. [115] proposed the ever-expanding IoT device ecosystem to shift towards a decentralized architecture in order to maintain its sustainability. From the consumer's perspective, there is lack of trust as well as need for "security through transparency" approach. Whereas, from the manufacturer's side, there is huge maintenance cost associated with the current centralized model. These issues can

Table 3 Threats to the IoT

SI. no.	Threats to the IoT	Vulnerabilities exploited
Threats at the perception layer		
1.	Eavesdropping [93, 94]	No encryption
		Unprotected communication channel
2.	Hardware Failure [95]	Unprotected interfaces (e.g., JTAG, UART)
		Developers fault (both software and hardware)
		Weak application/network/web security
3.	Data injection [96]	Weak access control
4.	Sybil attack [97]	Lack of identity management
5.	Side channel attack [98–100]	Lack of physical device protection
6.	Device compromise attack [101, 102]	Boot process vulnerabilities
		Vulnerable physical interfaces
7.	Node Cloning [103, 104]	Lack of tamper-proofing
		Lack of hardware security standardization
Threats at the adaptation layer		
8.	Impersonation attack [105]	Weak network access control
		Communication protocol weaknesses
		MAC Spoofing
9.	Channel congestion attack and collision attack [106, 107]	Flaws in communication protocols and medium access control
10.	Node replication attack [108]	Weak access control mechanism
11.	Eavesdropping and MITM attack [109]	Weak data security and authentication
12.	Blackhole attack, Selective forwarding attack and Wormhole attack [110]	Weaknesses in network routing protocols
Threats at the application layer		
13.	Malicious codes	Lack of authorization and authentication mechanism
		Lack of web/application security
14.	Data tempering and Brute force attacks	Lack of authorization and authentication mechanism
15.	SQL Injection attacks [111]	Injection flaws in LDAP and SQL/noSQL databases
16.	Data exposure attack [111]	Insecure APIs and web applications
17.	Cross-Site Scripting [112]	Lack of user awareness
		Web applications vulnerabilities
Threats at the semantics layer		
18.	User privacy compromise and identity theft [113, 114]	Lack of application/data security

be effectively countered by blockchain which itself is a trust less, scalable peer-to-peer network model capable of distributing data securely and operating transparently.

In order to understand the complete working of this, consider a setup where all IoT devices operate on a single blockchain network. The smart contract deployed by the manufacturer facilitates to store the hash of the latest network firmware update [116]. The devices use the smart contract's address or other discovery service to query the contract, receive new firmware updates and request them with its hash. The manufacturer's own node serves the initial file requests but can stop serving once this binary propagates to some good number of nodes. The configured devices are assumed to share their received binary thereby enabling the retrieval of the firmware updates by even those devices that joins the network after the manufacturer has stopped participating. These do not require any user interaction and happens automatically. Furthermore, a cryptocurrency exchanging blockchain network paves a way for easy exchange of service between devices and also provides a convenient billing layer. In order to make some profit or sustain their infrastructure costs, these devices storing the binary copy may charge for serving it. Other examples include EtherAPIs [117] that helps to monetize

API calls and Filecoin [118] that facilitates devices to lend their disk space on rent. With a cryptocurrency such as Ethereum or Bitcoin in place, every device receives proper compensation with the help of microtransactions for their usage. This is possible because every device can possess its own personal bank account and expose its resources to other devices [119].

Integration of IoT and blockchain also facilitates the sharing of property and services. Slock.it [120] introduces the concept of *"Slocks"* or smart electronic locks that can only be unlocked by the device that carries the appropriate token. On the same theme, the integration of IoT and blockchain in the energy sector facilitates peer-to-peer market place where machines are capable of buying and selling energy automatically on the basis of some user-defined criteria. For an instance, TransActive Grid [121] brings forth the concept of peer-to-peer market for renewable energy supply in New York. The deployed solar panels record the excess output on a blockchain and sells them in the neighbourhood via smart contracts [122].

The usefulness of blockchain and IoT integration can be seen in a typical supply chain example in which a container that is released from the manufacturing site (site A), gets consigned to the neighbouring port (site B) via railway, the gets shipped to the destination port (site C), is dispatched again to the distributors address (site D) and finally is received at the retailers site (site E). Therefore, the discussed process involves numerous checks and stakeholders along the way. In order to keep track of the asset, every stakeholder maintains their own database that they update on the basis of inputs received from other parties lying along the chain. A blockchain network introduced to track this asset is a shared database that comprise of cryptographically verified updates that is automatically propagated in order to create an auditable trial of information. Upon reaching the destination port, the shipping carrier sends a signed message to an agreed-upon, predefined smart contract such that everyone on the chain is aware of the current location of the container. The signed transaction acts as cryptographically verifiable receipt for the successful reception of the container at the destination port. The receiver also posts to the same smart contract in order to confirm its own possession with the container [123, 124].

3.2 The beauty of blockchain

Numerous transformations have been reported in information and communication technology over the past few years that facilitates efficient, quicker, easier and secured data exchange. Digital communications emerged with an advent of internet and it empowers data exchange through financial online transactions for receiving funds and making payments. The entire communication and transactional system pass through a trusted intermediate that guarantees secure delivery of financial transactions. This trusted party is liable for any fraud, delayed data delivery and failures in data updating. Due to existence of one network controller, several questions pop up.

- What will happen if the trusted party is hacked and all its data is seized by the adversary?
- What will happen if the trusted party can no longer remain trusted and become rogue?
- Why not communicate using peer-to-peer (P2P) instead of an intermediary that introduces additional communication delays?

Blockchain provides solution to all these problems by putting forth the premiere decentralized cryptocurrency named bitcoin [125, 126]. The transfer and exchange of bitcoin occurs using a shared distributed ledger that keeps track of all the transactions taking place within the network participants without any need of trusted centralized party. Bitcoin exploits the public key infrastructure of blockchain for controlling access and authenticating anonymous users. Owner digitally signs each transaction using a private key for source identification and authentication [127, 128]. Figure 3 depicts the basic blockchain characteristics.

In order to track the simultaneously occurring transactions, several transactions are stacked together in a structure termed as *block* that can be identified uniquely using its timestamp and hash. *Consensus mechanisms* are used to check the validity of the block and transactions among various distrusted users. Consensus mechanism refers to the updating of the shared ledger with the consensus or agreement of the majority of users. Considering the case of bitcoin, this updating mechanism needs to employ proof-of-work (PoW) scheme. In PoW consensus algorithm, nodes select a special value that must be smaller than the target value in order to establish trust and avoid any conflicts. The target value is set to estimate *nounce*, a one-time number which is generally 10 min. The scheme by which nodes devote their resources and perform rigorous computations to estimate the nounce is referred to as *mining* and the nodes taking part in this process are called *miners*. Blockchain uses public key cryptography to create and validate digital signatures. Every person in Blockchain has one or more addresses associated with a pair of private and public keys. One practical example of this concept is Bitcoin which is a decentralized (without any central party for recording or ordering), permission-less (no access control) and P2P cryptocurrency (work on machines of each and every stakeholders) [129].

Suppose P wants to send a Bitcoin to Q, for that Q sends his address to P. P adds Q's address and the fund of bitcoins to send in a 'transaction' message. P signs the transaction with his private key and his public key is

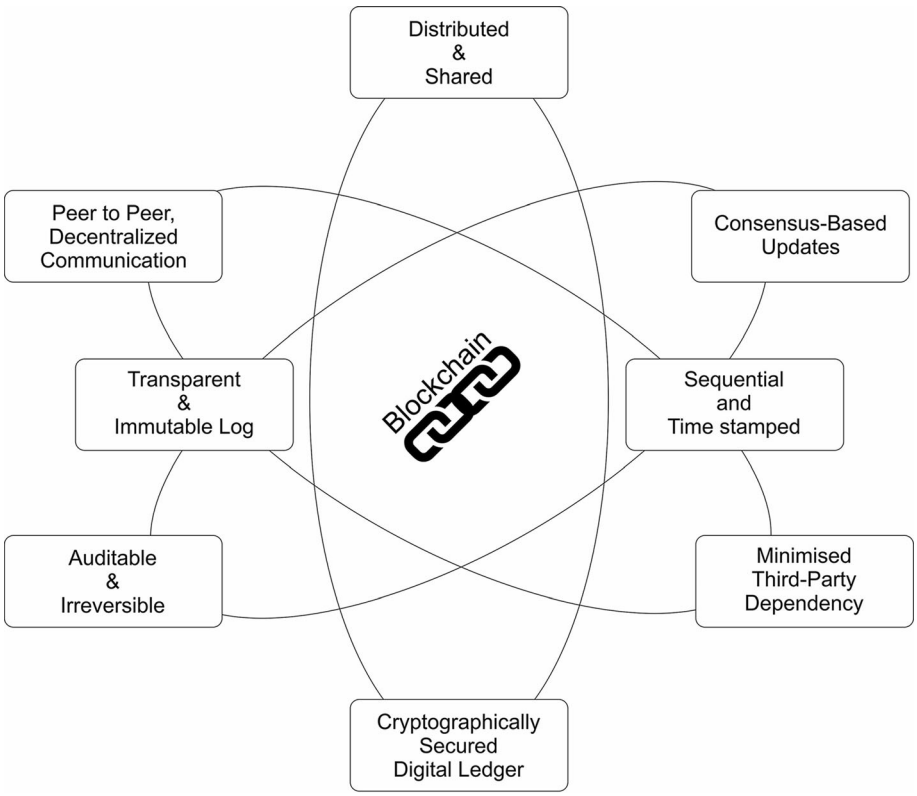

Fig. 3 Basic blockchain characteristics

known to everybody for signature verification. Only the user having private key can decrypt the encrypted message that is asymmetric cryptography [130, 131]. When a transaction is being carried out in a Blockchain, a node signs the transaction with his private key and that transaction is then broadcasted to its peers. The concept behind authenticating the transaction by signing it with the unique private key guarantees' integrity (as it can't be decrypted if there is any error during transmission) as well as authenticity (as it can only be signed by the user having specific private key). When the signed transaction is received, after being broadcasted by the peers, it is verified and validated before being retransmitted to other peers. This type of transactions which are verified and validated by the peers of the network are stored in a block (a container data structure to store a series of transactions) by special nodes called as miners. Those blocks which are packed by miners are broadcasted back into the complete network. All nodes then participate in verification process to verify whether the block consist of valid transactions or not. To create a tamper proof Blockchain, the hash of the preceding block is used to create the hash value of new blocks. A newly created block is discarded and not added in the existing blockchain if above mentioned condition is not satisfied. Otherwise it is added, if both the conditions are satisfied and verified successfully [132].

3.3 Blockchain evolution

Blockchain evolution can be categorized into three versions: Blockchain 1.0, 2.0 and 3.0. 1.0 version of the blockchain is related to bitcoin and cryptocurrencies. Bitcoin was the first cryptocurrency prototype invented to facilitate money transfer without any need of intermediates between parties. Bitcoin emergence enabled creation of more than 600 cryptocurrencies that serves as exchange tokens for various blockchain based applications [132]. *Ethereum*, an alternative to bitcoin is the most widely accepted cryptocurrency on the basis of market capitalization data. *Monero* and *ripple* are another cryptocurrency that guarantees the transactions un-traceability and enables instant payments respectively. *Blockchain 1.0* focuses on money aspect whereas *Blockchain 2.0* focuses on transferring, confirming and registering contracts or properties. Integration of Blockchain 2.0 and the *smart contracts* was initially permitted only by Ethereum but now it became the most significant characteristic of Blockchain 2.0. Smart contracts can be executed automatically without need of any external control as these are code pieces stored on the blockchain that executes after few specified conditions are met. For an instance, if a will of an individual is encoded using blockchain then in case of testator's death, assets are transferred automatically to the beneficiary by the smart contract. Smart contract applications can also be beneficial

for crowdfunding campaigns based on blockchain to trigger the payments automatically after achieving the goal. These can also serve as an effective tool to automize the betting system facilitating users to bet and also transfer the amount to the winners. Smart contracts can also be used in conjunction with IoT devices to unlock services after payment especially in case of intelligent hotel rooms. However, the application field is no longer limited to goods and finance transactions in *Blockchain 3.0* but it also embraces sectors like education, science, health, government and more [133, 134]. Considering the use of blockchain for government, it can enable the recording of election votes in a publicly verifiable and immutable manner thereby enhancing transparency [135].

3.4 Classification of blockchain

Depending on the data, it's availability and different action associated with those data, Blockchains are classified into three different types namely federated, private and public. In view of some authors private/permissioned and public/permission-less are considered as synonym of each other. But there is some difference in terms of authorization (permissioned vs. permission-less) and authentication (private vs. public). In *private blockchains*, access to the network is restricted by the owner. Coming to *public blockchains*, third party approval is not needed to join the blockchain. It can act as a node or a miner. A challenge-response based system is used to select the node to be added in blockchain where each node would attempt to solve the challenge. Then one question arises here that what will be the incentives for other nodes participating in that challenge. So, Economic incentives like Bitcoin, Litecoin or Ethereum are given to the miners for becoming a part of the challenge [136]. *Federated blockchain* or consortium blockchain is another type of permissioned blockchain similar to private blockchain. Consortium networks enforces transparency among various involved parties and can span multiple organizations. Consortium blockchain is used as reliably synchronised and auditable database that monitors the data exchange between the consortium members. Permission-less model is an open environment which is best suited for cryptocurrency which again is open control and free financial application whereas, permissioned model is a close environment truly suited for business applications such as Hyperledger Fabric [137], Smart Contract or Ripple [138]. We can also classify them into two categories, firstly as a blockchain where certain logic is used such as Smart Contracts and secondly as a blockchain where digital assets can be tracked such as Bitcoin. Also, there are some systems which uses tokens (Ripple) and some don't (Hyperledger). Here tokens can be referred as a proof, to justify occurrence of particular events at particular instance of time. Table 4 presents the comparative analysis of the three types of blockchains namely federated, private and public blockchains.

3.5 Blockchain platforms for IoT

In order to estimate the most suitable blockchain platform for IoT applications, comparison of the most widely accepted and prominent blockchain platforms including *IOTA* [139], *Hyperledger-Fabric* [140, 141], *Ethereum* [142, 143] and *Bitcoin* [144, 145] is presented in this subsection. A block less distributed ledger and successor of blockchain called IOTA is designed specifically for enabling micropayments in industrial IoT. IOTA addresses the issues of high transaction fees and scalability. Before initiating its own transaction, every node in IOTA validates any two previous transactions without the need for miners to mine a valid transaction block. IOTA do not possess consensus finality therefore are prone to latency causing forks in transaction confirmation. Hyperledger fabric and Ethereum have different architecture than blockchain as it is designed for M2M interactions and offers fee-less transactions. The scalability issues of blockchain can also be solved to some extent by using these platforms. IoT systems are designed for numerous applications ranging from industrial control systems to smart watches. Hyperledger fabric and Ethereum can be used in these systems owing to its applicability to multiple blockchain applications. Table 5 compares various blockchain platforms such as IOTA, Hyperledger Fabric, Ethereum and Bitcoin.

4 Working model of blockchain

The fundamental components of blockchain network along with their significance are explored in this section. Then, the various phases of blockchain functionality are discussed in which these elements collaboratively carry out secure communication among distrusted nodes. Next, stepwise overview of the network operation is presented. Major blockchain functioning is illustrated considering the example of bitcoin blockchain.

4.1 Core components

The core components of the blockchain system include asymmetric cryptography, transactions, secured distributed ledger and consensus mechanisms as depicted in Fig. 4.

Table 4 Comparison of federated, private and public blockchains

Supported features	Federated blockchain	Private blockchain	Public blockchain
Participation in consensus	Selected nodes among multiple organizations	Single organization	All nodes
Immutability	Partial	Partial	Yes
Permission less	No	No	Yes
Transaction processing speed	Faster	Faster	Slower
Access	Restricted	Restricted	Public read/write
Identity	Approved participants	Approved participants	Pseudo-anonymous

Table 5 Comparison of various platforms for IoT

Distinguishing characteristic features	IOTA [139]	Hyperledger-Fabric [140, 141]	Ethereum [142, 143]	Bitcoin [144, 145]
Participation of miners	Public	Private	Private, public and hybrid	Public
Trustless operation	Yes	Trusted validator nodes	Yes	Yes
Fee less	Yes	Optional	No	No
Run smart contracts	No	Yes	Yes	No
Attacks	Beta testing	1/3 faulty node attack	51% attack	Linking and 51% attack
Consensus	Tip selection algorithm	PBFT	PoS (Proof of Service) and PoW	PoW
Consensus finality	No	Yes	No	No
Data confidentiality	No	Yes	No	No
Authentication and integrity	Yes	Yes	Yes	Yes
Key management	No	Yes	No	No
ID management	No	Yes	No	No
User authentication	Digital signatures	Enrolment certificates	Digital signatures	Digital signatures
Transaction throughput	7–12 TPS	>3500 TPS	8–9 TPS	7 TPS
Transaction confirmation latency	60–3600 s	Least	15–20 s	600 s

4.1.1 Asymmetric key cryptography

Strength of public key cryptography are utilized by the blockchain network for their secure operation. Users possess a digital wallet for data exchange which is secured using user's private key. Private keys are kept secret from the user and functions to sign transactions digitally. The public key wallet functions as the address of the bitcoin known to all.

4.1.2 Transactions

Information exchange and sharing among nodes are enabled by blockchain on a P2P basis. Source generates a file and broadcasts it to the entire network that contains transfer information. These transactions that are generated and congregated in blocks continuously by the nodes represent the current blockchain state. Every transaction represents the currency transfer among nodes in the context of bitcoin. The current balance at all addresses is known to every node and they maintain existing blockchains copy that holds the history of preceding transactions. After every transaction, there is a change in the blockchain's state [146]. Owing to innumerable transactions beings generated every second, validating and verifying the legitimate ones and discarding the illegal transactions is of utmost importance.

4.1.3 Consensus mechanism

Nodes that utilise the blockchain platform for exchanging and sharing data do no possess a centralized authority to safeguard against security violations and resolve or regulate disputes. In order to ensure an unassailable exchange and keep track of the funds flow, there is a need of

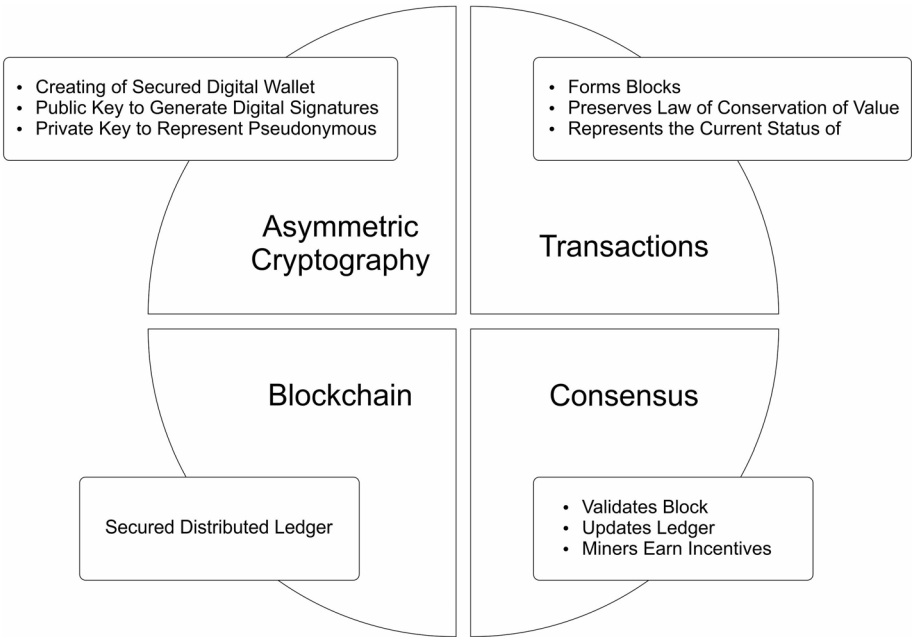

Fig. 4 Core components of a blockchain system

mechanism that can avoid frauds such as denial of *service attacks* and *double-spending problem* [147]. For maintaining a consistent state, each node must agree on a prevalent content-updating rules. Moreover, acceptance of blocks as part of blockchain is not allowed without getting the majority consent. This mechanism of creating the blocks and adding them to the existing ledger is known as *consensus mechanism*. After the process of signature verification, the recipients might regain outputs several times in case of bitcoin. The regained outputs might be used in subsequent transactions. Thus, Nakamoto [148] proposed a decentralized consensus-based cryptocurrency for avoiding the double spending problem. This consensus mechanism involves block mining in which there is a competition among miners to get the next valid block with the help of cryptographic hash. Reward is given in the form of bitcoin to the nodes that find the solution. This cryptographic hash is referred to as the *proof of work*.

4.2 Phases of operation

The phases involved in the entire block formation process of blockchain is detailed in the section below.

4.2.1 (Phase 1) transaction generation phase

Users within a network have the address of all other users before initiating any transfer. For an instance, if Alice wants to transfer 10 BTC to Bob then the transaction that executes the amount transfer among users includes the following.

- *Input transaction* The Unused Transaction Outputs (UTXOs) of the source transaction serves as input transaction. This refers to the transaction's hash that provides information about the source from which Alice received that 10 BTC that he wants to transfer.
- *Amount transferred* The amount transferred in this case is 10 BTC.
- *Hash value of the receiver's public key* This refers to the bitcoin address of Bob where this 10 BTC is to be received. The recipient's public key and the transaction identity (SHA 256 hash of input transaction) uniquely identifies a transaction. Further, digital signatures are generated for uniquely identifying the source using encryption via sender's private key. In case of any changed content, the signatures as well as the transaction identity is affected and the transaction is discarded if there is a mismatch.

4.2.2 (Phase 2) transaction confirmation phase

When Bob comes to know that Alice is crediting funds to his bitcoin address, he makes a confirmation about the existence of transaction in a valid ledger block and also about the non-existence of double spending by Alice. Transactions are committed only if the following operations takes place upon receipt of the transaction.

- Bob validates that there is no double spending in the UTXO of the referenced input transaction. Nakamoto proposed to redeem the output transaction in one subsequent transaction in order to prevent the double spending issues in Bitcoin. This means that only after

verifying both the transactions using signatures successfully, output is redeemed in next transaction.
- Use the UTXO for subsequent transaction.
- Validation of a transaction is confirmed therefore it must be associated with a valid block.
- During currency transfer, the *law of conservation of value* must be preserved. It states that the total input UTXOs is equal to total output UTXOs minus the coin base transactions amount.

Figure 5 depicts the transaction confirmation phase along with the verification process between the network nodes.

4.2.3 (Phase 3) claiming ownership phase

Output redeemable by legitimate recipient nodes is produced by each and every transaction in their public key hash. This hash uniquely identifies the users in the network and thereby authenticates them and preserves their privacy. Moreover, the users need a private key apart from their pseudonymous identity in order to gain access to their bitcoins. Users capable of generating valid signatures with the help of their private keys can only claim ownership and redeem their transaction outputs. In order to redeem funds, a user must therefore have both the private key and the public key hash.

4.2.4 (Phase 4) consensus and mining phase

In order to discard transactions or blocks to avoid any conflicts later on, nodes follow a consensus mechanism if there does not exist any third party. The PoW concept helps to achieve the consensus in bitcoin as it puts forth the amount of work put in for a block validation. Therefore, in order to accept a block and add it to the shared ledger, a cryptographic puzzle needs to be solved. This involves the nodes to accumulate all the verified transactions within the block and with the help of their own resources generate a SHA-256 hash value which is smaller than dynamically changing target value. The contents within a block include previous blocks hash, block version, timestamp, arbitrary nonce and listed transactions Merkle root hash. PoW is the random value decided by miners by repeated hashing.

4.2.5 (Phase 5) block validation phase

There are four mandatory block validation steps. Firstly, the chronological order of transactions based on their reference and occurrence is confirmed. Secondly, the current block referencing the previous blocks hash needs to be validated. Thirdly, the verification of the timestamp accuracy is done and finally the PoW for the current block is validated.

Table 6 presents the summary of various phases of blockchain operations.

4.3 Optimized blockchain architecture for IoT applications

Blockchain technology can bring forth numerous benefits to IoT. However, these are not explicitly devised to support IoT environments therefore various blockchain

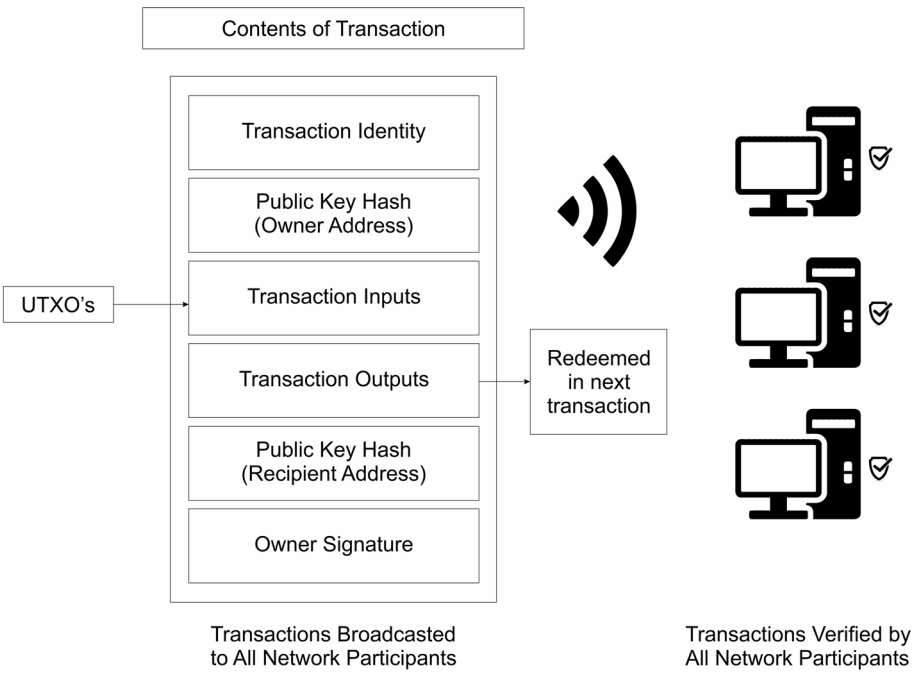

Fig. 5 The transaction confirmation phase

Table 6 Phases of blockchain operations

Phase of operation	Summary or description
(Phase 1) transaction generation phase	Input transaction
	Amount transferred
	Hash value of the receiver's public key
(Phase 2) transaction confirmation phase	After verifying both the transactions using signatures successfully, output is redeemed in next transaction.
	During currency transfer, the *law of conservation of value* must be preserved
(Phase 3) claiming ownership phase	In order to redeem funds, a user must have both the private key and the public key hash
(Phase 4) consensus and mining phase	In order to accept a block and add it to the shared ledger, a cryptographic puzzle needs to be solved
	The contents within a block include previous blocks hash, block version, timestamp, arbitrary nonce and listed transactions Merkle root hash
(Phase 5) block validation phase	The verification of the timestamp accuracy is done and finally the PoW for the current block is validated

components needs to be optimized to make them adaptable to such environments. Several authors analysed the performance of BIoT under various scenarios by considering some influential aspects especially the consensus algorithms. Generally, IoT applications generate huge amount of traffic therefor the architecture supporting Blockchain based IoT applications must be adapted to handling huge traffic. This problem is more prominent in traditional cloud-based architecture where the node layer forwards the data to the cloud using IoT gateways. Moreover, these architectures also possess inherent vulnerabilities as the cloud is susceptible to failure due to software failures, human errors, external intrusions, maintenance problems or cyber-attacks [149, 150]. Even if a single IoT device is compromised, the entire system breaks down due to Denial of Service attack [151], data altering, misleading systems [152] or eavesdropping attack [153, 154].

Several architectures proposed in the literature have explored the architectural issues associated with the BIoT service providers. Liao et al. [155] discussed merits and demerits of four different architectures namely Fully Distributed, Distributed Things, Pseudo Distributed Things and Fully Centralized Things. The work concludes that in most cases the Fully Distributed architecture must be followed by BIoT architectures and in case of constrained cost or power, other approaches might be suitable. In another work, Dorri et al. [156] proposed a theoretical lightweight BIoT architecture that mitigates the communication overhead introduced by the use of blockchain. The proposed architecture is home automation oriented and is divided into three layers: a cloud layer to provide remote storage; an overlay network of shared storage and peers; and a smart home layer that comprises of local storage, actuators and sensors.

IoT has gained much significance and attraction due to its global vision enabling the seamless interconnection between devices and the environment. Taking this into consideration, Daza et al. [157] proposed a blockchain based theoretical architecture that focusses on connecting heterogeneous devices and providing IoT services. This scheme is based on multi-layered hierarchical blockchain that builds a service discovery system. Li et al. [158] proposed another multi-layered IoT architecture that focussed on mitigating the blockchain deployment complexity by introducing different levels in IoT ecosystem and using one blockchain in one level. Samaniego et al. [159] presented another approach to counter the problem of hosting a blockchain on resource constrained traditional IoT hardware architecture. It evaluated the use of fog and cloud computing architectures for BIoT applications. The empirical performance evaluation of the system demonstrated that the fog system outperforms the cloud-based systems in terms of latency response time under high transmission loads. Stanciu et al. [160] presented another edge-based computing architecture that focussed on emergence of distributed and hierarchical platform that uses IEC 61499 standard. Sharma et al. [161] suggested to use software defined networks (SDN) for BIoT applications to control the fog nodes of the network. Computing intensive tasks are performed using cloud and low latency data access is provided using fog computing. The obtained results depicted that the proposed architecture increases throughput, mitigates delays and also detects several real time IoT network attacks. Table 7 presents the characteristic features of various proposed BIoT architectures in the literature.

Table 7 Proposed BIoT architecture

Proposed architecture	Characteristic features
Liao et al. [155]	Fully Distributed architecture must be followed by BIoT architectures
Dorri et al. [156]	Theoretical lightweight BIoT architecture that considers privacy and security issues
Daza et al. [157]	Blockchain based theoretical architecture that focusses on connecting heterogeneous devices and providing IoT services
Li et al. [158]	Multi-layered IoT architecture that focussed on mitigating the blockchain deployment complexity by introducing different levels in IoT ecosystem
Samaniego et al. [159]	Evaluated the use of fog and cloud computing architectures for BIoT applications
Stanciu et al. [160]	Edge-based computing architecture that focussed on emergence of distributed and hierarchical platform that uses IEC 61499 standard
Sharma et al. [161]	SDN for BIoT applications to control the fog nodes of the network

5 Blockchain-based IoT security

Exponential increase in attacks have been reported due to amalgamation of physical world and the internet leading to complex security implications [162]. The security issues faced by centralized IoT architectures and the potential benefits of blockchain integration with IoT is discussed in this section. *Over expanding edge* brings forth the major security challenge in IoT as nodes at the network edge are the most vulnerable points where huge range of attacks can be launched. A set of malicious nodes and other devices at the IoT edge may launch botnet attacks that can completely collapse the IoT service provisioning [163]. *Heavily centralized configurations* in IoT is another cause of threat to IoT service provisioning availability [164]. Not only availability but a central failure point is also a threat to authorisation and confidentiality as the service provider may tamper or misuse the user's data [165]. Furthermore, identity spoofing as well as analysing traffic information might lead to confidentiality compromising attack. IoT faces integrity attacks such as Byzantine attacks and modification attacks [166]. Injection attacks in centralized IoT configurations challenges data integrity as the decision-making policy in these configurations rely on the incoming data streams. IoT downtime, data theft and data alteration may lead to losses of varying intensity. Ensuring security is of utmost importance for a system where autonomous interaction among smart devices is required. The current IoT security solutions involves third party-based security solutions and are centralized.

Use of blockchain for enforcing security without being dependent on a third party have proved to be significantly beneficial for the IoT systems. With virtues of in-built protection, auditability, fault-tolerant design and decentralized public key infrastructure against numerous attacks, blockchain is able to deliver security to transactive networks such as Bitcoin. Since all devices involved in a transaction possess a dedicated blockchain address, the blockchain based solution is false authentication resistant. The blockchain consensus protocols are capable of preventing malicious users from launching DoS attacks as transaction fees is required every time even for making empty transactions [167]. Thus, blockchain is more than capable of providing improved security to the IoT stack as discussed in the subsection below.

5.1 Blockchain provides access control

In the recent past, numerous researchers proposed to enforce access control policies in an IoT system without the need of any third-party involvements. Axon et al. [168] presented a fault tolerant and secure public key infrastructure. Hashemi et al. [169] presented a multi layered blockchain architecture that performs access control and data storage at different layers. The proposed framework consists of three layers: (1) blockchain based decentralized storage for storing the user's data; (2) access control mechanism; (3) a messaging stream for negotiating access between the two parties. Blockchain data is stored in an encrypted format that can only be decrypted by the participants possessing access privileges. Zhang et al. [170] introduced a token-based access control approach in IoT. Quaddah et al. [171] presented a tokenised access control approach that assigns different access roles to different users and access privileges can be revoked using smart contracts. Novo et al. [172] proposed to store encrypted data chunks in blockchain and used smart contract policies and a tokenized approach for revoking and allowing IoT data access.

Blockchain can be used to detect malicious activity and manage access privileges in approaches that focusses on designing applications without tokenization or reducing

transaction fees. Dorri et al. [173] proposed to use local blockchains in connection with the public overlay blockchain. Publicly verifiable blockchains stores access privilege decisions thereby are capable of detecting attempts of unauthorized access. Ali et al. [174] enhanced the idea by not considering the transactions from unauthorised users. Shafagh et al. [175] presented a blockchain based access control schemes that stores data in decentralized off-chain hash tables. In this, the blockchain stores access privileges for various users and the nodes access the blockchain records for making access control decisions.

5.2 Blockchain maintains data integrity

In a Blockchain based IoT system, an adversary attempts to create false blocks. However, in publicly implemented blockchain, this is not at all possible due to the use of distributed consensus for the maintenance of canonical blockchain records. Biswas et al. [176] proposed to guarantee data integrity in a blockchain based smart city systems. Programmability was defined on top of the decentralized blockchain records using smart contracts and Ethereum blockchain. Dorri et al. [173] proposed to maintain the IoT data chunk records in the cloud using a multi-tiered blockchain framework. The employed public overlay blockchain maintains immutable data chunk records using hashing. Shafagh et al. [175] proposed data storage scheme based on immutable blockchain records and decentralized hash tables. Blockchain maintains data integrity and access control policies while data requests are made to the DHT nodes. Kang et al. [177] proposed a data integrity scheme employing blockchain which performs query-based integrity checks without the need of any third-party verification. Data integrity loss is detected by the blockchain record verification process. Yang et al. [178] presented a credibility assessment scheme based on blockchain for Internet of Vehicles. The blockchain based reputation scheme make decisions on the message credibility on the basis of the sender's reputation.

While applying blockchain to IoT for receiving secure software updates is a hot topic of interest. Lee et al. [179] proposed peer to peer schemes in which the embedded IoT devices receives secured updates and ensures firmware integrity in a blockchain network. Steger et al. [180] proposed a scalability ensuring tiered blockchain architecture and secured software update schemes for smart vehicles. This enables the software updates to propagate to the vehicles in a secured way without compromising the data integrity. Further, Boudguiga et al. [181] proposed to employ permissioned blockchains for storing the software updates in secured peer to peer fashion for IoT devices.

5.3 Blockchain improves availability

Solutions providing on-chain data storage have no central vulnerable points and therefore possess built-in availability features. This availability of the interaction records is further improved by off-chain storage mechanisms. In this section, we discuss the unique design solutions proposed to enhance the IoT availability. Alphand et al. [182] proposed an authorization scheme for IoT that employs blockchain for providing high liveness degree. Chakraborty et al. [183] proposed to handle the resource constrained issues of IoT devices by using multi-layered blockchain solutions. Nodes located at the higher level possess higher storage and computational capabilities whereas the resource constrained nodes situated at the lower layers are not capable of enforcing security policies. Higher layer nodes facilitate the communications among the lower level resource constrained nodes. Ali et al. [174] proposed smart contract and multi-layered blockchain scheme to guarantee access control. Public Ethereum blockchain is employed at the higher tier that ensures availability. Bahga et al. [184] proposed blockchain-based manufacturing system in which users have the flexibility of issuing direct manufacturing commands during transactions. It is beneficial for several transactions such as supply chain tracking, machine diagnostics and on-demand manufacturing. The authors also presented a diagnostics and machine maintenance use cases. This decentralized connected device enables the network to stay alive even in case of multiple machine faults.

5.4 Blockchain ensures data confidentiality

Blockchain based architectures possess in built confidentiality and authorization features as it involves every transaction to be signed using issuers private key. Axon et al. [168] proposed blockchain based PKI for effectively managing the IoT systems. It employed smart contracts for issuing orders such as recording energy usage information and changing working policies onto the blockchain. Ouaddah et al. [171] proposed a tokenised approach named "Fair Access" that allows access privileges by issuing custom cryptocurrency to transactions. The private key of the requester is used to sign the access granting transactions enabling confidentially revoked access privileges. Alphand et al. [182] proposed an IoT security management platform that maintains interaction records and enforces authorisation policies. Authors employed blockchain for enforcing flexibility in setting the authorisation policies along with maintaining a record of access events. Aitzhan et al. [185] proposed security schemes to enforce confidentiality in energy transacting smart grids. This work aims

to hide the energy producer's identity along with keeping the shared information confidential. Authors suggested to generate and alter the energy producers address in order to hide the producer's identity. Cha et al. [186] proposed a signature based blockchain that use Ethereum blockchain for maintaining confidentiality between IoT gateways and wearables. These gateways make use of smart contracts for interacting with these devices thereby making the IoT interactions confidential.

Table 8 shows the Blockchain based IoT security schemes proposed in recent research.

6 BIoT: applications and current challenges

6.1 BIoT applications

Blockchain technology has the potential to be applied in many use cases and fields. The evolution of blockchain applicability initiated with Version 1.0 of Blockchain (Bitcoin), then evolved towards the Version 2.0 (Smart contracts) and later on shifted to Version 3.0 of Blockchain (Coordination and efficiency applications). Smart contracts can be defined as decentralized self-sufficient code pieces capable of being executed when some predefined conditions are satisfied. These smarts contracts have huge application areas including crowd funding, mortgages or

Table 8 Blockchain based IoT security solutions

IoT security principles	Proposed solutions	Characteristic features
Access control	Axon et al. [168]	Fault tolerant and secure public key infrastructure
	Hashemi et al. [169]	Multi layered blockchain architecture
	Zhang et al. [170]	Token-based access control approach in IoT through smart contracts and blockchains
	Quaddah et al. [171]	Tokenised access control approach
	Novo et al. [172]	Store encrypted data chunks in blockchain
	Dorri et al. [173]	Use local blockchains in connection with the public overlay blockchain
	Ali et al. [174]	Drops transactions issued from unauthorised adversary
	Shafagh et al. [175]	Stores data in decentralized off-chain hash tables
Data Integrity	Dorri et al. [173]	Cloud based multi-layered blockchain
	Shafagh et al. [175]	Data storage scheme based on immutable blockchain records and decentralized hash tables
	Biswas et al. [176]	Decentralized blockchain records using smart contracts and Ethereum blockchain
	Kang et al. [177]	Blockchain based data integrity scheme for cloud
	Yang et al. [178]	Credibility assessment scheme based on blockchain for Internet of Vehicles
	Lee et al. [179]	Peer to peer schemes in which the embedded IoT devices receives secured updates and ensures firmware integrity
	Steger et al. [180]	Scalability ensuring tiered blockchain architecture
	Boudguiga et al. [181]	Permissioned blockchains for storing the software updates
Data availability	Ali et al. [174]	IPFS file access transaction over public ethernet blockchain
	Alphand et al. [182]	Authorization scheme for IoT that employs blockchain for providing high liveness degree.
	Chakraborty et al. [183]	Handle the resource constrained issues of IoT devices by using multi-layered blockchain solutions
	Bahga et al. [184]	Blockchain-based manufacturing system
Data confidentiality	Axon et al. [168]	Secure public key infrastructure
	Ouaddah et al. [171]	Tokenised approach named "Fair Access" that allows access privileges by issuing custom cryptocurrency to transactions
	Alphand et al. [182]	IoT security management platform that maintains interaction records and enforces authorisation policies
	Aitzhan et al. [185]	Enforce confidentiality in energy transacting smart grids
	Cha et al. [186]	Signature based blockchain that use Ethereum for maintaining confidentiality between IoT gateways

international transfers [187]. Beyond smart contracts and cryptocurrencies, blockchain can be used in IoT application areas like sensing [188], cyber law [189], crowd sensing [190], wearables [191], timestamping services [192], identity management [193], intelligent transportation system [194], healthcare applications [195] and smart living applications [196]. Blockchain is also useful for IoT based agricultural applications. Tian et al. [197] proposed a traceability system based on blockchain and RFID that tracks Chinese agri-food products and aims to enhance the food safety as well as quality. Huh et al. [198] proposed blockchain for managing IoT devices using a system capable of remotely configuring and controlling IoT devices. Authors also highlighted the significance of Ethereum as it facilitates bug corrections and simple maintenance.

Unification of blockchain and IoT also benefits the energy sector or the Internet of Energy (IoE) [199, 200]. Lundqvist et al. [201] proposed a blockchain based system facilitating IoE/IoT devices to make payments without any human intervention. They described an implementation showing smart cable connected to smart socket for paying bills of the consumed electricity. Moreover, there is an existence of healthcare BIoT applications. Bocek et al. [202] proposed a traceability application that uses blockchain technology and IoT sensors to verify data accessibility and integrity in pharmaceutical supply chain. Shae et al. [203] proposed another healthcare BIoT application that makes use of blockchain based architecture for precision medicine and clinical trials. Salahuddin et al. [204] proposed a smart generic healthcare system that uses blockchain, fog and cloud computing [205], IoT devices and message brokers.

Blockchain technology can also enhance the low-level security of IoT. It improves the remote attestation process which is capable of verifying the trustworthiness of the Trusted Computer Base (TCB) associated with the device [206]. This verification process is completed by managing the TCB measurements retrieved using a blockchain that stores these TCB measurements securely. Several other BIoT applications includes industrial processes [207] and smart cities [208]. Figure 6 depicts the various BIoT applications.

6.2 Current challenges related to BIoT applications

Several challenges are faced by emerging IoT ecosystem technologies such as 5G/4G broadband communication [209, 210], telemetry systems [211], RFID [212] and Cyber Physical Systems (CPSs) [213, 214]. These challenges are more prominent and rise additional concerns in case of mission critical applications. Integration of blockchain to this brings forth additional technical and operational requirements owing to the complexity associated with the BIoT applications. The major factors that affect the BIoT application development is described in further subsections.

6.2.1 Energy efficiency

Owing to the resource constrained IoT end nodes, energy efficiency is of utmost importance for enabling long-lasting node deployment. However, blockchains are power hungry and incurs high energy consumption due to *P2P communication* and *mining*. Blockchains such as bitcoin consumes enormous electricity in the mining process due to involvement of consensus algorithm. P2P communications require continuously powered devices which may lead to energy wastage [215]. Liao et al. [216] proposed energy efficient P2P protocols but this needs to be explored further for making it suitable for IoT networks.

6.2.2 Security

Three major security requirements that needs to be fulfilled to guarantee security in any information systems are *confidentiality*, *integrity* and *availability*. Validity of current IoT systems is preserved as long as system remains robust against leaks or attacks and centralized infrastructure administrators remain trusted. In contrast, a blockchain based applications are decentralized and the global system remains working even after some nodes are compromised. Guaranteeing internet security makes use of certificates that use public key infrastructure for preserving third part trusts. However, such authorities fail in certain circumstances [217]. Data integrity is another essential component for IoT applications. Liu et al. [218] proposed integrity service framework that uses blockchain technologies instead of trusting a third party for cloud based IoT applications. Moreover, huge range of attacks in IoT systems might compromise its availability. *Majority attack* or *51 percent attack* is the most feared attack for an IoT system. In such attack, entire blockchain can be controlled by one single miner to perform transactions at wish.

6.2.3 Privacy

Anonymity of blockchain users are not guaranteed as all the blockchain users are identified by their hash or public key and the transactions are shared for third parties to infer and analyse the actual user identities [219]. Privacy in IoT environments is even more complex as private user data can be revealed by IoT devices. IoT applications suffer from identity certification problem. Kravitz et al. [220] proposed to use permissioned blockchains for managing and securing the IoT nodes thereby providing an identity

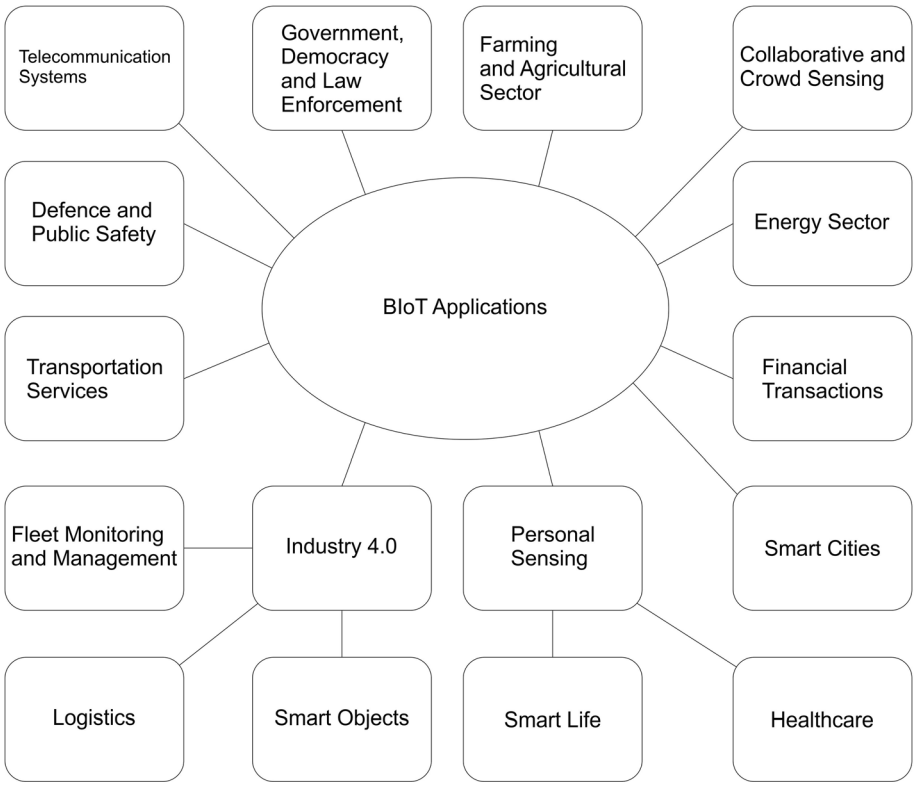

Fig. 6 BIoT applications

management solution with rotating asymmetric keys capable of countering attacks. Access controls in a private blockchain assumes the access controller's neutrality and reduces exposure. It also introduces added communication complexity. *Zero knowledge proof* is another scheme that avoids revealing of user identities during any transaction and thereby provides the desired level of authentication. Hayouni et al. [221] proposed to use homomorphic encryption scheme as another privacy preserving solution. It enables the transaction to be processed by third-party IoT services without the need of exposing the unencrypted data to them. However, the resource constrained nature of IoT devices makes the applicability of these techniques limited.

6.2.4 Throughput and latency

Deployment of an IoT might need a blockchain based architecture for managing huge number of transactions per unit time. However, this becomes a limitation for several networks such as bitcoins that can support not more than 7 transactions per second. However, Courtois et al. [222] proposed to increase this limit by modifying node behaviour and processing larger aspects. In terms of latency, the blockchain transactions consume more processing time. For an instance, block creation in bitcoin follows Poisson distribution and consumes more time. Even if it is capable of avoiding the double spending problems, merchants need to wait for a long time as before the transaction is confirmed, several blocks need to be added to the chain.

6.2.5 Blockchain infrastructure

Users store their transactions leading to periodic growth of blockchains that results in larger initial download time and use of enhanced miners having larger persistent memories. IoT nodes are not capable of handling the traditional blockchain and this brings forth the need to study blockchain compression techniques. Moreover, several IoT nodes might need to store unnecessary data leading to wastage of computational resources. Light weight nodes are more than capable of handling this issue and performing blockchain transactions. However, it requires several powerful nodes in IoT hierarchy to maintain a required degree of data centralization. Also, the block and transaction size need to be scaled on the basis of *bandwidth limitations* of the IoT systems. Larger transactions involve big payload and cannot be effectively managed by IoT devices while a smaller transaction elevate the energy consumption in communication. Considering the *infrastructure*, elements such as communication protocols, decentralized storage, network administration, address management and mining hardware are required for proper operation of blockchain.

7 Future research directions

Apart from its huge range of advantages, blockchain also faces numerous challenges in its advances and its adoption in IoT. These challenges can be broadly classified into three categories: *scalability*, *privacy preservation* and *utilization* in resource constrained environment. These administrative trade-offs, challenges and future research scope towards blockchain integration in IoT is discussed in this section.

7.1 Scalability issues in blockchain

Scaling the blockchain is an active research area and numerous approaches have been proposed in the recent research to improve the blockchain scalability [223, 224]. More promising blockchain based solution involves limiting the consensus over varied network portions or connecting multiple blockchains by developing inter blockchain communication. Blockchain scalability is still a paramount issue for its implementation in digital finance due to high networking overhead and performance demands of these applications. Existing public blockchain is not suitable enough for digital finance applications due to its high transaction processing speed requirements. Owing to the huge amount of transaction data in IoT, low throughput issues gets exacerbated. One potential direction to this end is to scale the blockchain vertically in the form of distributed database. However, scaling the blockchain horizontally tends to solve the scalability issues in blockchain making inter-blockchain communication an important research direction.

7.2 Constrained IoT edge device

Traditional internet is augmented by the advancements in IoT as these connect them to smart devices for carrying out automated tasks. Generally, IoT devices possess strict networking and computational constraints which renders them incapable to engage in PoW consensus or use blockchain based decentralized architectures. Integration of blockchain and these IoT devices results in limited degree of decentralization. Dorri et al. [225] proposed a memory optimized blockchain for large scale IoT networks. Extending blockchain to support the IoT edge is another key future research direction. High networking and performance overhead of blockchain limits the use of blockchain over constrained IoT devices. Use of computationally capable IoT gateways for performing end-to-end blockchain communications is a near acceptable proposed solution. Enabling gateways and IoT devices to use blockchain without the need to create a centralized block validation pool is another interesting research direction [226].

7.3 Blockchain infrastructure and complex technical challenges

Creation of comprehensive trust infrastructure that meets all the requirements for using blockchain in an IoT system is the need of the hour. Moreover, blockchain faces design limitations in implementation of smart contracts, in validation protocols or in transaction capacity. These limitations along with design issues to address the security, stability and cryptographic development requirements is another important research direction. Moreover, besides the technological challenges, moulding the regulatory environment such as international jurisdiction and decentralized ownership is the major issues for unlocking the potential BIoT values [227].

7.4 Cellular networks and blockchains for IoT

Finding a balance between the decentralized and centralized control mechanisms is an emerging research area with the evolution of cellular networks. IoT edge heavily relies on cellular networking. Decentralizing cellular networks enables the inherent security features of blockchain (application layer security features) to be used by the IoT edge [228]. However, research in this direction is at very nascent stage. Blockchains may prove an effective scheme to host virtualized resources and assist cellular networks with existing approaches such as optimization of application layer traffic [229]. Logical evolution of such networks can be enhanced by virtualized network resources and resource scheduling can be performed using blockchains. These issues can pave way for further research directions that will yield interesting outcomes.

7.5 Privacy concerns related to permission-less blockchains

In case of bitcoin, all the transaction records are accessible to the network participants. The generated blockchain addresses are associated with the stored transactions instead of being linked with any real-world entities. Users in such systems are capable of carrying out transactions on multiple addresses. Therefore, all the transaction information is stored at one address to avoid the information leakage [230]. Such open records can reveal user information due to interferences and also can be utilized to track and triangulate IP address of the user [231]. Drawing inferences from the graphical network analysis of the user transactions may lead to privacy breach [232]. Maintaining a balance between preserving privacy and accountability in

a Blockchain based IoT framework prompted many proposed solutions. Majority of the proposed solutions considers implementation of access policies either through smart contracts or within the blockchain itself. Tiered architecture is another promising method for preserving privacy in a blockchain based framework. Maintaining data integrity in such tiered architecture or within a private blockchains is an important challenge. Moreover, preventing the double spending problem and providing required level of auditability forced to sacrifice the blockchains anonymity, therefore guaranteeing privacy for blockchain based applications is a fertile research area [233].

7.6 Decentralizing IoT with machine learning (ML) and big data

ML is an Artificial Intelligence (AI) technique that can train machines and help devices learn from their past experience without relying on any complicated mathematical equation or requiring any kind of human assistance [234]. ML schemes can help IoT to a great extent in order to make intelligent decisions for optimizing automation tasks including energy transactions, scheduling and managing IoT assets. ML schemes can bolster security of the Blockchain based IoT architecture as it has the potential to identify as well as predict various cybersecurity attacks and vulnerabilities. Further, ML schemes can serve as an efficient mechanism to detect attacks in an IoT systems at an early stage by analysing the system behaviour [235]. Shen et al. [236] proposed a Support Vector Machine (SVM) training model over IoT data which is encrypted using blockchain and recorded on a distributed ledger. The proposed scheme achieves privacy preserving and thereby ensures confidentiality. In another work, Roldan et al. [237] proposed to integrate ML and Complex Event Processing (CEP) schemes for real time attack detection as well as efficient event management in an IoT system. ML algorithm requires a reliable data sample so that it can prepare accurate training data sets, as low-quality or noisy data might severely degrade the learning method. Therefore, decentralizing IoT with ML face a major challenge related to authentication of the training data sets [238]. Further, if the adversary is aware of the attack type and has the capability to manipulate the training dataset, it can easily modify its type and attacks in the network. Therefore, exact identification of attack to effectively distinguish between the desirable and non-desirable network states is another challenging issue that needs further investigation. Deep Learning (DL), a subset of ML has also been widely implemented for enhancing IoT security [239, 240] and traffic classification [241, 242]. DL has gained importance owing to its self-learning, unsupervised pre-training, non-manual feature engineering and faster processing capabilities. Furthermore, sensors and IoT devices continuously generate huge amount of structured, unstructured, or semi structured data. Big data technology is an effective paradigm that can process various types of data and also contribute to the security enhancement of the IoT systems [243]. Numerous big data based IoT solutions have been proposed. Guo et al. [244] proposed a scheme for secure big data collection in Internet of Vehicles. Chui et al. [245] proposed a big data and IoT integrated framework for monitoring the patient's behaviour (such as emotion, physical action and vital sign) in a healthcare unit. In another work, Zhou et al. [246] proposed a big data mining scheme for managing financial risks in commercial banks accompanied by IoT deployment. Although, temporary identifications, encryption and anonymity enforces data security, decisions need to be taken regarding the ethical factors, such as why and how to use the generated big IoT data [247]. Majority of the proposed strategy related to decentralization of IoT using ML and big data are still in their infancy and needs further investigation.

Table 9 presents the summary of future research directions towards blockchain integration in IoT.

8 Conclusion

Technological advances of internet enabled world, rising competition for scarce resources and increased societal challenges accelerated the transformation to a data-driven world. Today's IoT systems are lacking capability to defend themselves and are insecure majorly due to its resource constrained devices, immature standards, resources diversity, and the absence of secure hardware and software design, deployment, and development. In such systems, a centralized authorization, authentication and access models force the end users to trust a third party for processing, handling and managing their IoT data. In such an ecosystem, blockchain can offer a platform for sharing information to IoT that defies non-collaborative organizational structures. Blockchains achieve secure and immutable records using distributed consensus mechanisms thereby providing a *trust-less* record keeping environment. Further, blockchain is capable of providing a decentralized IoT fabric that needs no authorizing or managing intermediaries. However, one can easily fall into risks like amending any technology without adequately assuring its behaviour or applying it to the frameworks in which cost does not adequately compensate the improvement. Therefore, the benefits of applying blockchains to IoT systems needs careful analysis and caution.

Table 9 Future research directions towards BIoT

Research directions	Interpretations
Scalability issues in blockchain [223, 224]	Increasing storage requirements due to storage of network wide transactions
	Reduced transaction throughput owing to the decentralized consensus in permission less blockchains
Constrained IoT edge device [225, 226]	Computational complexity requirement of resource constrained IoT devices
	Need of substantial storage and computational capabilities for blockchain connected IoT gateways
Blockchain infrastructure [227]	Design limitations in implementation of smart contracts, in validation protocols or in transaction capacity
	Creation of comprehensive trust infrastructure
	Address the security, stability and cryptographic development requirements
Cellular networks and blockchains for IoT [228, 229]	Blockchains may prove an effective scheme to host virtualized resources and assist cellular networks
	Resource scheduling
Blockchain privacy concerns [230–233]	Pseudonymous addressing in blockchains leading to privacy requirements
	Permission less blockchain contents are publicly accessible for auditability
	Maintaining data integrity in tiered architecture
ML and big data for decentralizing IoT [234–247]	Leveraging blockchains for big data applications and maintaining crowdsensing
	Decentralizing IoT with ML related to authentication of the training data sets
	Taking decision regarding the ethical factors, such as why and how to use the generated big IoT data

In this paper, we presented a comprehensive survey of recent contributions in developing blockchain based services, applications and platforms suitable for new IoT era. The paper throws light on the main challenges that needs to be addressed for successful integration of blockchain and IoT. We highlighted various scopes within the IoT framework focussing on the characteristics, requirements and the possible security threats. We discussed evolution, basic functioning, classification and working models of blockchain along with the advantages of blockchain based decentralization. Moreover, a holistic approach to BIoT scenarios along with an optimized BIoT design aspects are presented. Furthermore, we provide some recommendations with the aim to guide future BIoT researchers about challenges that needs to be tackled before the deployment of further generation of BIoT applications. To conclude, we have conducted an in-depth survey of blockchain along with its characteristic features and technical working principles. We can conclude that BIoT applications do not have any one-size-fits-all solution. Therefore, reassessing the various factors and activities involved in BIoT applications is necessary. Even though, blockchain brings forth numerous advantages like decentralization, security, openness and publicly available transactions, still some investigation related to mining process and network stability of blockchain system needs to be done. We can conclude that development and deployment of BIoT is in nascent stage and additional technological advances are required to address the specific demands for its broader use.

References

1. Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. *IEEE Access, 6,* 67893–67926. https://doi.org/10.1109/access.2018.2879189.
2. Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics, 14*(11), 4724–4734. https://doi.org/10.1109/tii.2018.2852491.
3. Fan, K., Luo, Q., Zhang, K., & Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. *Information Sciences, 527,* 329–340. https://doi.org/10.1016/j.ins.2019.08.006.
4. Chi, T., & Chen, M. (2017). A frequency hopping method for spatial RFID/WiFi/Bluetooth scheduling in agricultural IoT. *Wireless Networks, 25*(2), 805–817. https://doi.org/10.1007/s11276-017-1593-z.
5. Chowdhury, A., & Raut, S. A. (2018). A survey study on internet of things resource management. *Journal of Network and Computer Applications, 120,* 42–60. https://doi.org/10.1016/j.jnca.2018.07.007.
6. Tran-Dang, H., & Kim, D. (2018). An information framework for internet of things services in physical internet. *IEEE Access, 6,* 43967–43977. https://doi.org/10.1109/access.2018.2864310.
7. Choo, K. R., Gritzalis, S., & Park, J. H. (2018). Cryptographic solutions for industrial internet-of-things: Research challenges

and opportunities. *IEEE Transactions on Industrial Informatics, 14*(8), 3567–3569. https://doi.org/10.1109/tii.2018.2841049.
8. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & Alvarenga, S. C. D. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications, 84,* 25–37. https://doi.org/10.1016/j.jnca.2017.02.009.
9. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical Systems and Signal Processing, 135,* 106382. https://doi.org/10.1016/j.ymssp.2019.106382.
10. Landau, S. (2013). Making sense from snowden: Whats significant in the NSA surveillance revelations. *IEEE Security and Privacy, 11*(4), 54–63. https://doi.org/10.1109/msp.2013.90.
11. Landau, S. (2014). Highlights from making sense of snowden, part II: Whats significant in the NSA revelations. *IEEE Security and Privacy, 12*(1), 62–64. https://doi.org/10.1109/msp.2013.161.
12. Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the internet of things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management, 51,* 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008.
13. Chettri, L., & Bera, R. (2020). A comprehensive survey on internet of things (IoT) toward 5G wireless systems. *IEEE Internet of Things Journal, 7*(1), 16–32. https://doi.org/10.1109/jiot.2019.2948888.
14. Corno, F., Russis, L. D., & Saenz, J. P. (2020). How is open source software development different in popular IoT projects? *IEEE Access, 8,* 28337–28348. https://doi.org/10.1109/access.2020.2972364.
15. Alaa, M., Zaidan, A., Zaidan, B., Talal, M., & Kiah, M. (2017). A review of smart home applications based on internet of things. *Journal of Network and Computer Applications, 97,* 48–65. https://doi.org/10.1016/j.jnca.2017.08.017.
16. Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? A systematic review. *PLoS ONE*. https://doi.org/10.1371/journal.pone.0163477.
17. Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. *Computer, 50*(9), 18–28. https://doi.org/10.1109/mc.2017.3571064.
18. Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons, 62*(3), 295–306. https://doi.org/10.1016/j.bushor.2019.01.009.
19. Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*. https://doi.org/10.1016/j.jii.2019.04.002.
20. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media.
21. Brody, P., Pureswaran, V., Panikkar, S., & Nair, S. (2015). Empowering the edge practical insights on a decentralized internet of things. IBM Institute for Business Value. Technical report.
22. Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*. https://doi.org/10.1016/j.jbvi.2019.e00151.
23. Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*. https://doi.org/10.5210/fm.v2i9.548.
24. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4,* 2292–2303. https://doi.org/10.1109/access.2016.2566339.
25. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the IEEE international congress on big data (big data congress), Honolulu, United States, 25–30 June 2017* (pp. 557–564). https://doi.org/10.1109/bigdatacongress.2017.85.
26. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82,* 395–411. https://doi.org/10.1016/j.future.2017.11.022.
27. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88,* 173–190. https://doi.org/10.1016/j.future.2018.05.046.
28. Yeow, K., Gani, A., Ahmad, R. W., Rodrigues, J. J., & Ko, K. (2018). Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access, 6,* 1513–1524. https://doi.org/10.1109/access.2017.2779263.
29. Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. *Sensors, 18*(8), 2575. https://doi.org/10.3390/s18082575.
30. Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., et al. (2019). Survey on blockchain for internet of things. *Computer Communications, 136,* 10–29. https://doi.org/10.1016/j.comcom.2019.01.006.
31. Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., & Rong, C. (2019). A comprehensive survey of blockchain: From theory to IoT applications and beyond. *IEEE Internet of Things Journal, 6*(5), 8114–8154. https://doi.org/10.1109/jiot.2019.2922538.
32. Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the internet of things. *IEEE Communications Surveys & Tutorials, 21*(2), 1636–1675. https://doi.org/10.1109/comst.2018.2874978.
33. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things, 8,* 100107. https://doi.org/10.1016/j.iot.2019.100107.
34. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36,* 55–81. https://doi.org/10.1016/j.tele.2018.11.006.
35. Hamad, S. A., Sheng, Q. Z., Zhang, W. E., & Nepal, S. (2020). Realizing an internet of secure things: A survey on issues and enabling technologies. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/comst.2020.2976075.
36. Butun, I., Osterberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644. https://doi.org/10.1109/comst.2019.2953364.
37. Lao, L., Li, Z., Hou, S., Xiao, B., Guo, S., & Yang, Y. (2020). A survey of IoT applications in blockchain systems. *ACM Computing Surveys, 53*(1), 1–32. https://doi.org/10.1145/3372136.
38. Maharaja, R., Iyer, P., & Ye, Z. (2019). A hybrid fog-cloud approach for securing the internet of things. *Cluster Computing*. https://doi.org/10.1007/s10586-019-02935-z.
39. Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii international conference on system sciences (HICSS)*. https://doi.org/10.1109/hicss.2016.714.
40. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials, 17*(3), 1294–1312. https://doi.org/10.1109/comst.2015.2388550.
41. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE*

Communications Surveys & Tutorials, 17(4), 2347–2376. https://doi.org/10.1109/comst.2015.2444095.
42. Siddiqui, F., Beley, J., Zeadally, S., & Braught, G. (2019). Secure and lightweight communication in heterogeneous IoT environments. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100093.
43. Hofer-Schmitz, K., & Stojanović, B. (2020). Towards formal verification of IoT protocols: A review. *Computer Networks, 174,* 107233. https://doi.org/10.1016/j.comnet.2020.107233.
44. Bhushan, B., & Sahoo, G. (2020). Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective. *Handbook of Computer Networks and Cyber Security*. https://doi.org/10.1007/978-3-030-22277-2_27.
45. Hamamreh, J. M., Furqan, H. M., & Arslan, H. (2019). Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 1773–1828. https://doi.org/10.1109/comst.2018.2878035.
46. Pecorella, T., Brilli, L., & Mucchi, L. (2016). The role of physical layer security in IoT: A novel perspective. *Information, 7*(3), 49. https://doi.org/10.3390/info7030049.
47. Kumar, A., Zhao, M., Wong, K., Guan, Y. L., & Chong, P. H. (2018). A comprehensive study of IoT and WSN MAC protocols: Research issues, challenges and opportunities. *IEEE Access, 6,* 76228–76262. https://doi.org/10.1109/access.2018.2883391.
48. Bakshi, A., Chen, L., Srinivasan, K., Koksal, C. E., & Eryilmaz, A. (2019). EMIT: An efficient MAC paradigm for the internet of things. *IEEE/ACM Transactions on Networking, 27*(4), 1572–1583. https://doi.org/10.1109/tnet.2019.2928002.
49. Cao, X., Song, Z., Yang, B., Elmossallamy, M. A., Qian, L., & Han, Z. (2020). A distributed ambient backscatter mac protocol for internet-of-things networks. *IEEE Internet of Things Journal, 7*(2), 1488–1501. https://doi.org/10.1109/jiot.2019.2955909.
50. Sun, X., & Ansari, N. (2018). Dynamic resource caching in the IoT application layer for smart cities. *IEEE Internet of Things Journal, 5*(2), 606–613. https://doi.org/10.1109/jiot.2017.2764418.
51. Perez, S., Hernandez-Ramos, J. L., Raza, S., & Skarmeta, A. (2020). Application layer key establishment for end-to-end security in IoT. *IEEE Internet of Things Journal, 7*(3), 2117–2128. https://doi.org/10.1109/jiot.2019.2959428.
52. Niu, R., & Varshney, P. K. (2008). Performance analysis of distributed detection in a random sensor field. *IEEE Transactions on Signal Processing, 56*(1), 339–349. https://doi.org/10.1109/tsp.2007.906770.
53. Ciuonzo, D., & Rossi, P. S. (2017). Distributed detection of a non-cooperative target via generalized locally-optimum approaches. *Information Fusion, 36,* 261–274. https://doi.org/10.1016/j.inffus.2016.12.006.
54. Dehkordi, S. A., Farajzadeh, K., Rezazadeh, J., Farahbakhsh, R., Sandrasegaran, K., & Dehkordi, M. A. (2019). A survey on data aggregation techniques in IoT sensor networks. *Wireless Networks, 26*(2), 1243–1263. https://doi.org/10.1007/s11276-019-02142-z.
55. Lau, B. P., Marakkalage, S. H., Zhou, Y., Hassan, N. U., Yuen, C., Zhang, M., et al. (2019). A survey of data fusion in smart city applications. *Information Fusion, 52,* 357–374. https://doi.org/10.1016/j.inffus.2019.05.004.
56. Ciuonzo, D., & Rossi, P. S. (2019). Data fusion in wireless sensor networks: A statistical signal processing perspective. *The Institution of Engineering and Technology (IET)*. https://doi.org/10.1049/pbce117e.
57. Al-Jarrah, M. A., Yaseen, M. A., Al-Dweik, A., Dobre, O. A., & Alsusa, E. (2020). Decision fusion for IoT-based wireless sensor networks. *IEEE Internet of Things Journal, 7*(2), 1313–1326. https://doi.org/10.1109/jiot.2019.2954720.
58. Ciuonzo, D., & Rossi, P. S. (2014). Decision fusion with unknown sensor detection probability. *IEEE Signal Processing Letters, 21*(2), 208–212. https://doi.org/10.1109/lsp.2013.2295054.
59. Ciuonzo, D., Rossi, P. S., & Dey, S. (2014). Massive MIMO meets decision fusion: Decode-and-fuse vs. decode-then-fuse. In *2014 IEEE 8th sensor array and multichannel signal processing workshop (SAM)*. https://doi.org/10.1109/sam.2014.6882391.
60. Zhu, R., Zhang, X., Liu, X., Shu, W., Mao, T., & Jalaian, B. (2015). ERDT: Energy-efficient reliable decision transmission for intelligent cooperative spectrum sensing in industrial IoT. *IEEE Access, 3,* 2366–2378. https://doi.org/10.1109/access.2015.2501644.
61. Zhang, Y., Liu, Y., Zhang, Z., & Zhao, N. (2018). Collaborative fusion for distributed target classification using evidence theory in IOT environment. *IEEE Access, 6,* 62314–62323. https://doi.org/10.1109/access.2018.2876282.
62. Mohammad, F. R., Ciuonzo, D., & Mohammed, Z. A. (2018). Mean-based blind hard decision fusion rules. *IEEE Signal Processing Letters, 25*(5), 630–634. https://doi.org/10.1109/lsp.2018.2809859.
63. Bletsas, A., Siachalou, S., & Sahalos, J. (2009). Anti-collision backscatter sensor networks. *IEEE Transactions on Wireless Communications, 8*(10), 5018–5029. https://doi.org/10.1109/twc.2009.080834.
64. Ciuonzo, D., Gelli, G., Pescape, A., & Verde, F. (2019). Decision fusion rules in ambient backscatter wireless sensor networks. In *2019 IEEE 30th annual international symposium on personal, indoor and mobile radio communications (PIMRC)*. https://doi.org/10.1109/pimrc.2019.8904358.
65. Yeh, T., Wu, C., & Tseng, Y. (2011). Improvement of the RFID authentication scheme based on quadratic residues. *Computer Communications, 34*(3), 337–341. https://doi.org/10.1016/j.comcom.2010.05.011.
66. Yang, C., Wang, X., & Chin, K. (2020). On max–min throughput in backscatter-assisted wirelessly powered IoT. *IEEE Internet of Things Journal, 7*(1), 137–147. https://doi.org/10.1109/jiot.2019.2947399.
67. Ciuonzo, D., Romano, G., & Rossi, P. S. (2013). Optimality of received energy in decision fusion over rayleigh fading diversity MAC with non-identical sensors. *IEEE Transactions on Signal Processing, 61*(1), 22–27. https://doi.org/10.1109/tsp.2012.2223694.
68. Altinel, D., & Kurt, G. K. (2019). Modeling of multiple energy sources for hybrid energy harvesting IoT systems. *IEEE Internet of Things Journal, 6*(6), 10846–10854. https://doi.org/10.1109/jiot.2019.2942071.
69. Bhushan, B., & Sahoo, G. (2019). E^2 SR^2 E^2 SR^2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks. *Wireless Networks, 25*(5), 2697–2721. https://doi.org/10.1007/s11276-019-01988-7.
70. Zhao, W., Wang, G., Atapattu, S., Tellambura, C., & Guan, H. (2018). Outage analysis of ambient backscatter communication systems. *IEEE Communications Letters, 22*(8), 1736–1739. https://doi.org/10.1109/lcomm.2018.2842774.
71. Ma, Z., Feng, L., & Xu, F. (2019). Design and analysis of a distributed and demand-based backscatter MAC protocol for internet of things networks. *IEEE Internet of Things Journal, 6*(1), 1246–1256. https://doi.org/10.1109/jiot.2018.2869015.
72. Nguyen, T. D., Khan, J. Y., & Ngo, D. T. (2018). A distributed energy-harvesting-aware routing algorithm for heterogeneous IoT networks. *IEEE Transactions on Green Communications*

and Networking, 2(4), 1115–1127. https://doi.org/10.1109/tgcn.2018.2839593.
73. Khairy, S., Han, M., Cai, L. X., & Cheng, Y. (2019). Sustainable wireless IoT networks with RF energy charging over Wi-Fi (CoWiFi). *IEEE Internet of Things Journal, 6*(6), 10205–10218. https://doi.org/10.1109/jiot.2019.2936837.
74. Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in internet of things. *Future Generation Computer Systems, 100,* 144–164. https://doi.org/10.1016/j.future.2019.04.038.
75. Karkouch, A., Mousannif, H., Moatassime, H. A., & Noel, T. (2016). Data quality in internet of things: A state-of-the-art survey. *Journal of Network and Computer Applications, 73,* 57–81. https://doi.org/10.1016/j.jnca.2016.08.002.
76. Maffei, A., Srinivasan, S., Castillejo, P., Martinez, J. F., Iannelli, L., Bjerkan, E., et al. (2018). A semantic-middleware-supported receding horizon optimal power flow in energy grids. *IEEE Transactions on Industrial Informatics, 14*(1), 35–46. https://doi.org/10.1109/tii.2017.2655047.
77. Cruz, M. A., Rodrigues, J. J., Al-Muhtadi, J., Korotaev, V. V., & Albuquerque, V. H. (2018). A reference model for internet of things middleware. *IEEE Internet of Things Journal, 5*(2), 871–883. https://doi.org/10.1109/jiot.2018.2796561.
78. Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in internet of things frameworks: A systematic literature review. *Internet of Things, 6,* 100050. https://doi.org/10.1016/j.iot.2019.100050.
79. Miloslavskaya, N., & Tolstoy, A. (2018). Internet of things: Information security challenges and solutions. *Cluster Computing, 22*(1), 103–119. https://doi.org/10.1007/s10586-018-2823-6.
80. Zhao, R., Wang, L., Zhang, X., Zhang, Y., Wang, L., & Peng, H. (2018). A OneM2M-compliant stacked middleware promoting IoT research and development. *IEEE Access, 6,* 63546–63559. https://doi.org/10.1109/access.2018.2876197.
81. Rodriguez-Molina, J., & Kammen, D. M. (2018). Middleware architectures for the smart grid: A survey on the state-of-the-art, taxonomy and main open issues. *IEEE Communications Surveys & Tutorials, 20*(4), 2992–3033. https://doi.org/10.1109/comst.2018.2846284.
82. Al-Roubaiey, A. A., Sheltami, T. R., Mahmoud, A. S., & Salah, K. (2019). Reliable middleware for wireless sensor-actuator networks. *IEEE Access, 7,* 14099–14111. https://doi.org/10.1109/access.2019.2893623.
83. Alshinina, R. A., & Elleithy, K. M. (2018). A highly accurate deep learning based approach for developing wireless sensor network middleware. *IEEE Access, 6,* 29885–29898. https://doi.org/10.1109/access.2018.2844255.
84. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7.
85. Ibrahim, A., & Dalkılıc, G. (2017). Review of different classes of RFID authentication protocols. *Wireless Networks, 25*(3), 961–974. https://doi.org/10.1007/s11276-017-1638-3.
86. Luo, X., Yin, L., Li, C., Wang, C., Fang, F., Zhu, C., et al. (2020). A lightweight privacy-preserving communication protocol for heterogeneous IoT environment. *IEEE Access, 8,* 67192–67204. https://doi.org/10.1109/access.2020.2978525.
87. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal, 6*(5), 8182–8201. https://doi.org/10.1109/jiot.2019.2935189.
88. Gochhayat, S. P., Lal, C., Sharma, L., Sharma, D. P., Gupta, D., Saucedo, J. A. M., et al. (2019). Reliable and secure data transfer in IoT networks. *Wireless Networks*. https://doi.org/10.1007/s11276-019-02036-0.
89. Imran, M., Jabbar, S., Chilamkurti, N., & Rodrigues, J. J. (2019). Enabling technologies for social internet of things. *Future Generation Computer Systems, 92,* 715–717. https://doi.org/10.1016/j.future.2018.11.018.
90. Li, C., & Palanisamy, B. (2019). Privacy in internet of things: From principles to technologies. *IEEE Internet of Things Journal, 6*(1), 488–505. https://doi.org/10.1109/jiot.2018.2864168.
91. Rathee, G., Sandhu, R., Saini, H., Sivaram, M., & Dhasarathan, V. (2019). A trust computed framework for IoT devices and fog computing environment. *Wireless Networks*. https://doi.org/10.1007/s11276-019-02106-3.
92. Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE, 102*(8), 1283–1295. https://doi.org/10.1109/jproc.2014.2335155.
93. Liu, X., Wei, X., Guo, L., & Liu, Y. (2019). SecLight: A new and practical VLC eavesdropping-resilient framework for IoT devices. *IEEE Access, 7,* 19109–19124. https://doi.org/10.1109/access.2019.2897565.
94. Bhushan, B., & Sahoo, G. (2017). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications, 98*(2), 2037–2077. https://doi.org/10.1007/s11277-017-4962-0.
95. Bhushan, B., & Sahoo, G. (2017). A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks. In *2017 international conference on signal processing and communication (ICSPC)*. https://doi.org/10.1109/cspc.2017.8305856.
96. Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2016). Threats to networking cloud and edge data centers in the internet of things. *IEEE Cloud Computing, 3*(3), 64–71. https://doi.org/10.1109/mcc.2016.63.
97. Mishra, A. K., Tripathy, A. K., Puthal, D., & Yang, L. T. (2019). Analytical model for sybil attack phases in internet of things. *IEEE Internet of Things Journal, 6*(1), 379–387. https://doi.org/10.1109/jiot.2018.2843769.
98. Wu, J., Tseng, Y., Huang, S., & Tsai, T. (2019). Leakage-resilient certificate-based signature resistant to side-channel attacks. *IEEE Access, 7,* 19041–19053. https://doi.org/10.1109/access.2019.2896773.
99. Tseng, Y., Huang, S., Tsai, T., & Tseng, L. (2015). A novel ID-based authentication and key exchange protocol resistant to ephemeral-secret-leakage attacks for mobile devices. *International Journal of Distributed Sensor Networks, 11*(5), 898716. https://doi.org/10.1155/2015/898716.
100. Tseng, Y., Wu, J., Hung, R., & Chien, H. (2018). Leakage-resilient certificate-based encryption scheme for IoT environments. In *2018 9th international conference on awareness science and technology (iCAST)*. https://doi.org/10.1109/icawst.2018.8517196.
101. Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R., & Jin, Y. (2016). Security analysis on consumer and industrial IoT devices. In *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*. https://doi.org/10.1109/aspdac.2016.7428064.
102. Arias, O., Wurm, J., Hoang, K., & Jin, Y. (2015). Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems, 1*(2), 99–109. https://doi.org/10.1109/tmscs.2015.2498605.
103. Balamurugan, B., & Biswas, D. (2017). Security in network layer of IoT. *Security Breaches and Threat Prevention in the Internet of Things Advances in Information Security, Privacy, and Ethics*. https://doi.org/10.4018/978-1-5225-2296-6.ch003.

104. Jaitly, S., Malhotra, H., & Bhushan, B. (2017). Security vulnerabilities and countermeasures against jamming attacks in wireless sensor networks: A survey. In *2017 international conference on computer, communications and electronics (Comptelix)*. https://doi.org/10.1109/comptelix.2017.8004033.
105. Reddy, A. G., Yoon, E.-J., Das, A. K., Odelu, V., & Yoo, K.-Y. (2017). Design of mutually authenticated key agreement protocol resistant to impersonation attacks for multi-server environment. *IEEE Access, 5,* 3622–3639. https://doi.org/10.1109/access.2017.2666258.
106. Godoy, P. D., Cayssials, R. L., & Garino, C. G. G. (2018). Communication channel occupation and congestion in wireless sensor networks. *Computers & Electrical Engineering, 72,* 846–858. https://doi.org/10.1016/j.compeleceng.2017.12.049.
107. Nizzi, F., Pecorella, T., Esposito, F., Pierucci, L., & Fantacci, R. (2019). IoT security via address shuffling: The easy way. *IEEE Internet of Things Journal, 6*(2), 3764–3774. https://doi.org/10.1109/jiot.2019.2892003.
108. Yu, C.-M., Tsou, Y.-T., Lu, C.-S., & Kuo, S.-Y. (2013). Localized algorithms for detection of node replication attacks in mobile sensor networks. *IEEE Transactions on Information Forensics and Security, 8*(5), 754–768. https://doi.org/10.1109/tifs.2013.2255285.
109. Bhushan, B., Sahoo, G., & Rai, A. K. (2017). Man-in-the-middle attack in wireless and computer networking—A review. In *2017 3rd international conference on advances in computing, communication & automation (ICACCA) (fall)*. https://doi.org/10.1109/icaccaf.2017.8344724.
110. Bhushan, B., & Sahoo, G. (2017). Detection and defense mechanisms against wormhole attacks in wireless sensor networks. In *2017 3rd international conference on advances in computing, communication & automation (ICACCA) (fall)*. https://doi.org/10.1109/icaccaf.2017.8344730.
111. OWASP Top 10 2017—The Ten Most Critical Web Application Security Risks. (2017). [Online]. https://www.owasp.org/index.php/Category:OWASPTopTen2017Project.
112. SQLi, XSS zero-days expose Belkin IoT devices, Android smartphones. (2016). [Online]. https://www.csoonline.com/article/3138935/security/sqli-xsszero-days-expose-belkin-iot-devices-android-smartphones.html.
113. Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in the internet of things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications, 81,* 111–124. https://doi.org/10.1016/j.jnca.2016.08.007.
114. Zhao, F., Sun, Z., & Jin, H. (2015). Topic-centric and semantic-aware retrieval system for internet of things. *Information Fusion, 23,* 33–42. https://doi.org/10.1016/j.inffus.2014.01.001.
115. Brody, P., & Pureswaran, V. (2014). *Device democracy: Saving the future of the Internet of Things*. IBM Institute for Business Value, technical report, September 2014. [Online]. http://www935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/.
116. Benet, J. (2015). *Replication on IPFS—or, the backing-up content model*. [Online]. https://github.com/ipfs/faq/issues/47.
117. EtherAPIs: Decentralized, Anonymous, Trustless APIs, accessed on March 15, 2019. [Online]. https://etherapis.io/.
118. Filecoin—A cryptocurrency operated file storage network [Online]. http://filecoin.io/. Accessed on March 15, 2019.
119. Yassami, S., Drego, N., Sergeev, I., Julian, T., Harding, D., & Srinivasan, B. S. (2016). True micropayments with Bitcoin. [Online]. https://medium.com/@21/true-micropayments-with-bitcoine64fec23ffd8.
120. Slock.it—Blockchain + IoT [Online]. https://slock.it/faq.md. Accessed on March 15, 2019.
121. TransActive Grid [Online]. http://transactivegrid.net/. Accessed on March 15, 2016.
122. Rutkin, A. (2016). Blockchain-based microgrid gives power to consumers in New York [Online]. https://www.newscientist.com/article/2079334-blockchain-based-microgrid-gives-power-to-consumersin-new-york/.
123. Chang, S. E., & Chen, Y. (2020). When blockchain meets supply chain: A systematic literature review on current development and potential applications. *IEEE Access, 8,* 62478–62494. https://doi.org/10.1109/access.2020.2983601.
124. Vaio, A. D., & Varriale, L. (2020). Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *International Journal of Information Management, 52,* 102014. https://doi.org/10.1016/j.ijinfomgt.2019.09.010.
125. Jang, H., & Lee, J. (2018). An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information. *IEEE Access, 6,* 5427–5437. https://doi.org/10.1109/access.2017.2779181.
126. Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—How to make bitcoin a better currency. *Financial Cryptography and Data Security Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-642-32946-3_29.
127. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.020.
128. Roy, D. G., Das, P., De, D., & Buyya, R. (2019). QoS-aware secure transaction framework for internet of things using blockchain mechanism. *Journal of Network and Computer Applications, 144,* 59–78. https://doi.org/10.1016/j.jnca.2019.06.014.
129. Li, D., Cai, Z., Deng, L., Yao, X., & Wang, H. H. (2018). Information security model of block chain based on intrusion sensing in the IoT environment. *Cluster Computing*. https://doi.org/10.1007/s10586-018-2516-1.
130. Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems, 97,* 512–529. https://doi.org/10.1016/j.future.2019.02.060.
131. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications, 126,* 45–58. https://doi.org/10.1016/j.jnca.2018.10.020.
132. Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. *Journal of Network and Computer Applications, 127,* 43–58. https://doi.org/10.1016/j.jnca.2018.11.003.
133. Gupta, S., Sinha, S., & Bhushan, B. (2020). Emergence of blockchain technology: Fundamentals, working and its various implementations. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3569577.
134. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49*(11), 2266–2277. https://doi.org/10.1109/tsmc.2019.2895123.
135. Soni, S., & Bhushan, B. (2019). A comprehensive survey on blockchain: Working, security analysis, privacy threats and potential applications. In *2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT)*. https://doi.org/10.1109/icicict46008.2019.8993210.
136. Liu, J., Li, W., Karame, G. O., & Asokan, N. (2018). Toward fairness of cryptocurrency payments. *IEEE Security and Privacy, 16*(3), 81–89. https://doi.org/10.1109/msp.2018.2701163.

137. Wang, X., Xu, X., Feagan, L., Huang, S., Jiao, L., & Zhao, W. (2018). Inter-bank payment system on enterprise blockchain platform. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*. https://doi.org/10.1109/cloud.2018.00085.
138. Wei, P., Zhang, M., Jiang, W., & Nie, D. (2016). A new model for sand-ripple scattering based on SSA method and practical ripple profiles. *IEEE Transactions on Geoscience and Remote Sensing, 54*(4), 2450–2459. https://doi.org/10.1109/tgrs.2015.2501400.
139. Sarfraz, U., Alam, M., Zeadally, S., & Khan, A. (2019). Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions. *Computer Networks, 148,* 361–372. https://doi.org/10.1016/j.comnet.2018.11.019.
140. Khan, M. Y., Zuhairi, M. F., Ali, T., Alghamdi, T., & Marmolejo-Saucedo, J. A. (2019). An extended access control model for permissioned blockchain frameworks. *Wireless Networks*. https://doi.org/10.1007/s11276-019-01968-x.
141. The-Linux-Foundation, Hyperledger business blockchain technologies (2019). https://www.hyperledger.org/projects. Last Accessed June 12, 2019.
142. Buterin, V., et al., A next-generation smart contract and decentralized application platform, white paper.
143. Nizamuddin, N., Salah, K., Azad, M. A., Arshad, J., & Rehman, M. (2019). Decentralized document version control using ethereum blockchain and IPFS. *Computers & Electrical Engineering, 76,* 183–197. https://doi.org/10.1016/j.compeleceng.2019.03.014.
144. Gozgor, G., Tiwari, A. K., Demir, E., & Akron, S. (2019). The relationship between Bitcoin returns and trade policy uncertainty. *Finance Research Letters, 29,* 75–82. https://doi.org/10.1016/j.frl.2019.03.016.
145. Alshamsi, A., & Andras, P. P. (2019). User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies, 126,* 94–110. https://doi.org/10.1016/j.ijhcs.2019.02.004.
146. Hasan, H. R., & Salah, K. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access, 7,* 41596–41606. https://doi.org/10.1109/access.2019.2905689.
147. Karame, G. O., Androulaki, E., & Capkun, S. (2012). Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM conference on computer and communications security—CCS 12*. https://doi.org/10.1145/2382196.2382292.
148. Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. cryptography mailing list. https://metzdowd.com.
149. Tsai, T., Tseng, Y., Hung, Y., & Huang, S. (2016). Cryptanalysis and improvement of a provable data possession scheme in public cloud storage. In: *2016 third international conference on computing measurement control and sensor network (CMCSN)*. https://doi.org/10.1109/cmcsn.2016.18.
150. Wu, T., Tseng, Y., Huang, S., & Lai, Y. (2017). Non-repudiable provable data possession scheme with designated verifier in cloud storage systems. *IEEE Access, 5,* 19333–19341. https://doi.org/10.1109/access.2017.2753243.
151. Imran, M., Durad, M. H., Khan, F. A., & Derhab, A. (2019). Toward an optimal solution against Denial of Service attacks in Software Defined Networks. *Future Generation Computer Systems, 92,* 444–453. https://doi.org/10.1016/j.future.2018.09.022.
152. Yu, T., Wang, X., & Shami, A. (2017). Recursive principal component analysis-based data outlier detection and sensor data aggregation in IoT systems. *IEEE Internet of Things Journal, 4*(6), 2207–2216. https://doi.org/10.1109/jiot.2017.2756025.
153. Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access, 4,* 2840–2853. https://doi.org/10.1109/access.2016.2575863.
154. Li, X., Wang, H., Dai, H.-N., Wang, Y., & Zhao, Q. (2016). An analytical study on eavesdropping attacks in wireless nets of things. *Mobile Information Systems, 2016,* 1–10. https://doi.org/10.1155/2016/4313475.
155. Liao, C., Bao, S., Cheng, C., & Chen, K. (2017). On design issues and architectural styles for blockchain-driven IoT services. In *2017 IEEE international conference on consumer electronics—Taiwan (ICCE-TW)*. https://doi.org/10.1109/icce-china.2017.7991140.
156. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized block chain for IoT. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation - IoTDI*. https://doi.org/10.1145/3054977.3055003.
157. Daza, V., Pietro, R. D., Klimek, I., & Signorini, M. (2017). CONNECT: CONtextual NamE disCovery for blockchain-based services in the IoT. In *2017 IEEE international conference on communications (ICC)*. https://doi.org/10.1109/icc.2017.7996641.
158. Li, C., & Zhang, L. (2017). A blockchain based new secure multi-layer network model for internet of things. In *2017 IEEE international congress on internet of things (ICIOT)*. https://doi.org/10.1109/ieee.iciot.2017.34.
159. Samaniego, M., & Deters, R. (2016). Blockchain as a service for IoT. In *2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*. https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.102.
160. Stanciu, A. (2017). Blockchain based distributed control system for edge computing. In *2017 21st international conference on control systems and computer science (CSCS)*. https://doi.org/10.1109/cscs.2017.102.
161. Sharma, P. K., Chen, M., & Park, J. H. (2018). A software defined fog node based distributed blockchain cloud architecture for IoT. *IEEE Access, 6,* 115–124. https://doi.org/10.1109/access.2017.2757955.
162. Correia, M., Veronese, G. S., Neves, N. F., & Verissimo, P. (2011). Byzantine consensus in asynchronous message-passing systems: A survey. *International Journal of Critical Computer-Based Systems, 2*(2), 141. https://doi.org/10.1504/ijccbs.2011.041257.
163. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/mc.2017.201.
164. Macaulay, T. (2017). Availability and reliability requirements in the IoT. *RIoT Control*. https://doi.org/10.1016/b978-0-12-419971-2.00008-x.
165. Macaulay, T. (2017). Confidentiality and integrity and privacy requirements in the iot. *RIoT Control*. https://doi.org/10.1016/b978-0-12-419971-2.00007-8.
166. Wu, J., Song, T., Yu, Y., Wang, C., & Hu, J. (2018). Generalized byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks. *IEEE Access, 6,* 53272–53286. https://doi.org/10.1109/access.2018.2866485.
167. Wan, S., Li, M., Liu, G., & Wang, C. (2019). Recent advances in consensus protocols for blockchain: A survey. *Wireless Networks*. https://doi.org/10.1007/s11276-019-02195-0.
168. Axon, L., & Goldsmith, M. (2017). PB-PKI: A privacy-aware blockchain-based PKI. In *Proceedings of the 14th international joint conference on E-business and telecommunications*. https://doi.org/10.5220/0006419203110318.
169. Hashemi, S. H., Faghri, F., Rausch, P., & Campbell, R. H. (2016). World of Empowered IoT Users. In *2016 IEEE first international conference on internet-of-things design and implementation (IoTDI)*. https://doi.org/10.1109/iotdi.2015.39.

170. Zhang, Y., & Wen, J. (2016). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications, 10*(4), 983–994. https://doi.org/10.1007/s12083-016-0456-1.
171. Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2016). FairAccess: A new Blockchain-based access control framework for the internet of things. *Security and Communication Networks, 9*(18), 5943–5964. https://doi.org/10.1002/sec.1748.
172. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal, 5*(2), 1184–1195. https://doi.org/10.1109/jiot.2018.2812239.
173. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. https://doi.org/10.1109/percomw.2017.7917634.
174. Ali, M. S., Dolui, K., & Antonelli, F. (2017). IoT data privacy via blockchains and IPFS. *Proceedings of the Seventh International Conference on the Internet of Things - IoT*. https://doi.org/10.1145/3131542.3131563.
175. Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017). Towards blockchain-based auditable storage and sharing of IoT Data. In *Proceedings of the 2017 on cloud computing security workshop—CCSW 17*. https://doi.org/10.1145/3140649.3140656.
176. Biswas, K., & Muthukkumarasamy, V. (2016). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications.* https://doi.org/10.1109/hpcc-smartcity-dss.2016.0198.
177. Kang, J., Yu, R., Huang, X., & Zhang, Y. (2018). Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems, 19*(8), 2627–2637. https://doi.org/10.1109/tits.2017.2764095.
178. Yang, Z., Zheng, K., Yang, K., & Leung, V. C. (2017). A blockchain-based reputation system for data credibility assessment in vehicular networks. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. https://doi.org/10.1109/pimrc.2017.8292724.
179. Lee, B., & Lee, J. (2016). Blockchain-based secure firmware update for embedded devices in an internet of things environment. *The Journal of Supercomputing, 73*(3), 1152–1167. https://doi.org/10.1007/s11227-016-1870-0.
180. Steger, M., Dorri, A., Kanhere, S. S., Römer, K., Jurdak, R., & Karner, M. (2017). Secure wireless automotive software updates using blockchains: A proof of concept. *Advanced Microsystems for Automotive Applications 2017 Lecture Notes in Mobility, 1,* 137–149. https://doi.org/10.1007/978-3-319-66972-4_12.
181. Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., Quesnel, F., Roger, A., & Sirdey, R. (2017). Towards better availability and accountability for IoT updates by means of a blockchain. In *2017 IEEE European symposium on security and privacy workshops (EuroS&PW)*. https://doi.org/10.1109/eurospw.2017.50.
182. Alphand, O., Amoretti, M., Claeys, T., Dallasta, S., Duda, A., Ferrari, G., et al. (2018). IoTChain: A blockchain security architecture for the internet of things. In *2018 IEEE wireless communications and networking conference (WCNC)*. https://doi.org/10.1109/wcnc.2018.8377385.
183. Chakraborty, R. B., Pandey, M., & Rautaray, S. S. (2018). Managing computation load on a blockchain—Based multi-Layered internet-of-things network. *Procedia Computer Science, 132,* 469–476. https://doi.org/10.1016/j.procs.2018.05.146.
184. Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications, 09*(10), 533–546. https://doi.org/10.4236/jsea.2016.910036.
185. Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing, 15*(5), 840–852. https://doi.org/10.1109/tdsc.2016.2616861.
186. Cha, S., Chen, J., Su, C., & Yeh, K. (2018). A blockchain connected gateway for BLE-based devices in the internet of things. *IEEE Access, 6,* 24639–24649. https://doi.org/10.1109/access.2018.2799942.
187. Swanson, T., Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger system. http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.
188. Zhang, Y., & Wen, J. (2015). An IoT electric business model based on the protocol of bitcoin. In *2015 18th international conference on intelligence in next generation networks*. https://doi.org/10.1109/icin.2015.7073830.
189. Wright, A., & Filippi, P. D. (2015). Decentralized blockchain technology and the rise of lex cryptographia. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2580664.
190. Tanas, C., Delgado-Segura, S., & Herrera-Joancomartí, J. (2016). An integrated reward and reputation mechanism for MCS preserving users' privacy. *Lecture Notes in Computer Science Data Privacy Management, and Security Assurance*. https://doi.org/10.1007/978-3-319-29883-2_6.
191. Siddiqi, M., All, S. T., & Sivaraman, V. (2017). Secure lightweight context-driven data logging for bodyworn sensing devices. In *2017 5th international symposium on digital forensic and security (ISDFS)*. https://doi.org/10.1109/isdfs.2017.7916500.
192. Gipp, B., Meuschke, N., Gernandt, A. (2015). Decentralized trusted timestamping using the crypto currency bitcoin. In *Proceedings of the iconference, newport beach, United States*, 24–27 March 2015.
193. Wilson, D., & Ateniese, G. (2015). From pretty good to great: Enhancing PGP using bitcoin and the blockchain. *Network and System Security Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-319-25645-0_25.
194. Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal, 4*(6), 1832–1843. https://doi.org/10.1109/jiot.2017.2740569.
195. Mcghin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135,* 62–75. https://doi.org/10.1016/j.jnca.2019.02.027.
196. Aggarwal, S., Chaudhary, R., Aujla, G. S., Kumar, N., Choo, K.-K. R., & Zomaya, A. Y. (2019). Blockchain for smart communities: Applications, challenges and opportunities. *Journal of Network and Computer Applications, 144,* 13–48. https://doi.org/10.1016/j.jnca.2019.06.018.
197. Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)*. https://doi.org/10.1109/icsssm.2016.7538424.
198. Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*. https://doi.org/10.23919/icact.2017.7890132.

199. Blanco-Novoa, Ó., Fernández-Caramés, T., Fraga-Lamas, P., & Castedo, L. (2017). An electricity price-aware open-source smart socket for the internet of energy. *Sensors, 17*(3), 643. https://doi.org/10.3390/s17030643.
200. Almusaylim, Z. A., & Zaman, N. (2018). A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). *Wireless Networks, 25*(6), 3193–3204. https://doi.org/10.1007/s11276-018-1712-5.
201. Lundqvist, T., Blanche, A. D., & Andersson, H. R. (2017). Thing-to-thing electricity micro payments using blockchain technology. In *2017 global internet of things summit (GIoTS)*. https://doi.org/10.1109/giots.2017.8016254.
202. Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)*. https://doi.org/10.23919/inm.2017.7987376.
203. Shae, Z., & Tsai, J. J. (2017). On the design of a blockchain platform for clinical trial and precision medicine. In *2017 IEEE 37th international conference on distributed computing systems (ICDCS)*. https://doi.org/10.1109/icdcs.2017.61.
204. Salahuddin, M. A., Al-Fuqaha, A., Guizani, M., Shuaib, K., & Sallabi, F. (2017). Softwarization of internet of things infrastructure for secure and smart healthcare. *Computer, 50*(7), 74–79. https://doi.org/10.1109/mc.2017.195.
205. Dolui, K., & Datta, S. K. (2017). Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In *2017 global internet of things summit (GIoTS)*. https://doi.org/10.1109/giots.2017.8016213.
206. Park, J., & Kim, K. (2017). TM-Coin: Trustworthy management of TCB measurements in IoT. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom Workshops)*. https://doi.org/10.1109/percomw.2017.7917640.
207. Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)*. https://doi.org/10.1109/temscon.2017.7998367.
208. Andersen, M. P., Fierro, G., & Culler, D. E. (2017). Enabling synergy in IoT: Platform to service and beyond. *Journal of Network and Computer Applications, 81,* 96–110. https://doi.org/10.1016/j.jnca.2016.10.017.
209. Yang, S., Yin, D., Song, X., Dong, X., Manogaran, G., Mastorakis, G., et al. (2019). Security situation assessment for massive MIMO systems for 5G communications. *Future Generation Computer Systems, 98,* 25–34. https://doi.org/10.1016/j.future.2019.03.036.
210. Tello-Oquendo, L., Lin, S., Akyildiz, I. F., & Pla, V. (2019). Software-defined architecture for QoS-aware IoT deployments in 5G systems. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2019.101911.
211. Ellis, R. D., Flaherty-Walia, K. E., Collins, A. B., Bickford, J. W., Boucek, R., Burnsed, S. L., et al. (2019). Acoustic telemetry array evolution: From species- and project-specific designs to large-scale, multispecies, cooperative networks. *Fisheries Research, 209,* 186–195. https://doi.org/10.1016/j.fishres.2018.09.015.
212. Lee, C., Chen, S., Li, C., Cheng, C., & Lai, Y. (2019). Security enhancement on an RFID ownership transfer protocol based on cloud. *Future Generation Computer Systems, 93,* 266–277. https://doi.org/10.1016/j.future.2018.10.040.
213. Chejerla, B. K., & Madria, S. (2019). Information fusion architecture for secure cyber physical systems. *Computers & Security, 85,* 122–137. https://doi.org/10.1016/j.cose.2019.04.006.
214. Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I., & Benedetto, M. D. (2019). State of the art of cyber-physical systems security: An automatic control perspective. *Journal of Systems and Software, 149,* 174–216. https://doi.org/10.1016/j.jss.2018.12.006.
215. Zhou, Z., Xie, M., Zhu, T., Xu, W., Yi, P., Huang, Z., et al. (2014). EEP2P: An energy-efficient and economy-efficient P2P network protocol. *International Green Computing Conference*. https://doi.org/10.1109/igcc.2014.7039171.
216. Liao, C., Cheng, S., & Domb, M. (2017). On designing energy efficient Wi-Fi P2P connections for internet of things. In *2017 IEEE 85th vehicular technology conference (VTC Spring)*. https://doi.org/10.1109/vtcspring.2017.8108292.
217. Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. *Computer, 44*(4), 91–93. https://doi.org/10.1109/mc.2011.115.
218. Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In *2017 IEEE international conference on web services (ICWS)*. https://doi.org/10.1109/icws.2017.54.
219. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., Mccoy, D., Voelker, G. M., et al. (2016). A fistful of bitcoins. *Communications of the ACM, 59*(4), 86–93. https://doi.org/10.1145/2896384.
220. Kravitz, D. W., & Cooper, J. (2017). Securing user identity and transactions symbiotically: IoT meets blockchain. In *2017 global internet of things summit (GIoTS)*. https://doi.org/10.1109/giots.2017.8016280.
221. Hayouni, H., & Hamdi, M. (2016). Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues. In *2016 IEEE 13th international conference on networking, sensing, and control (ICNSC)*. https://doi.org/10.1109/icnsc.2016.7479039.
222. Courtois, N. T., Emirdag, P., & Nagy, D. A. (2014). Could bitcoin transactions be 100x faster? In *Proceedings of the 11th international conference on security and cryptography*. https://doi.org/10.5220/0005102804260431.
223. Zhong, L., Wu, Q., Xie, J., Guan, Z., & Qin, B. (2019). A secure large-scale instant payment system based on blockchain. *Computers & Security, 84,* 349–364. https://doi.org/10.1016/j.cose.2019.04.007.
224. Lu, Q., Xu, X., Liu, Y., Weber, I., Zhu, L., & Zhang, W. (2019). UBaaS: A unified blockchain as a service platform. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2019.05.051.
225. Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). MOF-BC: A memory optimized and flexible blockchain for large scale networks. *Future Generation Computer Systems, 92,* 357–373. https://doi.org/10.1016/j.future.2018.10.002.
226. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., & Imran, M. (2019). Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems, 100,* 325–343. https://doi.org/10.1016/j.future.2019.05.023.
227. Turk, Ž., & Klinc, R. (2017). Potentials of blockchain technology for construction management. *Procedia Engineering, 196,* 638–645. https://doi.org/10.1016/j.proeng.2017.08.052.
228. Elazhary, H. (2019). Internet of things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. *Journal of Network and Computer Applications, 128,* 105–140. https://doi.org/10.1016/j.jnca.2018.10.021.
229. Cruz, M. A., Rodrigues, J. J., Lorenz, P., Solic, P., Al-Muhtadi, J., & Albuquerque, V. H. (2019). A proposal for bridging application layer protocols to HTTP on IoT solutions. *Future Generation Computer Systems, 97,* 145–152. https://doi.org/10.1016/j.future.2019.02.009.

230. Herrera-Joancomartí, J. (2015). Research and challenges on bitcoin anonymity. *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-319-17016-9_1.
231. Biryukov, A., Khovratovich, D., & Pustogarov, I. (2014). Deanonymisation of clients in bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security—CCS 14*. https://doi.org/10.1145/2660267.2660379.
232. Feld, S., Schönfeld, M., & Werner, M. (2014). Analyzing the deployment of bitcoins P2P network under an AS-level perspective. *Procedia Computer Science, 32,* 1121–1126. https://doi.org/10.1016/j.procs.2014.05.542.
233. Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications, 149,* 102481. https://doi.org/10.1016/j.jnca.2019.102481.
234. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science, 349*(6245), 255–260. https://doi.org/10.1126/science.aaa8415.
235. Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of internet of things (IoT): A survey. *Journal of Network and Computer Applications, 161,* 102630. https://doi.org/10.1016/j.jnca.2020.102630.
236. Shen, M., Tang, X., Zhu, L., Du, X., & Guizani, M. (2019). Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities. *IEEE Internet of Things Journal, 6*(5), 7702–7712. https://doi.org/10.1109/jiot.2019.2901840.
237. Roldán, J., Boubeta-Puig, J., Martínez, J. L., & Ortiz, G. (2020). Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. *Expert Systems with Applications, 149,* 113251. https://doi.org/10.1016/j.eswa.2020.113251.
238. Nweke, H. F., Teh, Y. W., Al-Garadi, M. A., & Alo, U. R. (2018). Deep learning algorithms for human activity recognition using mobile and wearable sensor networks: State of the art and research challenges. *Expert Systems with Applications, 105,* 233–261. https://doi.org/10.1016/j.eswa.2018.03.056.
239. Singh, S. K., Jeong, Y., & Park, J. H. (2020). A deep learning-based IoT-oriented infrastructure for secure smart city. *Sustainable Cities and Society*. https://doi.org/10.1016/j.scs.2020.102252.
240. Ren, Z., Wu, H., Ning, Q., Hussain, I., & Chen, B. (2020). End-to-end malware detection for android IoT devices using deep learning. *Ad Hoc Networks, 101,* 102098. https://doi.org/10.1016/j.adhoc.2020.102098.
241. Aceto, G., Ciuonzo, D., Montieri, A., & Pescape, A. (2019). Mobile encrypted traffic classification using deep learning: Experimental evaluation, lessons learned, and challenges. *IEEE Transactions on Network and Service Management, 16*(2), 445–458. https://doi.org/10.1109/tnsm.2019.2899085.
242. Aceto, G., Ciuonzo, D., Montieri, A., Persico, V., & Pescape, A. (2019). Know your big data trade-offs when classifying encrypted mobile traffic with deep learning. In *2019 network traffic measurement and analysis conference (TMA)*. https://doi.org/10.23919/tma.2019.8784565.
243. Sezer, O. B., Dogdu, E., & Ozbayoglu, A. M. (2018). Context-aware computing, learning, and big data in internet of things: A survey. *IEEE Internet of Things Journal, 5*(1), 1–27. https://doi.org/10.1109/jiot.2017.2773600.
244. Guo, L., Dong, M., Ota, K., Li, Q., Ye, T., Wu, J., et al. (2017). A secure mechanism for big data collection in large scale internet of vehicle. *IEEE Internet of Things Journal, 4*(2), 601–610. https://doi.org/10.1109/jiot.2017.2686451.
245. Chui, K. T., Liu, R. W., Lytras, M. D., & Zhao, M. (2019). Big data and IoT solution for patient behaviour monitoring. *Behaviour & Information Technology, 38*(9), 940–949. https://doi.org/10.1080/0144929x.2019.1584245.
246. Zhou, H., Sun, G., Fu, S., Liu, J., Zhou, X., & Zhou, J. (2019). A big data mining approach of PSO-based BP neural network for financial risk management with IoT. *IEEE Access, 7,* 154035–154043. https://doi.org/10.1109/access.2019.2948949.
247. Tsai, C., Lai, C., Chao, H., & Vasilakos, A. V. (2015). Big data analytics: A survey. *Journal of Big Data, 2*(1), 1. https://doi.org/10.1186/s40537-015-0030-3.

Bharat Bhushan received the B.Tech. degree in computer science and engineering from SHIATS, Allahabad, India in 2012, and the M.Tech. degree in information security from Birla Institute of Technology, Mesra, Jharkhand, India in 2015, and is currently working toward the Ph.D. degree at Birla Institute of Technology, Mesra, Jharkhand, India. From 2012 through 2013, he worked as a network engineer at HCL Infosystems Ltd., Noida, India. He is IEEE student member. He has published more than 50 scientific research publications in reputed International Journals and Conferences including SCI Indexed journal publications such as Wireless Personal communication and Wireless Networks. His research interests include the security and attacks in wireless sensor networks, security in networking systems, Internet of Things and Blockchain.

Chinmayee Sahoo received the B.Tech. degree in computer science from GMR Institute of Technology, Andhra Pradesh, India in 2014 and the M.Tech. degree in information security from Birla Institute of Technology, Mesra, Jharkhand, India in 2018. Her research interests include the Machine Learning, Internet of Things and Blockchain.

Preeti Sinha received the B.Tech. degree in computer science and engineering from SHIATS, Allahabad, India in 2016, and the M.Tech. degree in information security from Birla Institute of Technology, Mesra, Jharkhand, India in 2018. From 2017 through 2018, she worked as a software engineer at NVIDIA, Hyderabad, India. Her research interests include the security and attacks in Cyber Physical Systems, Internet of Things and Blockchain.

Aditya Khamparia is an eminent academician; plays versatile roles and responsibilities juggling between lectures, research, publications, consultancy, community service and PhD supervision etc. With Seven years of rich expertise in teaching and two years in industry; he focuses on rational and practical learning. Currently, He is working as Associate Professor of Computer Science and Engineering at Lovely Professional University, Punjab, India. His research area is Machine Learning, Soft Computing, Educational Technologies, IoT, Semantic Web and Ontologies. He has published more than 50 scientific research publications in reputed International/National Journals and Conferences, which are indexed in various international databases. Invited as a Faculty Resource Person/Session Chair/Reviewer/TPC member in different FDP, conferences and journals. He is member of CSI, IET, ISTE, IAENG, ACM and IACSIT. He is also acting as reviewer and member of various renowned national and international conferences/journals.