Wireless Personal Communications (2022) 123:3661–3697
https://doi.org/10.1007/s11277-021-09308-z

Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective

B. Nagajayanthi[1]

Accepted: 20 October 2021 / Published online: 18 November 2021

Abstract
Internet connects people to people, people to machine, and machine to machine for a life of serendipity through a Cloud. Internet of Things networks objects or people and integrates them with software to collect and exchange data. The Internet of things (IoT) influences our lives based on how we ruminate, respond, and anticipate. IoT 2021 heralds from the fringes to the data ecosystem and panaches a comfort zone. IoT is overwhelmingly embraced by businessmen and consumers due to increased productivity and convenience. Internet of Things facilitates intelligent device control with cloud vendors like Amazon and Google using artificial intelligence for data analytics, and with digital assistants like Alexa and Siri providing a voice user interface. Smart IoT is all about duplex connecting, processing, and implementing. Centralized IoT architecture is vulnerable to cyber-attacks. With Block Chain, it is possible to maintain transparency and security of the transaction's data. Robotic Process Automation (RPA) using bots has automated laborious tasks in 2019. Embedded Internet using Facial Recognition could reduce the coronavirus pandemic crisis by making a paradigm shift from fingerprint sensors to facial recognition. Security concerns are addressed with micro-segmentation approaches. IoT, an incredible vision of the future makes systems adaptive with customized features, responsive with increased efficiency, and procurable with optimized cost. This research delivers a comprehensive insight into the technical perspectives of IoT, focusing on interoperability, flexibility, scalability, mobility, security, transparency, standardization, and low energy. A smart classroom is implemented based on the concepts of IoT.

Keywords Internet-of-things · IPv6 · Standardization · Cyber-security · Low-energy

1 Introduction

Billions of things [155] are integrated over the Internet and are embedded with software to communicate seamlessly. Standardization of IoT devices is achievable with limited vendors based on Platform, Connectivity [45], and Application. Initially Kevin Ashton [1] proposed IoT. Then later on, the Internet of Things (IoT) rooted in Massachusetts of Technology

✉ B. Nagajayanthi
nagajayanthi.b@vit.ac.in

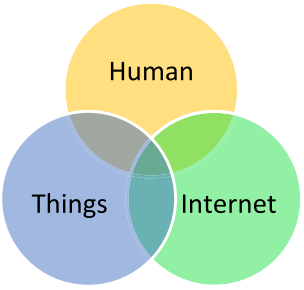
[1] Vellore Institute of Technology, Chennai Campus, Chennai, Tamil Nadu 600127, India

(MIT) and evolved around 2009 [60]. With IoT, homes become smarter [23] and smart cars [204] make our commute easier and safer. For smart homes to be customized, they need to be secured [255]. IoT visualizes distributed data networks with bilateral communication. In the first pre-internet phase, communication was through the telephone line and short message service (SMS). In the second phase, mobile and E-Mail took over in the Internet of content phase where information in the form of texts and images were exchanged. In the third Internet of Services phase, E-Commerce plunged in. In the fourth Internet of People phase, people communicated through social media such as Facebook, Skype, etc., In the enduring Era, devices connected and communicated through the Internet.Lately, interconnected devices [25] perform without human intervention based on Artificial Intelligence integration as depicted in Fig. 1.

With the sensational skyrocketed boom in IoT devices from million to 30 billion in 2020, the ecosystem [130] of IoT is becoming smarter [61] with pressing concerns on security and universal adaptability. When the devices talk to each other and to the person we get a customized environment. In the morning, when the alarm is connected to the heater, toaster, and internet we can get hot water from the heater, meal, and favorite music from the internet. Sensors embedded in every device continuously emit data and power the internet [181]. Devices collect information about the behavior and store it in the cloud. This facilitates machine learning without manual programming. QoS parameter based resource allocation [256] could be used for efficient management. End nodes like sensors collect data, process it using data analytics [233], and sends it to the cloud [252]. How do the devices create data? How is this data collected? With a lot of devices talking to each other, how is this huge data customized? Where do these data go? How this data is processed [191]? IoT provides a common repository for the devices to manage the data and a common language for these devices to communicate. Data analytics [44] is performed and valuable information is extracted as per requirement [142]. This data is shared securely with the devices for automation and efficiency. IoT is the synchronization of Human, Things, and the Internet as shown in Fig. 2. Analogous to people communicating through their five senses, the internet senses and communicates, thereby interconnecting people and things. Electronic machines transfer data to cloud over TCP/IP [274].Lost devices could be found using a mobile App. Public transportation, self- driving cars, connected apps, and real-time traffic information will revolutionize [196] the driving modalities. Based on its vision [75], IoT extends to

Fig. 1 Incremental Stages of IoT

Fig. 2 Evolution of IoT



the Web-of-Things (WoT) if objects are integrated into the Web, Cloud-of-Things (CoT), and Internet of Nano-Things (IoNT) [254]. IoT builds a smart environment [111] based on how it is integrated into the societal, professional, and personal requirements [123]. If it is M2M [157], it is directly between devices. This does not require an Internet Connection. Due to its limited potential, the future [169] of IoT is based on 5G, customized mobile App, software development, Artificial Intelligence, deployment, and cloud-based digital innovations. Due to its massive embracement, IoT is analyzed using simulations such as Omnet++[95]. Tagra et al. [268] analyzed lightweight IoT using java framework. Forecasting could be done using Google Trends Tool [102].

The organizational structure of this review contributes towards: Overview, IoT Eco-system Functional Modules, Novel physiognomies of IoT, Significance of application-oriented IoT, Research Issues and Open Challenges [119], Architectural Insights, Design Issues related to security and lightweight algorithms, Inferences and Future directions.

2 IoT Ecosystem-Functional Artifacts

An ecosystem comprises of the devices, people, data, and processes.

- ***Devices*** Things should sense, actuate, and interact with other things so IoT applications utilize sensor, actuator, processing unit, power supply, network connectivity, and a unique ID for deployment [82]. Things collect data from the environment. Data could be temperature or live video. A smartphone [96] cannot sense these parameters. Devices (Things) should be IP-enabled, dynamic, heterogeneous [91], interoperable, and scalable with a communication protocol such as Bluetooth or Wi-Fi to communicate with other things. Based on the data such as the image from a camera, the device moves an actuator or controls a motor. In yet another approach, multiple sensors gather information about humans. If a human approaches a robot, the human–machine interaction is made satisfactory by using chatbots along with Artificial Intelligence and Machine Learning Algorithms. [20].
- IoT has heterogeneous [63] devices running on different platforms [175]. IoT platform is an intelligent [131] layer that connects things to the network and facilitates communiqué, device management, and functionality of applications. So the devices should be interoperable [109].Various scalable distributed architectures such as Distributed Internet-Like Architecture (DIAT) addresses heterogeneity and scalability issues in IoT [49]. FogBus offers platform-independent interfaces [253].
- ***Interoperability*** is based on: (i) Device interoperability which manages the exchange of data between different devices and permits the addition of new devices (ii) Network interoperability that operates on multi-service and multi-vendor networks. This also manages addressing, routing and security issues [177, 294]. Peer-to-peer routing was proposed using a Distributed Hash Table (DHT) approach to guarantee scalability [90]. Multi-Technology interoperation reduces hardware resource usage but consumes more energy and reduces battery lifetime due to simultaneously active radio resources [9]. (iii) Data syntax format interoperability (iv) Platform interoperability (v) Semantic interoperability enables different services [174].
- ***Connectivity*** State of devices are expected to change dynamically. With an increase in the number of devices, data gets increased. It should be possible to extend the existing features of IoT. A huge amount of data is sent to the cloud using commu-

nication media such as Mobile, Bluetooth, Wi-Fi networks etc., Devices should be network connectivity enabled.

- ***Communication Protocols*** Devices and servers communicate through the protocols in the physical layer, network layer, and the application layer.
- ***Data Processing and Associated Services*** Once the data is collected in the Cloud, it is processed by the respective software. Data processing varies from reading parameters to identifying objects. IoT provides services such as Device Discovery, Data Analytics, and Device Control. Data should be location or environment-specific. Data access should not be location-specific. Mobility is supported. Data is processed intelligently using data analytics techniques such as Artificial Intelligence and Machine Learning [78] for operational efficiency. Big data [32] collected is processed in the Cloud. Using analyzed intelligent data, the device is automated and could be remotely controlled.
- ***User Interface*** The processed data is made available to the end-user either as a message or as a control element fed through an interface. For example in healthcare, real-time patient monitoring aids doctors in decision making.
- ***Management*** This provides functions to manage an IoT system. IoT perspective is ecosystem-based. People generate and sustain IoT. As the network increase [35] with the number of devices, the amount of data to be handled is a massive challenge. Analyzing, processing, and delivering the data accurately at the right time is the success of real-time streaming IoT.
- ***Security and Secrecy*** With online processing of personal data, endpoints need to be secured.
- ***Application*** IoT gains real-time insight into data assets. With this a production unit can be modeled based on accurate predictions. This provides modules to monitor, visualize, and predict futuristic prospects [228].
- ***IoT objects*** Machine, device, Users, or applications communicate through the Internet to consume, request or access digital information. Devices are connected to the Internet through a broadband modem provided by an ISP or through a wired /wireless connection using a router. A gateway connects the nodes to the Internet. A protocol is used to connect the devices and they are identified by an IP address.

3 IoT–A Substantial Frontier- Contributions and Utilities

IoT unifies heterogeneous things with interoperability through an IP based architecture. Internet-of-things [213] integrates [265] sensing, networking, storage, and analytics based on the trending areas of health, transport, industrial automation, etc. IoT is still in the nascent stage of development. It meets its key artifacts through these design contributions and utilities [243]. IoT forms an extensive design space comprising of various dimensions that include:

Accuracy Monotonous applications are less error-prone.

Application-Specific Cloud service providers are application-specific.

Automated Interoperability with Control IoT requires to be self-adaptive with intelligence [291], autonomous for data collection, and dynamic to the ecosystem with minimal plug and play configuration pre-requisites [49]. IoT depends on the social, environmental, and business [113] perspectives in the future [193].

Economical IoT promotes economic resource utilization [43]. It minimizes cost, time, and labor. It maximizes productivity returns and minimizes cost [55]. It assures quality and security.

Efficiency With IoT, large volumes of data are processed without harnessing the system performance and with minimum manual power. This eases informative decision making for real-time applications [59].

Co-existence Industries [165] require suitability and co-existence between hardware and software integration [56].

Context-Aware Based on the sensed information from the physical and environmental resources, IoT devices will enable ambient intelligence and the infrastructure is configured.

Data sharing IoT analyses and delivers data irrespective of location in real-time. This encourages mobility, reduction in production cost, and generates revenue.

Dynamic and Adaptive Devices connect, disconnect, and dynamically adapt based on battery lifetime, mobility, and other operating conditions. For example, surveillance cameras adapt their resolution based on movement and mode as per time.

Integrated Infrastructure IoT devices are made smarter through the dynamic integration [65] of hardware, software, and networking based on the application.

Intelligent Decision Making Distribution Systems IoT employs different algorithms, data mining, and data analytics for taking decisions [93]. IoT is multi-hop in nature. It improves the energy [81] efficiency and lifetime of the system. Dhananjay et al. [58] used a semantic fusion model as a novel framework to encapsulate data processed from the sensor.

IoT buoyed Technologies Different hardware platforms such as Processor, operating systems like LiteOS, cloud service providers such as Amazon [26], wireless technologies like LoRa are used for different applications. As IoT gains momentum, wireless resources proliferate dramatically [148].

Multi-faceted Data Specific Design Data comes in different sizes and formats. Novel architectural design is required to handle multifaceted data.

Multi-protocol Integration Integrates protocols in the subsequent layers based on the application.

Safety and Security Monitoring improves safety. Sensors and suitable algorithms improve security.

Self-Configuring IoT can integrate, fetch data, set-up a network, fetch software, analyze data, and control a device.

Skills Internet skills are required for IoT acceptance and usage [220].

Transparency Devices are connected, so it is possible to track assets.

Ultra-low latency LTE (Long Term Evolution) and 5G [264] provides connectivity for future IoT devices with less delay [144, 186, 245].

Unique Identifier Each device has a unique identifier such as an IP Address or URL. This is coordinated with the infrastructure for control and monitoring.

4 Research Issues and Impediments

Ample research issues and narrations like vulnerable attacks, protocols exist. But there are less mitigating solutions in IoT. For example, RFID is a vulnerable source [187] in terms of person and asset tracking [170] and on the other side, it monitors [5] for safety purposes [288]. Blocker RFID tags were proposed for consumers to selectively block RFID readers

from scanning and disclosing when required, thereby protecting privacy [151].Some of the major research challenges [58, 298] and obstacles faced by IoT are described below:

Application Based on the application, hardware, software, and tools are integrated [71].

Authentication and Authorization Clouds and mobile components [163] do not have sufficiently strong passwords. 80% have weak passwords.

Complex Computing Architecture With differing heterogeneous Operating Systems and hardware, a complex computing [97] architecture is required. Architectural solutions vary from standard to commercial depending on the major requirements of interoperability and security [67].

Confidentiality When data is transferred over the Internet from different devices, it needs to be secured.

Constraints Limitations [69] faced by IoT include:

(i) ***Hardware Limitations***: Miniaturized Hardware is battery powered and so precise cryptographic algorithms that consume a lot of power is perilous. RAM has memory constraints so Light Weight OS with less complex computational complexity is used. Conventional algorithms occupy space. Tamper resistant packages are required for IoT as they remain connected and unattended for a long time.

(ii) ***Software Limitations***: Software packages need to be fault-tolerant and thin. Dynamic reprogramming is not possible.

(iii) ***Network Limitations***: Mobility resilient algorithms are required. Security algorithms need to be scalable to accommodate the proliferating IoT devices. Unified security algorithm for dynamic topology, multifarious devices, multi-protocol networking, multi-vendor, and multi-medium is hard to design. Data integrity and QoS are disrupted. For data integrity, a random time hopping sequence is used to hide data. Device ports are exposed to the device level, interface level, and gateway level service providers.

(iv) ***Security Constraints***: Integrity, Anonymity, Authentication, Authorization, and Non-repudiation [18] is to be warranted. Access level security should certify authentication, authorization, and access control. IoT devices should be resilient against attacks [283].

(v) ***Serviceable Constraints***: Robust network should self-organize and sustain from hardware or software catastrophe.

(vi) ***Attacks*** can be internal /external based on device location, active/passive depending on the level of attack, physical /logical based on the nature of the damage, user-credentials in hardware/software depending on the type of compromised host attack.

Constant update and Uninterrupted Network Connectivity Software requires updates for effective operability. Software updates are not encrypted mostly. Devices need to be online always and are unattended. This leads to vulnerable attacks. Devices are deprived of power.

Cyber-Security IoT [125] is vulnerable to cyberattacks which poses daunting challenges [242] to digital forensic experts [16]. Blockchain builds trust in sharing information [15]. Bitcoin [207] is used to exchange value across Internet [17]. With embedded [270] technologies, the attack could be from the device or from the cloud or from the network [261]. IoT devices communicate through the application programming interface over the Internet and connect the cyber world to the physical world. IoT is vulnerable [79] to denial of service attacks [163], virus attacks, and so on. Thwarting such attackers is a challenge. Cyber Physical Systems (CPS) compute, communicate, integrate, and control technologies for

stability, reliability, and efficiency in the application domain. This involves Artificial Intelligence and knowledge integration [149] into the systems to develop solutions for complex problems. Cesar et al. [46] added smartness to IoT and CPS in his research using Decisional DNA to capture, store, and reuse data.

Data Analysis Big data [94] should be interpreted and analyzed with fidelity. Big data can be structured, unstructured, or semi-structured. This finds use in e-health and m-health services [83].

Data-Centric Architecture Data storage varies. Currently, Redundant Array of independent Disk (RAID) architecture is insufficient. A centralized architecture is required for data storage. Many real-time applications model their communication pattern using a data-centric approach [64].

Data Volume A huge amount of data needs to be processed and handled. Storage needs to be reliable and secured.

Dedicated and Limited spectrum With an increasing number of devices, bandwidth and spectrum will increase. But the electromagnetic spectrum is limited. [150]

Encryption 70% of the devices fail to encrypt and transfers sensitive data over the network.

Hardware, Software, and Firmware IoT is an integration of both hardware and software. There is a misconception that it is software oriented. Challenge associated with hardware is miniaturization and power consumption. 60% of the software are not encrypted during updates [117].

Heterogeneity IoT is a complex heterogeneous networking platform**.** A plethora of devices working on different platforms and protocols, need to collect, connect, and communicate information to form an IoT. This faces addressing and optimization issues.

Identification Challenge is to identify and integrate suitable technologies for an application.

Interoperability Establishing synchronization among different platforms is challenging. Different sensors collect diverse data [140] and have interoperability issues.

IoT Forensics Big Data challenges faced by forensics [8] investigators include dynamically adaptive diverse data formats [3, 33] and insufficient real-time log statistical analysis. Threats caused due to viruses, mass surveillance etc., [157] lead to disruption in the IoT network. Tools available currently with the forensics team [15, 51] are not suitable for the IoT environment. [50].Computer Aided Investigative Environment (CAINE) is an open-source interactive forensic tool. Intelligent Edge Fabric (IEF) scans forensics images, chat history, and forensic data [8, 251]. Huge data transfer in IoT opens the way to intruders and cybercrimes. Vulnerability issues are analyzed [182] from forensics viewpoint towards challenges involved in cloud security and privacy. Francesco et al. [89] analyses on the vulnerabilities in IoT and the methodologies in developing digital [277] traces to combat cybercrimes. Traces were developed from movement, location, network traffic, and so on. Forensic preparedness will protect smart cities from criminal threats [305].An investigation of the crime scene would aid and minimize threats [51].

Light Weight IoT Integration of IoT with resource-constrained environments [62], was envisaged using light application layer protocols such as, Constrained Application Protocol (CoAP) [250] and Message Queue Telemetry Protocol (MQTT). CoAP is a web transfer protocol which is used for low power lossy networks. This uses Representational State Transfer (REST) architecture and UDP protocol [70, 221]. In CoAP, resources are identified by URI [126] and deployed using HTTP (Hypertext transfer protocol). CoAP consumes less bandwidth and MQTT does not include resource discovery mechanisms [68]. A Light Weight security architecture HIMMO was proposed to

warranty back-end authentication, key–agreement, and protection against Denial-of-Service (DoS) attacks [199]. A hybrid approach [114] was proposed for RFID tags [263] to ensure data confidentiality [227].

Low Power Constraints Tiny devices with low power-constrained [120] resource is required for IoT. Low power is required to operate sensors. Energy could be harvested from peripheral and vibrational movements for energy-efficient sensing. E.g., Advanced Metering Infrastructure is used for low energy in smart homes.

Mobility Devices are in different locations. Users prefer data access from anywhere and at any time. Connectivity provides mobility.

Multiple location and Networks Data should be communicated reliably over the network. When the user changes the location and uses different networks for connectivity, the investigation becomes complex.

Network 2G for voice, 3G for voice and data. 4G for broadband internet and 5G provides transmission speed [88] up to 10Gbps; connects thousands of devices reliably [9, 37]. Network Optimization for IoT traffic improves routing, QoS, security, data rate, response time, and redundant data elimination [258]. 70% of the devices use unencrypted network services.

Performance, Investment, and Evaluation For evaluation, services need to be updated time-to-time on a regular basis. End users need better features at a lower cost.

Proprietary IoT needs ownership to maintain and grow as per needs. With heterogeneous hardware and software from multiple vendors, proprietary is difficult to realize. Managing and maintaining the numerous resources is a challenging task.

Reliability With system failure in hardware or threat induced in software, IoT faces a major setback.

Robust Communication Interface and Network technology Applying a suitable communication technology to interconnect the heterogeneous devices to the Internet is a challenging task. To meet these issues, a Mobility First Architecture was proposed by Li et al. [168]

Scalability and Network Supervision IoT connects and manages billions of devices to an existing infrastructure without affecting its existing functionalities and services [138].IoT could be integrated with process awareness to support pervasive [162] computing environments [159].

Security and Privacy Big data requires stringent security measures. Devices collect personal information [139]. 80% of devices have privacy [36, 160] concerns. Secured IoT is achievable with tools to monitor endpoints. IoT devices are to be scanned before connectivity. A dedicated network secures IoT devices. For IoT, the devices are connected online wirelessly [247] and remain unattended. This compromises authentication and data integrity in IoT. It is prone to sleep deprivation attack as the battery constrained device remains 'ON' always. Collected data should be used only by authorized personnel [22]. When networks are large, erroneous data could be sent, the network could be made unavailable. IoT is resource-constrained, so public key encryption algorithms are hard to use. Lightweight cryptosystems [158] are required. IPv6 routing protocol is open to threats [106] so traditional encryption techniques do not apply. Security measures based on Confidentiality [28], Authentication, Availability, and Integrity [21] is implemented. This gets complicated with automated configuration. Physical safety of the devices is required. IoT deployment and its widespread applicability is constrained due to its insufficient measures towards encryption, trust and data privacy [169, 235, 272].

Service-Oriented Architecture (SOA) Design This design faces scalability, processing, and data transfer issues. Powerful service description language, service discovery [219] methods are yet to be catered to the needs [282].

Signal processing This identifies data, collects the required data and processes it suitable for a particular application.

Software-Defined Network (SDN) This controls network and nodes dynamically based on programming. SDN combined with a deterministic virtual network (DVN) and lightweight encryption facilitates ultra-low latencies and improved security suitable for Industrial IoT [269].

Standardization Yet there is no existing standardization [209] in connecting disparate networks [11]. IEEE has produced more than 80 standards [143] relating to IoT [223]. In 2013, universities and industries collaborated [135] and developed an architectural reference model [54] for IoT referred to as IoT-A, which is no longer active. IEEE standardization is required to preserve data flow across heterogeneous networks (HetNet) and provide design specifications for information exchange and processing. In smart home automation [84], different devices are from different vendors. IoT faces connectivity issues [240].

Traffic Threats IoT device ports decide on the network traffic. These ports are susceptible to threats [110].

Uncontrolled Environment One model will not fit for all. Getting accurate and stabilized results for IoT in an uncontrolled environment is the challenge [153].

Unified Information Infrastructure Different devices occupy different bandwidths. A unified information infrastructure suitable for heterogeneous devices is required.

Unique ID Due to limited IPv4 addresses, it is impossible to consign each device with a unique identifier. This is overcome using IPv6. Network plays a major role in IoT. IPv6 routing protocol (RPL) is used for resource-constrained low power lossy network (LLN). This improves network lifetime, throughput and QoS. Internet Protocol (IP) manages traffic load from multiple devices and provides seamless [99] connectivity [217]. RPL is used for real-time applications to transmit sensitive data [30]. It replaces an up-to-date route in case of dynamic network changes.

Virtualization Lot of challenges exist in realizing, developing, and adopting a model to the existing scenario to meet the requirements [121].

Web Interface 60% of the devices raised concerns about insecure web interfacing such as cross-scripting and weak session management.

Compatibility 5G is revolutionizing IoT with faster data rate [245] for future IoT applications [241] such as virtual reality, high definition video streaming, and augmented reality with 25 Mbps for optimized performance. 5G is in its budding stage and requires scalability, low-latency for video games, upgraded handover efficiency, increased battery life-time, time constraints for real-time applications and smart service provider to provide services as per application and mobility [122]. Radio Access Technology (RAT) and antenna innovations serve the purpose. Modulation is implemented in the physical layer. Timely handling of multiple input data will produce errors. These issues need to be handled. Mutual shaping between 5G and IoT will improve business models [183]. IoT along with high efficiency video coding is used in smart city framework for media security [189].

5 Categories of IoT

IoT is an embedded internet technology encompassing the physical and digital components. IoT categories are based on its applications [133]:

(i) ***Consumer IoT (C-IoT)*** for smart home automation proliferates the quality of people's life with saving in time and money. Smart Homes are automated and networked with electronics, sensors, and software to reduce energy wastage in devices and to improve safety [200]. Researchers analyze the revenue patterns targeted by the manufacturing companies [87]. Smart Homes use Arduino [47] as cyber physical systems for energy monitoring [167].
(ii) ***Commercial IoT*** Healthcare Automation and Transport Automation uses Vehicle to Vehicle Communication. In-home care, IoT devices such as wearable sensors are fused with IoT services[188] such as telemedicine [296].With increasing chronic diseases, Clinic centric is focused on Patient-centric using a multi-layer e-Health Architecture [29]. Information and communication technologies (ICT) provide promising e-Health solutions [152]. An anti-counterfeit platform is used to check the creditability in online purchases [170].
(iii) ***Industrial IoT (IIoT)*** This integrates operational and informational technologies to design autonomic industrial plants, smart agriculture etc. [165]. With IIoT, [257] for intelligent transportation, a vehicle and its movement could be monitored. Based on the predictions, traffic could be anticipated resulting in shortest route discovery and time-saving [176].
(iv) ***Infrastructure IoT*** This connects smart cities with sensors and user-friendly apps. Big data is used to provide smart transportation, smart healthcare etc., in cities [124]. Fiware is an open platform for smart cities [85].
(v) ***Military IoT*** Robots are used for surveillance in disaster-prone areas.

6 IoT Communication Technologies

IoT design related to the applications of IoT include connectivity, cost, coverage, deployment, infrastructure, lifetime, mobility, modality, QoS, size and topology for cellular and non-cellular technologies [77]. Some of them are:

(i) ***RFID*** Radio Frequency Identification has a tag and a reader [7]. This uses the radiofrequency electromagnetic field to transfer data associated with the object. Each RFID has a unique ID.This is of low cost [171]. It has a microchip along with an antenna as a package. RFID Tags could be self -powered active tags or signal powered passive tags. They monitor objects [146] in real-time without Line-of-Sight. Passive RFID tags are made duplex to remotely exchange data for communication [72].
(ii) ***Zensys Wave (Z-Wave)*** This is a low power wireless communication protocol used for home automation to connect devices within 30 m.
(iii) ***Long Term Evolution (LTE)*** [76] This is a high-speed wireless communication protocol that transfers data between mobiles with high throughput and low latency.
(iv) ***Long Range (LoRa)*** This is a digital wireless technology that is used to connect devices remotely over a long-range.

(v) ***NearField Communication (NFC)*** This is a short-range, low power, radio communication wireless link enabled on mobile devices within close proximity of 20 cm, and operating at a licensed frequency range of 13.56 MHz to exchange data. Unlike Bluetooth, pairing is not required. Security is achieved using key agreement techniques [115, 214]. NFC [103] facilitates contactless communication [41].

(vi) ***Ultra-Wideband (UWB)*** This technology supports data transmission with low power over short distances. If sensors are deployed for applications, it consumes wider bandwidth.

(vii) ***Machine to Machine Communication (M2M)*** This connects devices to the network or devices to a gateway [244] and then to a network for information transfer.

(viii) ***IPv6 Low Power Wireless Personal Area Network (6LoWPAN)*** This low power IP Network Protocol defines encapsulation and header mechanisms [210]. This supports multiple communication platforms like Ethernet, Wi-Fi etc. Integrating management protocols such as 6LoWPAN [300], CoAP into IPv6 is a challenge [201].

7 IoT Architecture and it's Operating Systems

IoT is conceptualized to reality by jumbling up different technologies. IoT Vision is to interconnect heterogeneous devices Anywhere, Anytime and with Any-media using IP, communicates and processes data using Cloud and embedded software. For example, to analyze multimedia traffic, media-aware traffic architecture is proposed for IoT. IoT is an interdisciplinary field that is oriented towards three prototypes: Things oriented (devices), Internet-oriented (middleware), and Semantic oriented (knowledge) [107] e.g., WoT. IoT expands human–human communication to human-things and things-things to exchange information between the physical world and the virtual world [124]. Architecture can be user-centric or cloud-centric. In user-centric, the user will be at the center and uses data and infrastructure depending on the applications. Economically cloud-centric is better. Al-Fuqaha et al. envisioned IoT [10] as a technology that enables physical objects to see, hear, think, share information, coordinate decisions, and perform jobs.

IoT requires a power-optimized communication stack, reliable peer-to-peer communication stack, and an Internet empowered communication stack [184]. IoT architecture facilitates a systematic understanding of the tools, technologies [216], and methodologies that are vital to a developer to connect the digital world and the physical world [72] and to build the infrastructure. IoT Architecture is framed, based on the application such as healthcare and its pre-requisites such as security [228]. Currently, RFID and healthcare are rated stringent. Data is created by the device. Data is sent to centralized service using HTTP/CoAP/MQTT. HTTP is not suitable for low bandwidth applications. MQTT—A Resource-constrained protocol uses publish /subscribe model. It has low overhead, lower bandwidth, but has no encryption procedures [211]. CoAP is suitable for low power and low bandwidth applications. A centralized server is risky in case of data loss without back-up. IoT architecture [302] should satisfy scalability, interoperability, reliability, and Quality of Service. IoT requires real-time analytics, a platform to analyze the aggregated data, a cloud to collect the data, trigger remote action and send remote notifications. IoT enabling technologies in tandem comprises of the hardware, middleware, and application occupying the perceptive, network, and application layers respectively. The basic architecture of IoT is a three-layer architecture [124, 157, 215, 290]. It consists of the physical layer, network

layer, and the application layer as shown in Fig. 3. A clarified insight into the lifecycle of the processes involved in IoT leads to prediction in future developments.

(i) ***IoT Things (The Physical Layer)*** This is the physical layer that senses and gathers entities from the environment [303]. This specifies the path between adjacent nodes for data transfer. Hardware consists of wireless sensors [179], Robotic cameras, Radio Frequency Identification Tags (RFID) etc., based on the application. Barcode facilitates automatic identification of anything. Wireless Sensor Networks [122] are cost-efficient and power-efficient. Physical devices and controllers referred to as 'Things' collect and transmit the data on receiving the command.

Sensors collect data and share it with the centralized system for analytics. Sensors have transceivers, processing units, A/D converters, and recently they operate on one frequency range, making it less complex. Actuators [190] control the things using the electrical inputs. Simply put, for the smart room controller, a temperature sensor senses the heat, and sends the signal to the control center. The control center sends commands to the sprinkler. The sprinkler turns on and puts out the flame.

Sensorpedia is a new integration platform that guides users regarding identifying and sharing of sensor data. Sensor data is processed on a Google map. Users can search and explore [299] published sensor data using an interface [104]. In some cases, data would be time-sensitive. In other cases, this data velocity creates an avalanche. For data that entails profound processing, it is sent to the cloud. Short-wave technologies like Bluetooth permits devices to communicate with each other. IPv6 connects sensors to the internet without additional processing.

Technologies used in the physical layer like Bluetooth, Wi-Fi (devices are connected by radio), BLE (short distances), and 6LoWPAN (IPV6 and low power personal wireless personal area network) are suitable for IoT. 5G improves data rate and latency [224]. BLE uses Blue–voice [98] for providing Speech Streaming Services.

(ii) ***IoT Network Layer*** This connects devices to servers and specifies the communication path over the network (IP Address). Data collected from the sensors are processed and analyzed intelligently for optimized decision making. Raw data collected from the sensors is converted into digital streams by Data Acquisition systems. Data acquisition samples the real-time physical entities and converts it into digital streams suitable for transmission using analog-to-digital conversion. The Internet gateway aggregates these digitized data and routes it to Wi-Fi or wired LAN for further processing. This layer inclusive of switches and routers is responsible for secured,

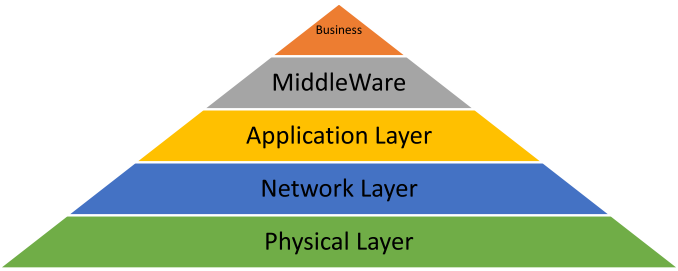


Fig. 3 IoT Architecture

reliable, and timely delivery of data. Data is stored and retrieved as per queries. Efficient net centric algorithm could be used to reconstruct the data efficiently [166].

(a) Challenges involved in Data Analytics and Processing

Data analysis varies depending on the volume, velocity at which the data is generated, and the structure of the data. Data analysis is done using Machine Learning by fitting the data into the model. Based on the pattern generated from Machine Learning, a predictive analysis (of what would happen), prescriptive analysis (steps to be followed next), and adaptive analysis (to be in line with the changes) could be done. IoT includes real-time streaming data without delay using a real-time framework such as Apache Storm. If the size of the data is huge, then distributed data analytics is used to reduce the load on a single server such as Apache Hadoop Server. Data is distributed across several nodes and is processed using the MapReduce engine.

Apart from Data Processing, storing a huge amount of data is not feasible using the traditional database approach. IBM Cloudant provides a solution. Amazon, Microsoft [192], Google provide infrastructure, platform, and software as a service. Consumers save a lot of money and manpower. Based on consumption, charges are applicable.

(iii) ***IoT Cloud and Application Layer***: This provides application-specific services to the user. This specifies the interfaces and protocols used by IoT devices [40].Once the data is aggregated, the information is either stored locally or in a centralized remote server for analysis. Then it is fed to new applications and services. IoT requires platforms, tools, and libraries to visualize the data. IBM's BlueMix is a platform that connects innumerable devices and sensors and provides API's for data visualization in formats specific to the device [266]. ThingSpeak supports sensor data along with MATLAB for visualization. Individual software work as per requirements on device control, visualization, and analytics. Data and conclusions are shared with other applications leading to innovative IoT.

(a) IoT and Cloud Integration involves

- **Device Management**: As devices increase, management [230] such as registration, updating of software complexity, and cost increases. With Cloud, based on usage, charges apply.
- **Resource Pooling**: Based on demand, resources are integrated into the Cloud [108].
- **Data Storage:** Large scale data and Long term data is stored in the Cloud.
- **Access Control:** There is access control authentication for Cloud.

IoT employs protocols, networks, and applications [236]. IoT applications are based on monitoring, control, automation, and optimization [101]. Commonly used operating systems to enable the functionalities of the application domain are TinyOS [164], LiteOS, Contiki etc. They require few kiloBytes of RAM and provide optimized low power Internet Communication. Software Development Kits (SDK) supports application programming using C, C++, and Java etc. Software connects IoT objects to the network using communication protocols. Table 1. Displays the functionality and the types of devices associated with each layer.

Table 1 IoT Layer functionalities

Layer	Functionality	Devices
Physical	Identifies and collects data such as temperature	RFID /sensor
Network	Addresses each device with a unique Id and transfers data from the physical layer to the Application Layer	Wired/Wireless Network Wi-Fi/Bluetooth/ZigBee etc
Middleware Layer	Stores, Analyses, and processes the data. This facilitates Interoperability, context-aware detection, Device and Data management, Security, and Privacy	Service Management, Decision Making, Ubiquitous Computing, Data Processing
Application	Provides application-specific services to the user. This facilitates Reporting, Application, and control	Smart Home, Remote Healthcare, Smart transportation
Business Layer	Manages services and applications of IoT. Uses data to build models. Manages user's privacy	Graphs, Flow charts

Due to the trending applications in IoT, different layers are proposed by practitioners. A five-layered approach includes Middleware Layer and Business Layer to the basic prototype [280].

(iv) ***Middle-Ware Layer***: A middleware is a software that interconnects and manages these heterogeneous components. Smart Things is a Samsung cloud-based platform, which supports 300 plus devices for user control home automation. Web-of-Things and cloud is used as an interoperable platform for smart home [24].This layer is between the application and technology layer to aid design workflow [147], data management [2], and interoperability [57]. Data Management combines multiple databases and unifies interfaces [33]. Centralized storage archives data and also integrates both structured and non-structured data [92]. HTML5, Web Socket, Canvas supports real-time applications. HTML5 and Adobe Flash are preferred for low latency [304].Middleware manages the services offered by things, stores it, processes it, and analyses the data [172]. Middleware is specific to the application. For example, ASPIRE is specific for RFID. There is no generic middleware common for smart home, smart transport etc., Middleware delivers application layer interfaces (API) for physical layer communication and related services to the applications [31]. IoT-ICN architecture is included in the middle layer. Real-world deployment is yet to be implemented. Wang et al. [285] proposed a data platform (RESTful Web Service) as a middleware to access physical objects with a unique URI.

(v) ***Business Layer*** provides business models and graphs along with the data.

CISCO [Cisco] as shown in Fig. 4 has proposed a seven-layer reference model based on the functionality:

The physical layer has things ranging from a small chip to a big machine. These devices convert the data from analog to digital and are being controlled by the net. The Connectivity (Network) layer connects the IP –Enabled devices. If they are not IP Enabled, they are connected via gateways. This layer associates the necessary switches, routers, and protocols

Fig. 4 IoT Reference Model

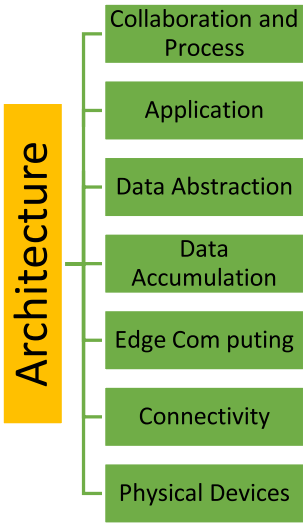
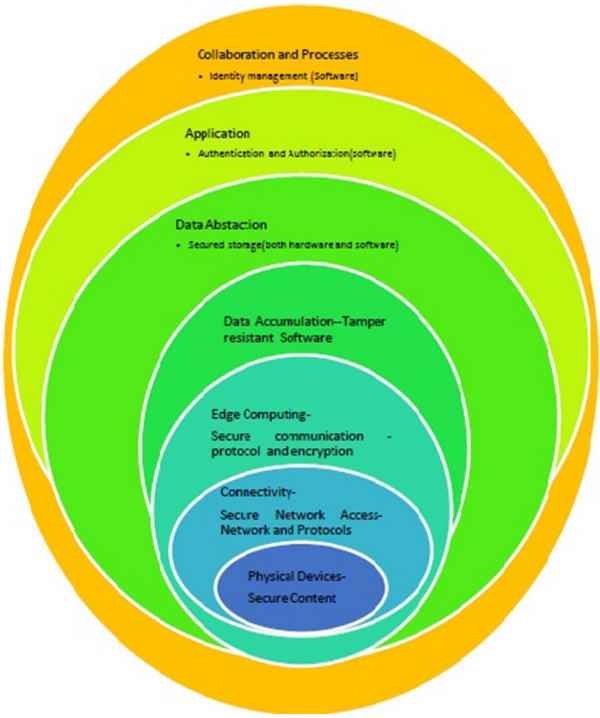


Fig. 5 IoT Security



required for connectivity. Security is associated with this layer. The Edge Computing [267] layer translates the data into a form that is suitable for storage [39]. Fog Computing [286] bridges the gap between data centers and IoT devices [13]. It is considered as a mini cloud which is close to the IoT devices [273]. For example, the sensor provides several samples per second in a day. The Data Accumulation Layer keeps the data. Certain applications cannot run the data at network speed. This layer has data filters and converts data into relational tables. The Data Abstraction Layer collects data from multiple sources and reconciles differences in terms of format etc. Information interpretation occurs in the Application Layer. This gives data at the right time for real-time applications. Collaboration and processes layer involves collaboration for business logic to meet people and people use applications as per requirement. Security is involved in each of the layers. Devices have an IPAddress and communicates with the services offered by the Cloud. Devices without an IPAddress use short-range communication protocol such as ZigBee [48] and connect with an IoT Gateway which communicates with the services offered by the cloud.

In future, there is a likelihood that the number of base stations will upsurge than the number of mobile phones [145]. Figure 4 and Figure 5 relates the layers in the IoT architecture with their associated security.

Operating system [212] design features [74] include low memory requirements, low cost, low power consumption, small size, low processing power [38], heterogeneity, catering to multiple network stacks, security, and energy-efficiency [225]. OS is usually embedded. It collects and communicates data over the Internet. TinyOS is used for low power wireless devices with commands and tasks for inter-component communication and tasks for intra-component communication. Contiki OS [4] is an open-source lightweight portable OS with low power, low memory, low processing, and low bandwidth. RIOT OS is

the Linux of IoT [27].This uses minimal resource devices and provides real-time services. Ubuntu OS is suitable for IoT devices [275].Instead of the conventional programming languages, IoT uses scripting languages like Bash Shell in platforms such as GNU/Linux [112].

8 Taxonomy for IoT Security Framework:

The Interagency International Cyber Security Standardization Working Group has formed the IoT task group in 2017 to formulate the cybersecurity standards [53] for IoT [118]. LTE is preferred for better bandwidth, and spectral efficiency but IoT architecture suffers from threats [116]. Salman et.al. reviewed [238] on the existing standards and protocols for IoT. Common attacks in IoT include DoS attack, Man-in-the-Middle Attack. IoT security demands research on the privacy of data [218, 259, and 128], prevention of loss of data from personalized devices, leading to impersonation attacks and prevention of malware via botnets which leads to Distributed Denial of Service Attacks (DDoS) [51]. For IoT devices to be secured, it requires to ensure authentication, integrity, confidentiality, availability, authorization, secrecy, and non-repudiation. To ensure these, cryptographic techniques [249] such as encryption at the wearable device level (AES and SHA algorithm), device level (Public Key Exchange (PKE)), network-level are implemented in an IoT Ecosystem. For a wider area of coverage and data stored in a Cloud, Internet Protocol Security (IPSec) and Secure Socket Layer (SSL)) are used. Symmetric (AES) algorithms, Asymmetric algorithms (RSA), Light Weight Algorithms, and Digital Signatures are used in IPSec for authentication [260]. IoT Botnets are massively attacked and controlled by Hackers [19]. For instance, Mirai cyberattack tool used brute force attack [194] and took over numerous IoT devices. This remains a mystery. Botnets IoT Security is based on the Application domain, Architectural Domain, Data domain, and Communication Channel.

In the physical layer, the sensor nodes operate with stringent power and memory requirements. This makes frequency hopping spread spectrum and public-key encryption hard to realize. Sensors could be compromised by transmitters and antennas from a distance [178]. RFID Tags suffer due to security issues [156] in wireless technologies [28]. This requires mutual authentication [197] implementation in high frequency RFID tags [206]. A lightweight security algorithm with low power and area is achievable by using a combination of encryption algorithms [205].

Network Layer is prone to man-in-the-middle attacks. Authentication prevents unauthorized access. Data sharing at the application layer poses threats to access control and privacy, resulting in disclosure of data. The application layer across heterogeneous networks demands user privacy and authentication. Physical layer security (PLS) is used to avoid data leakage. Challenge is to provide reliable security with low power. Modulation techniques decide upon the data rate, bandwidth, spectral efficiency, and power of the hardware used. PLS also depends on modulation in wireless technologies. If data is less, narrowband is used. If the data is more, then wideband communication is used. With bulky directional antennas, secrecy is improved. By performing modulation after encryption, low power consumption and reduced hardware complexity is achieved [222]. Narrowband IoT supports features like deep coverage both indoors and outdoors, less complex multiple devices, and low power consumption. With low power, security is compromised [77]. 5G supports narrow-band IoT and increasing traffic [9].

IPv6 communication protocol is used for IoT in the physical layer. Datagram Transport Layer Security Protocol (DTLS) [154] is used in the network layer. Constrained Application Protocol (CoAP) is used in the Application layer and IPv6 is used for addressing in the proposed lightweight security architecture [232]. AMQP supports various communication patterns [3]. IoT protocol stack is not categorized as OSI or TCP/IP [246] protocol suite. IoT security protocols operate in multiple layers to provide security. The chosen type of protocol depends on the node as to whether it is constrained or not. A comparison of the some of the protocols used in conventional internet and IoT networks is detailed in Table 2. There are many more protocols apart from those compared.

Not all the protocols are used. For example, while loading a webpage from a domain, the web browser makes a Domain Name System (DNS) request using a HTTP request and sends it to the internet. These protocols are used in each layer. WLAN-IP-TCP-HTTP. If the webpage is served over HTTPS, then multiple protocols are used in the application layer. Each layer uses a different protocol. IoT Security framework depends on time constraints, power and energy consumption, lightweight constraints, reliability, robustness, and smart applicability. [284]

9 Low Energy Methodologies

Energy Efficiency is required for battery constrained IoT Devices. Zeeshan et al. has provided energy-optimized solutions [301] for wireless technologies operating with IoT. Towards 2025, IoT devices will reach 11 trillion [ISO/IEC].Almost every device will have an internet node, and devices need to sustain energy. Green IoT is proposed for energy conservation [52].

Energy consumed by the sensor nodes is reduced by:

(i) ***Variable Duty Cycle*** The duty cycle is varied, based on the ON time and OFF time of the node. This is made automatically adjustable.
(ii) ***Multilayer based approach*** Nodes are grouped as layers. Applying optimization techniques to these layers, power is reduced.
(iii) ***Low power Protocols for sensor networks*** Vakulya et al. proposed two protocols namely queue response protocol and piggybacking protocol for low power [279]. This is achieved with an increase in latency.
(iv) ***Frame size control*** Based on the MAC frame size, optimization is achieved.
(v) ***Low latency*** IoT deals with real-time data applications where continuous data stream is required with low latency. This is achieved using parameter tuning, with frame synchronization and sleeping behavior.
(vi) ***Priority-based*** By assigning pre-defined priority smartly to the nodes, nodes with the highest priority can access the media. This saves power.
(vii) ***Variable back-off*** By varying Back-off exponent (BE) and Contention Window Length (CW) of MAC, throughput, packet delivery ratio, and low energy is achieved.
(viii) ***Self –configuration*** Networks are configured with less overhead.

Table 2 Comparison of protocols used in Internet and IoT network

Layers	Communication protocols used in internet	Security protocols used in internet	Communication protocols used in IoT network	Security protocols used in IoT network
Data link layer- Sends and describes how data is sent between hosts	IEEE 802.3 Ethernet/ IEEE 802.11 WLAN/Wi-Fi	WPA2	IEEE 802.15.4 /Wi-Fi/ Bluetooth/Ethernet	WPA2
Network layer- sends/addresses/receives data/controls packet movement in the network	IP/ARP/ICMP/IGMP	IPv4/IPv6	IPv6, 6LoWPAN,RPL	IPSec
Transport layer	TCP/UDP	SSL/TLS/SSH	UDP/TCP	DTLS/TLS
Application layer	HTTP/SMTP/TLS/ DNS	PGP/HTTPS	COAP/MQTT/ AMQP	User Defined

10 Standardization of IoT

Smart objects consume and process large volumes of data that need to be transferred securely. This requires universally accepted standardization of protocols for interoperability between devices and applications [134]. IoT is one of the context data for smart applications. IoT devices connect through the network through messaging and communication protocols at each layer. The protocol depends on the type of application and the range of communication. Based on the range extending from local to global [100, 287], the corresponding standardization varies. 6LowPAN, BLE are such examples. Application layer protocols used are CoAP, MQTT.

(i) ***Ultra-Short range*** Near-Field Communication (NFC) and RFID is used for healthcare based on the operating frequency range. The adaptability between RFID and NFC is analyzed by Bravo et al. [41]. NFC works for medium-range frequencies in the ISM band and RFID is used for high frequencies.

(ii) ***Short Range*** Bluetooth uses IEEE 802.15.1 [105]. Among 4 versions each one has an added feature. Bluetooth Low Energy (BLE)-Single mode has one protocol and provides low energy [37]. BLE Dual-mode has low power and uses Gaussian Frequency shift keying for range extension [42]. For power optimization, low baud rate, less channel usage, FHSS mode is used. Bluetooth 5.0 [229] has inherent range, data rate extensions, advertising extension features [66]. Its broadcasting message ability makes it suitable for IoT applications. Bluetooth security is vital in IoT [214, 226]. Safety of the IoT application depends on the technologies used.

(iii) ***Bluetooth, Zigbee*** [120] consumed low power but the area of coverage is less. Centenaro et al. used low power wide area network [45] to connect the node to the base station directly.

11 Threats due to IoT

Traditional security does not work with IoT Security. Recently in 2017, the data network of a well-known University was hacked. In healthcare, if IoMT devices were hacked [231], this could endanger the lives of patients. Industrial Utilities that depend on IIoT are at risk. If IoT sensors are compromised, massive compliance and legal issues would crop in. Unsecured gateways in an organization provides a pathway for cybercriminals.

IoT devices have less processing power and memory. So they are catastrophic and lack robust security protocols to protect themselves from threats. IoT devices are connected to the Internet. They are exposed to the hackers through webcams, mails, search engines, etc. It is not just devices, but also the protocols and networks that connect these devices to the Internet are exposed. There is no end-to-end encryption. There are no standards or procedures to ensure security in IoT. How often are the secret AES keys renewed in smart home automation [161]? Data collected from the sensor is sent to different devices and networks owned by different service providers. A webcam could take personal footages and stream the footages if hacked. A single error in code, could malfunction an automated industry. A skilled hacker could control a smart car.

IoT is a disruptive technology [208] with a lot of data. One sticking point in IoT is the insidious security risks. There are no serious security quality assurance checks in their

product development cycle. IoT enabled Mirai Botnet was developed in 2016 to combat threats against insecure IoT devices. With 5G, huge data, energy conservation, wideband is achievable at the cost of inflated infrastructure, health hazards due to waves, and impermeability to solid obstacles. These challenges [73] are insurmountable. Hash-based techniques and firewalls are used to secure RFID Tags. Artificial Intelligence could be used to identify the usage patterns and alert the user about abnormalities.

12 Mitigations

IoT must be secured from hardware, software, and OS. To prevent DoS (Denial-of-Service) Attack, DTLS and IPSec are used to verify the host address. These protocols are also used for authentication and encryption. Currently,existing routing protocols are insecure. Decentralized topology is preferred for mitigating threats. Applications, Management, and Data Analytics are decentralized using a distributed model referred to as Fog Computing [137, 173]. Object-based security with digital signatures is secured than peer-to-peer encryption [262]. The intrusion detection system (IDS) is required to prevent unauthorized access to IoT [153]. But these introduce challenges to power, bandwidth, and network. Legislations should be made mandatory as in Verizon for IoT [281]. Other issues of research are IoT mobility, Standardization, etc., with the integration of IoT in wearables. IoT is the thrust area vulnerable to cyber security threats in the near future.

Artificial Intelligence is providing promising solutions in IoT. IoT Security could be improved by a combination of government regulations, privacy controls, standards and AI. With Covid-19, IoT is widely adopted in IT, in industries as IIoT, in healthcare as IoMT and in many more. With less workforce there are more security breaches. With Covid-19, there is an increase in the usage of IoT, thereby resulting in increased cyber-attacks. Vendors are working on specific security solutions. Devices need to be authenticated. Network needs to be protected. Data needs to be encrypted and secured using API and PKI. Public Key Infrastructure policies is an effective solution to encrypt data using symmetric and asymmetric encryption. SSL along with asymmetric cryptography comes handy in providing end to end [14] encryption. Cryptographic algorithms like ECC with shorter key could be preferred than RSA. Server certificate could be verified before the data is sent from the sensor. Communication could be secured using encryption, AES 256 or TLS. IoT Security Analytics could be used rather than just securing the gateways from harmful threats. IoT network is protected with anti-malware, anti-virus, firewall, and intrusion prevention etc. IoT devices need to be protected by authentication.

13 IoT in Academics -Smart Academics Management

As an IoT application, an economical smart classroom was implemented.Smart classroom is a pivotal innovative tool for teaching. A prototype is set using raspberry pi and a raspberry pi camera to record lectures of faculties. Recorded lectures uploaded into the website could be accessed with a given username and a password provided for each student. The quality of education [234] is a vital demand in today's competitive setting. Technology has affected us in each facet. Intuitive categories are a progressive approach of education. Attendance could be taken by uploading a picture using IoT. Students presence in online classes could be monitored using IoT. Quality and Systematic

teaching is provided to the students. New teaching methodologies involve instructional material, 3D animated modules and videos.

(i) ***Implementation*** The Raspberry Pi module along with a 5MP color camera module is used for recording the lecture. Using Raspivid, lectures were recorded.Once recorded, the recorded video is uploaded using Raspbian software in a google drive as shown in Fig. 6.

This is accessible by the student using a username and a password. The website is designed for the students using XAMPP and PHP software. A database was created with the help of MySQL. The apache software in XAMPP can be used to generate the request and response for the website. The login credentials is the request and the output received is the response. If the entered username and password matches with the credentials stored in the database, then the user is redirected to the link where the materials are available. This application is useful during coronavirus (Covid-19) pandemic crisis as the students are not able to attend the classes in person.

(ii) ***Analysis*** Fig. 7 displays the user interface of the website. Students login and access to the drive are shown in Figs. 7 and 8 to watch the recordings.

These days everything is 'smart' starting from vehicles and homes to nanobots. The concept of IoT has played an important [132] role in our day to day life. Technology has immensely developed over a period of time and the real usage of this technology in academics is noticeable during the coronavirus (covid-19) pandemic situation. This eco-friendly concept would come in handy to students who miss their classes during unavoidable circumstances. The smart classroom is an enhanced sharing mode that improves teaching and learning opportunities by a group of students with limited resources.

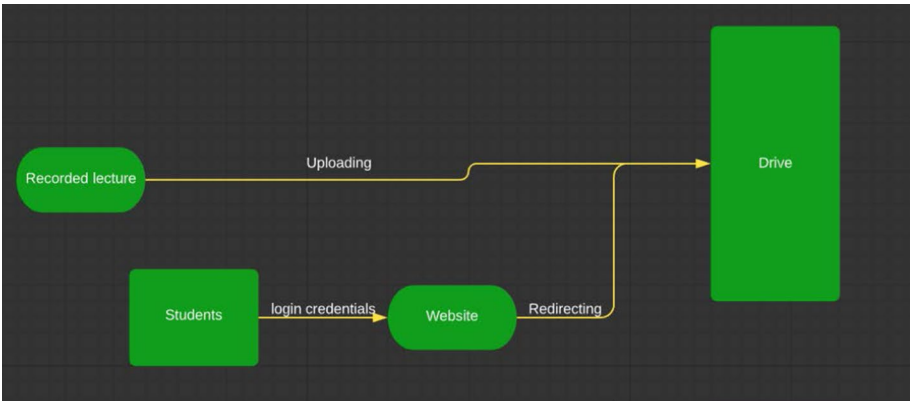
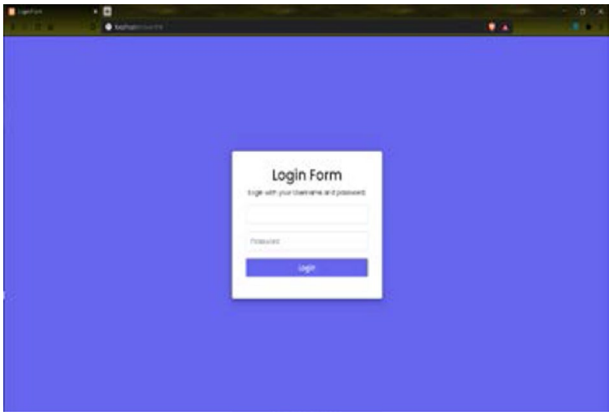


Fig. 6 Smart Academics

Fig. 7 User Interface



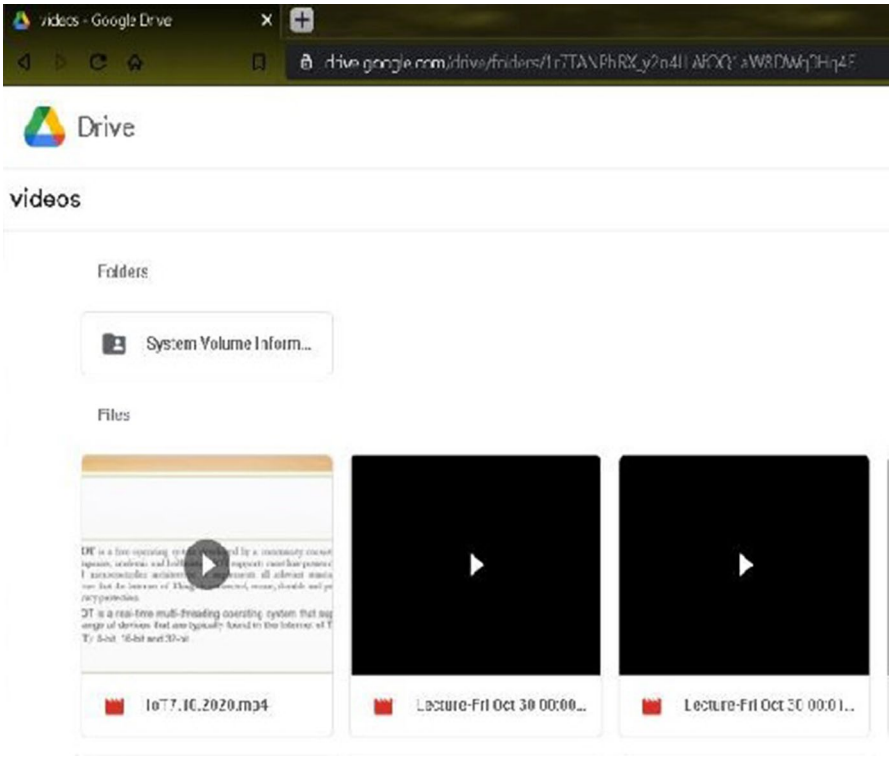


Fig. 8 Video Recording

14 Futuristic Research Inclinations

Information-centric network (ICN) [40] forms the future of IoT. IoT devices provide content. It targets content by name and not by location. It supports multicasting and mobility. It integrates network functionalities in the form of content rather than by location address

[295]. Challenges faced by IoT are at the technology level, communication and networking level, and intelligence level. Smart objects integration is done at the technology level. At the communication and networking level, challenges are involved in the networking and ubiquitous service provisions. Data fusion and service detection is done at the intelligence level. IoT cannot be globally deployed without a precise architecture. IoT-A –Architecture –seamlessly integrates heterogeneous devices. Handling heterogeneous devices is a major task. Effective measures are required to handle the increasing number of IoT devices and Big Data [180].Streaming is used for collecting the data from heterogeneous devices, process it, and make it available in real-time without latency [63, 203]. With proliferating wearable devices and mobiles, IoT is embarking towards personalized health care [152]. Intelligent algorithms are used for analyzing specific diseases. Mobile apps collect jogging activity, tracking [292], and life–logging data. These aspects along with specific algorithms are used in IoT personalized healthcare solutions [202]. IoT serves as a tool for quality education. [150]. IoT supports teaching and promotes academic performance. 5G and IoT will form the mobile broadband [127] in the future and thrive the growth of IIoT [141]. This flourishes the economic growth of the country. Human 4.0 augments human with features that are integrated with the neural system [237].This technology makes IoT fully autonomous with a foreseeable future. CloudIoT bridges Cloud and IoT and is gaining momentum [12]. Digitization improves economy, management control and provides hybrid solutions [86]. Forensic vigilance is required for smart cities. Digital Witness is collected with a privacy warranty [15]. Security depends on the data, location of data, tools [195] used to analyze data etc. Conjoining cloud forensics with client forensics, and logistical solutions are obtained for an Internet-of-Anything (IoA) Era, where swarms of resources are connected. Block Chain [239] provides viable de-centralized secured management solutions but hashing functions and the key could be compromised [193]. The Government is working towards standardization [271, 129, and 100]. Mohammad (2013) et al. [198] used user-centered tools such as Microsoft Gadgeteer to thrive interest in the user towards IoT. Future IoT would have recyclable materials, and power independent systems with embedded intelligence [136]. Future IoT architecture [293] should use narrowband and cater to hardware and software solutions [248]. IoT is deployed in e-Learning for virtual labs and the global library [34] to improve the teaching–learning process [185]. As a part of digital learning, M-Learning is in the earlier stage of research [297]. Internet of Medical Things (IoMT) is used to manage medical services [6] and healthcare workers by connecting medical devices and applications [80]. Information skills, communication skills, strategic skills [278], and content creation skills are required besides for IoT operability [276].

15 Conclusion

Internet-of-Things is a proven technology in the field of automation connecting the virtual world of intelligent objects to the real world of things. It generates and processes data from a lot of implanted devices. With increased connectivity, quality of life, optimized energy, time, cost, and labor, IoT improves by preventing unplanned downtime. Automation improves efficiency, connectivity, and integration [289]. With data-rich resources, newer innovations will burgeon. With IoT, comfort, local-to-global connectivity, eco-friendly support, quality of life, and safety increases. Hazardous ecosystems could be remotely controlled and monitored. Organizations connect the physical world (hardware) to the digital world (software, data analytics) and build an organizational structure to meet

the expectations. This article has a systematic insight into the contributions, pre-requisites, research challenges, and architectural design factors integrated into IoT for futuristic remedial measures. Companies need to shift from the traditional approach towards virtual IoT for satisfactory returns. We are heading towards a world where everything will be connected with IoT reaching escape velocity. IoT adds brain and provides the ability to communicate. IoT devices draw power from outlets or they are powered by batteries. This limitation could be thwarted by using IoT devices powering up from other sources of energy. To listen to a song, it is not necessary to have the song stored in the device. If the device is connected to a cloud and if we are able to play the desired song then it is a smart device. If we are planning for a flight travel and if the flight is cancelled, we might travel unnecessarily in worst environment conditions. But if we have an IoT device, if customized,we would get notification and we could avoid hurdles. After the coronavirus pandemic crisis, based on the virtual usage pattern and social distancing modes, prognostications reveal that IoT and Cloud usage in Education, Business, Healthcare, and Automation would cater to the need of the hour.

Author contribution Original.

Funding Not applicable.

Declarations

Conflicts of interest Not applicable.

Ethics approval Not applicable.

Consent to participate Yes.

Consent for publication Yes.

References

1. A brief history of internet of things. (2019). Creative Commons License. Available at http://postscapes.com/internet-of-things-history.
2. Abu-Elkheir, M., Hayajneh, M., & Ali, N. (2013). Data management for the internet of things: Design primitives and solution. *Sensors, 13*, 15582–15612.
3. Advanced Message Queuing Protocol (AMQP) 1.0 approved as an International Standard. (2012). OASIS Standard. Available: https://www.amqp.org/.
4. Adam Dunkels, Bjorn Gronvall, Voigt Thiemo. (2004). Contiki-a lightweight and flexible operating system for Tiny networked sensors. In 29th Annual IEEE International Conference on Local Computer Networks (LCN). IEEE, pp. 455–462. https://doi.org/10.1109/LCN.2004.38.
5. Aggarwal, R., Das, M.L. (2012). RFID security in the context of "internet of things". In Proceedings of the First International Conference on Security of Internet Things, ACM, pp. 51–56.
6. Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. (2019). Seclap: secure and lightweight RFID authentication protocol for medical IoT. *Future Generation Computer Systems, 101*, 621–634.
7. Agrawal, S., & Vieira, D. (2013). A survey on Internet of Things. *Abakós, 1*(2), 78–95.
8. MacDermott, Aine., Baker, Thar., Shi, Qi. (2018). IoT forensics: Challenges for the IoA Era. In 2018 9th IFIP International Conference on New Technologies, Mobility and Security. NTMS, IEEE, pp. 1–5.
9. Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the internet of things: communication technologies and challenges. *IEEE Access, 6*, 3619–3647.

10. Ala, A.-F., Mohsen, G., Meidi, M., Mohammed, A., & Moussa, A. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys and Tutorials., 17*, 2347–2376.
11. Colakovic, A., & Hadzialic, M. (2018). Internet of Things (IoT): A Review of enabling technologies, challenges and open research issues. *Computer Networks, 144*, 17–39.
12. Botta, A., De Donato, W., Porsico, V., & Perscape, A. (2016). Integration of cloud computing and internet of things: A Survey. *Future Generation Computer Systems, 56*, 684–700.
13. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing, 21*(2), 34–42.
14. An Application layer approach to End-to-End Security for the Internet of Things. (2019). OmaSpecWorks https://omaspecworks.org/an-application-layer-approach-to-end-to-end-security-for-the-internet-of-things/www.ipso-alliance.org
15. Nieto, A., Rios, R., & Lopez, J. (2018). IoT-forensics meets privacy: Towards cooperative digital investigations. *Sensors, 18*(2), 492.
16. 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.
17. Antonopoulos, A. M. (2014). *Mastering Bitcoin, Unlocking Digital Cryptocurrencies*. O'Reilly Media Inc.
18. Anthony Ricigliano. (2013). Disadvantages of Internet of Things. Available at http://anthonyricigliano.blogspot.com/2013/08/3-disadvantages-of-internet-of-things.html.
19. A quick history of IoT botnets. (2018). Radware, https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/.
20. Gardecki, A., et al. (2018). Innovative Internet of things –reinforced human recognition for human-machine interaction purposes. *International Federation of Automatic Control., 51*(6), 138–143.
21. Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on emerging topics in computing, 5*(4), 586–602.
22. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787–2805.
23. Asadullah, M., Raza, A. (2016). An overview of home automation systems. 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), IEEE, 2016, pp. 27–31.
24. Iqbal, A., Ullah, F., Anwar, H., Kwak, K. S., Imran, M., Jamal, W., & ur Rahman, A. (2018). Interoperable internet-of-things platform for smart home system using web of-objects and cloud. *Sustainable Cities and Society., 38*, 636–646.
25. Avi Itzkovitch, (2013). The Internet of Things and the Mythical Smart Fridge. Available at http://uxmag.com/articles.
26. AWS IoT. Available from: https://aws.amazon.com/iot/
27. Baccelli Emmanuel, Hahm Oliver, Gunes Mesut, Matthias Wahlisch, Thomas C. Schmidt, (2013). RIOT OS: Towards an OS for the internet of things. IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 79–80, https://doi.org/10.1109/INFCOMW.2013.6970748.
28. Mbarek, B., Ge, M., & Pitner, T. (2020). An efficient mutual authentication scheme for internet of things. *Internet of Things., 9*, 1094–1105.
29. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems., 78*, 659–676.
30. Alabsi, B. A., Anbar, M., & Anickam, S. (2018). A comprehensive review on security attacks in dynamic wireless sensor networks based on RPL protocol. *International Journal of Pure and Applied Mathematics., 119*(12), 12481–12495.
31. Bandyopadhyay, S., Sengupta, M., Maiti, S., & Dutta, S. (2011). Role of middleware for internet of things: A study. *International Journal of Computer Science and Engineering Survey., 2*(3), 94–105.
32. Bangui, H., Ge, M., Buhnova, B. (2018). Exploring big data clustering algorithms for internet of things applications. International Conference on Internet of Things, Big Data and Security, Springer, pp. 269–276.
33. Bassirou Diène, Joel J.P.C. Rodrigues, Ousmane Diallo,EL Hadji Malick Ndoye, Valery V. Korotaev, (2020). Data management techniques for Internet of Things. Mechanical Systems and Signal Processing 138.
34. Majid, B., Karol, L., & Mayra, L. (2017). IoT advantages on E-Learning in the smart cities. *International Journal of Development Research, 7*(12), 17747–17753.
35. Soret, B., Peterson, K. I., Jorgensen, N. T. K., & Lopez, V. F. (2015). Interference co- ordination for dense wireless networks. *IEEE Communications Magazine, 53*, 102–109.

36. Berrehili, F.Z., Belmekki, A. (2017). Privacy preservation in the internet of things. Proceedings of the Advances in Ubiquitous Networking (UNet'16). Springer, Singapore, pp. 163–175.
37. BLE, Smart Bluetooth low energy (Online): Availability: http://www.bluetooth.com/Pages/Bluetooth-Smart.aspx.
38. Biddlecombe E. (2005). UN Predicts Internet of Things. http://news.bbc.co.uk/2/hi/technology/4440334.stm.
39. Bonomi, F., Milito, R., Zhu, J., Addepalli, S. (2012). Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ACM, 2012, pp. 13–16.
40. Nour, B., Sharif, K., Li, F., Biswas, S., Moungla, H., Guizani, M., & Wang, Y. (2019). A survey of internet of things communication using ICN: A use case perspective. *Computer Communications, 142*, 95–123.
41. Bravo, J., Hervas, R., Nava, S.W., Chavira, G., Sanchez, C., (2007). Towards natural interaction by enabling technologies: a near field communication approach. In: European Conference on Ambient Intelligence. Springer, 11, pp. 338–351
42. Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors, 12*, 11734–11753.
43. Casavant, T. L., & Kuhl, J. G. (1988). A taxonomy of scheduling in general-purpose distributed computing systems. *IEEE Transactions on Software Engineering, 14*(2), 141–154.
44. Cella, C.H., Duffy, G.W., McGuckin, J.P., Desai, M. (2019). WO/2019/094721-Methods and systems for the industrial internet of things, https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2019094721.
45. Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communication, 23*(5), 60–67.
46. Sanin, C., Haoxi, Z., Imran Shafiq, Md., Waris, M., Silva, C., de Oliveira, E., & Szczerbicki,. (2019). Experience based knowledge representation for internet of things and cyber physical systems with case studies. *Future Generation Computer Systems, 92*, 604–616.
47. Charalampos Doukas, (2012). Building Internet of Things with the Arduino. ACM Available at http://www.buildinginternetofthings.com/.
48. Withanage, Chathura., Ashok, Rahul., Yuen, C., Otto, K. (2014). A comparison of the popular home automation technologies. In: innovative smart grid technologies-Asia (ISGT Asia), IEEE, pp. 600–605. https://doi.org/10.1109/ISGT-Asia.2014.6873860.
49. Chayan Sarkar, S. N., Nambi, A. U., Venkatesha Prasad, R., Rahim, A., Neisse, R., & Baldini, G. (2015). DIAT: a scalable distributed architecture for IoT. *IEEE Internet of Things, 2*(3), 230–239.
50. Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy R. Leschke (2017). Potential forensic analysis of IoT Data: An overview of the state-of-the-art and future possibilities. Proceedings In: 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), IEEE, pp.705–710.
51. Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2018). Internet of things forensics: The need, process models, and open issues. *IT Professional, 20*, 40–49.
52. Zhu, C., Leung, V. C. M., Shu, L., & Ngai, E.-H. (2015). Green internet of things for smart world. *IEEE Access, 3*, 2151–2162.
53. Cichonski, J., Franklin, J.M., Bartock, M. (2017). Guide to LTE security. NIST Computer Security.
54. CISCO, (2014). The internet of things reference model. White Paper, June 2014.
55. Columbus L. (2015). Roundup of internet of things forecasts and market estimates. Forbes, December 7.
56. Compton, K., & Hauck, S. (2002). Reconfigurable computing: a survey of systems and software. *ACM Computing Surveys (CSUR), 34*(2), 171–210.
57. Deugd, D. S., Carroll, R., Kelly, K., Millett, B., & Ricker, J. (2006). SODA: Service oriented device architecture. *IEEE Pervasive Computing, 5*(3), 94–96.
58. Dhananjay Singh, Gaurav Tripathi, Anto J. Jara, (2014). A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services. In: Proceedings of IEEE World Forum on Internet of Things, At Seoul, pp. 287–292.
59. Dan Vargas, (2016). How the Internet of Things is driving cost-saving efficiencies for manufacturers. Big data hardware solutions, Available from: https://blog.shi.com/hardware/internet-things-driving-cost-savingefficiencies-manufacturers/

60. Dave Evans, (2011). The Internet of Things: How the Next Evolution of the Internet is Changing Everything. Cisco IBSG © 2011.
61. Dave Thaler, (2015). Architectural Considerations in Smart Object Networking. IETF RFC 7452.
62. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry, (2017). IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things. (Cisco Press, 2017).
63. Corral-Plaza, D., Medina-Bulo, I., Ortiz, G., Boubeta-Puig, J., & UCASE Software Engineering Research Group. (2020). A stream processing architecture for heterogeneous data sources in the Internet of Things. Computer Standards and Interfaces 70, 103426.
64. (DDS) Data distribution services (2015), Version 1.4, Object Management Group (OMG), April 2015.
65. Diaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99–117.
66. Di Marco, P., Skillermark, P., Larmo, A., Arvidson, P., & Chirikov, R. (2017). Performance evaluation of the data transfer modes in Bluetooth 5. *IEEE Communication Standards Magazine, 1*(2), 92–97.
67. Di Martino, B., Rak, M., Ficco, M., Esposito, A., Maisto, S. A., & Nacchia, S. (2018). Internet of things reference architectures, security and interoperability: A survey. *Internet of Things, 1*(2), 99–112.
68. Dinesh Thangavel, M. Xiaoping, Alvin Valera, T. Hwee-Xian, Colin Keng-Yan Tan (2014) Performance evaluation of MQTT and CoAP via a common middleware. IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks, Singapore, 2014, pp. 1–6
69. Disadvantages of internet of things, available at https://sites.google.com/a/cortland.edu/...internet-ofthings/disadvantages.
70. Dominique Guinard, Iulia Ion, Simon Mayer, (2012). In search of an Internet of things service architecture –REST or WS –A Developer's Perspective. Mobile and Ubiquitous Systems: Computing, Networking and Services. Springer, Berlin, Heidelberg, pp.326–337.
71. Dominik Bilgeri, Veronika Brandt, Marco Lang, Jan Tesch, Markus Weinberger, (2015). The IoT business model builder. A White Paper of the Bosch IoT Lab in collaboration with Bosch Software Innovations GmbH, 2015
72. Dominik Bilgeri, Felix Wortmann, Elgar Fleisch, (2017) How digital transformation affects large manufacturing companies organization.
73. Edward. T. Chen, (2017). The Internet of things: Opportunities, issues, and challenges. In: The Internet of Things in the Modern Business Environment. IGI Global, pp. 167–187.
74. Elena-Lenz. (2013). Internet of Things: Six Key Characteristics Available at http://designmind.frogdesign.com/blog/internet-of-thingssix-key-characteristics.html
75. Elkhodr Mahmoud, Shahrestani, S., Cheung, H., (2013). The internet of things: vision and challenges. TENCON Spring Conference, pp. 218–222.
76. Soltanmohammadi, E., Ghavami, K., & Pour, M. N. (2016). A survey of traffic issues in machine-to-machine communications over LTE. *IEEE Internet of Things Journal, 3*(6), 865–884.
77. Eshita Rastogi, Navrati Saxena, Abhishek Roy, Dong Ryeol Shin, (2020). Narrowband internet of things: A comprehensive study. Computer Networks 173.
78. Evanson Mwangi Karanja, Shedden Masupe, Mandu Gasennelwe Jeffrey, (2020). Analysis of internet of things malware using image texture features and machine learning techniques . Internet of Things 9.
79. Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, (2017). Internet of things security: A survey. Journal of Network and Computer Applications, 10–28.
80. Faisal, A., Abdullah, A., Vivek, S., & Sajjan, S. (2019). IoMT-SAF: Internet of medical things security assessment framework. *Internet of Things, 8*, 100–123.
81. Fang, X., Misra, S., Xue, G., Yang, D. (2011). Smart Grid–The New and Improved Power Grid: A Survey. IEEE Communications Surveys and Tutorials, pp. 1–37.
82. Firouzi, F., Farahani, B., Weinberger, M., DePace, G., & Aliee, F. S. (2020). *IoT Fundamentals: Definitions, Architectures, Challenges, and Promises*. Springer.
83. Firouzi, F., Farahani, B., Ibrahim, M., & Chakrabarty, K. (2018). From EDA to IoT eHealth: Promises, challenges, and solutions. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 37*(12), 2965–2978.
84. Fernandes, E., Rahmati, A., Jung, J., & Prakash, A. (2017). Security implications of permission models in smart-home application frameworks. *IEEE Security & Privacy, 15*(2), 24–30.
85. FIWARE. Available from: https://www.fiware.org/
86. Fleisch, E., Weinberger, M., Wortmann, F. (2014). Business Models and the Internet of Things. Bosch IoT Lab Whitepaper (Bosch Internet of Things and Services Lab, 2014).

87. Fleisch, E., et al. (2016). Revenue models and the internet of things? A Consumer IoT-based Investigation. ETH Zurich.
88. Flynn, M. J. (1966). Very high-speed computing systems. *Proceedings of the IEEE, 54*(12), 1901–1909.
89. Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation, 28*, 22–29.
90. Federica Paganelli, David Parlanti, (2012). A DHT-based discovery service for the Internet of Things. Journal of Computer Networks and Communication.
91. Gama, K., Wanderley, R., Maranhao, D., Garcia, V.C. (2015). A web-based platform for scavenger hunt games using the Internet of Things. In: Proc 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), 2015, 597–598.
92. Gan, G., Lu, Z., Jiang, J. (2011). Internet of things security analysis. In: IEEE International Conference on Internet Technology and Applications (iTAP), pp. 1–4.
93. Gartner, (2017) Gartner Top 10 Technology Trends. https://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017.
94. Ge, M., Bangui, H., & Buhnova, B. (2018). Big data for internet of things: A survey. *Future Generation Computer Systems, 87*, 601–614.
95. Giancarlo Fortino, Wilma Russo, and Claudio Savaglio, (2017). Simulation of Agent-oriented Internet of Things Systems. Proceedings in 2016 Federal conference on Computer Science and Information Systems.
96. Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2017). Enabling IoT interoperability through opportunistic smartphone based mobile gateways. *Journal of Network and Computer Applications, 81*, 74–84.
97. Gill, S.S., Chana, I., Singh, M., Buyya, R. (2019). RADAR: self-configuring and self-healing in resource management for enhancing quality of cloud services. Concurrency and Computation Practice and Experience, 31(1)
98. Gentili, M., Sannino, R., & Petracca, M. (2016). BlueVoice: Voice communications over bluetooth low energy in the internet of things scenario. *Computer Communications, 89*, 51–59.
99. Glikson, A., Nastic, S., Dustdar, S. (2017). Device less edge computing: extending server less computing to the edge of the network. In: Proceedings of the 10th ACM International Systems and Storage Conference, ACM, 2017, pp. 28.
100. Global Information Infrastructure, Internet protocol aspects and next-generation networks, Next Generation Networks–Frameworks and Functional Architecture Models: Overview of the Internet of Things. (2012). ITU-T Recommendation Y.2060 Series Y.
101. Gluhak Alexander, Srdjan Krco, Michele Nati , Dennis Pfisterer , Nathalie Mitton , Tahiry Razafindralambo, (2011). A Survey on facilities for experimental Internet of Things research. IEEE Communication Magazine, pp. 58–67.
102. Google Trends, Explore, http://www.google.com/trends/explore?hl=en-US#q=internet+of+things.
103. Gonzalez, G.R., Organero, M.M., Kloos, C.D. (2008). Early infrastructure of an internet of things in spaces for learning. In: Advanced Learning Technologies, 2008. ICALT'08. Eighth IEEE International Conference on. IEEE, pp. 381–383.
104. Gorman, B. L., Resseguie, D. R., & Tomkins-Tinch, C. (2009). Sensorpedia: Information sharing across incompatible sensor systems. In 2009 International Symposium on Collaborative Technologies and Systems (pp. 448-454). IEEE.
105. Gragopoulos, I., Tsetsinas, I., Karapistoli, E., & Pavlidou, F.-N. (2008). FP-MAC: A distributed MAC algorithm for 802.15. 4-like wireless sensor networks. *Ad Hoc Networks, 6*(6), 953–969.
106. Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the internet of things: Challenges, threats and solutions. *Internet of Things, 5*, 41–70.
107. Gubbi Jayavardana, Buyya Rajkumar, Marusic Slaven, Palaniswami Marimuthu, (2013). Internet of Things (IoT): a Vision, Architectural Elements, and Future directions . Future Generation Computer Systems, pp. 1645–1660.
108. Gupta, A., & Jha, R. K. (2015). A survey of 5G network: Architecture and emerging technologies. *IEEE Access, 3*, 1206–1232.
109. H2020 –UNIFY-IoT Project, Supporting Internet of Things Activities on Innovation Ecosystems (2016) (Online). Available: http://www.unify-iot.eu/wp-content/uploads/2016/10/D03_01_WP02_H2020_UNIFY-IoT_Final.Pdf.
110. Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. *Journal of Network and Computer Applications, 154*, 102538.
111. 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.

112. Hsieh, H. C., Chang, K. D., Wang, L. F., Chen, J. L., & Chao, H. C. (2015). ScriptIoT: A script framework for and internet-of-things applications. *IEEE Internet of Things Journal, 3*(4), 628–636.
113. Haller, S., Karnouskos, S., & Schroth, C. (2008). The internet of things in an enterprise context. *Future Internet Symposium, Springer, 2008*, 14–28.
114. Haritha, C. B., & Nagajayanthi, B. (2018). VLSI based enhanced security algorithm for IoT. *International Journal of Pure and Applied Mathematics, 120*(9), 249–257.
115. Haselsteiner, E., Breitfuß, K. (2006). Security in near field communication (NFC). In: Workshop on RFID security, pp. 1–11.
116. He, L., Yan, Z., & Atiquzzaman, M. (2018). LTE/LTE- A network security data collection and analysis for security measurement: A survey. *IEEE Access, 6*, 4220–4242.
117. Hewlett Packard, (2015) Internet of things research study.
118. Hogan, M., Piccarreta, B. (2018). NIST Interagency Report (NISTIR) 8200 Interagency Report on the status of international cybersecurity standardization for the Internet of Things (IoT), https://csrc.nist.gov/publications/detail/nistir/8200/draft. Accessed on August 2018.
119. Ma, H.-D. (2011). Internet of things: Objectives and scientific challenges. *Journal of Computer Science and Technology., 26*(6), 919–924.
120. Kai, H. Y., Chun, P. A., & Nien, H. H. (2009). A comprehensive analysis of low-power operation for beacon-enabled IEEE 802.15. 4 wireless networks. *IEEE Transactions on Wireless Communications, 8*(11), 5601–5611.
121. Akyildiz, I. F., Nie, S., Chun, S., & Lin, M. C. (2016). 5G roadmap: 10 key enabling technologies. *Computer Networks, 10*, 17–48.
122. Ian, F., Akyildiz, W., Su, Y., & Sankarasubramaniam, E. C. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*, 393–422.
123. Hashema, I. A. T., Chang, V., Anuar, N. B., Adewolea, K., Yaqooba, I., Gani, A., Ahmeda, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management, 36*(5), 748–758.
124. Mashal, I., Alsaryrah, O., Chung, T. Y., Yang, C. Z., Kuo, W. H., & Agrawal, D. P. (2015). Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks, 28*, 68–90.
125. Yaqoob, I., Hashem, I. A. T., Arif Ahmed, S. M., Kazmi, A., & Hong, C. S. (2019). Internet of things forensics: recent advances, taxonomy, requirements and open challenges. *Future Generation Computer Systems, 92*, 265–275.
126. Fette, I., Melnikov, A. (2011). The WebSocket protocol, IETF RFC 6455 (December) (2011). (Online). Available https://tools.ietf.org/html/rfc6455.
127. IMT Vision, (2015). Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU-R Recommendation M.2083–0.
128. Information Matters data driven innovation news and analysis, Data driven innovation newsletter, http://informationmatters.net/internet-of-things-statistics/
129. Information Processing Systems (1989). – Open Systems Interconnection – Basic Reference Model - Part 2: Security Architecture.
130. In Lee, (2019). The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things, Vol.7.
131. Intelligent IoT. Available from: https://www2.deloitte.com/insights/us/en/focus/signals-forstrategists/intelligent-iot-internet-of-things-artificial-intelligence.html
132. International Telecommunications Union (2005). ITU Internet Reports 2005: The Internet of Things. Available at www.itu.int/internetofthings/
133. Internet of Things, Available at http://en.wikipedia.org/wiki/Internet_of_Things
134. Internet of Things –IoT Standards-ETSI-https://www.etsi.org/technologies/internet-of-things.
135. Internet of Things World Forum. Available from: https://www.iotwf.com/
136. Internet of Things in (2020). A Roadmap for the future. INFSO D.4 networked enterprise and RFID INFSO G.2 Micro & Nano systems, Co-operation with the RFID Working Group of the ETP EPOSS Version 1.1, 27 May, 2008.
137. Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N., & Mahmoudi, C. (2018). Fog computing conceptual model: Recommendations of the National Institute of Standards and Technology. *NIST Special Publications*. https://doi.org/10.6028/NIST.SP.500-325
138. IoT-A (Internet-of-Things Architecture), Initial Architectural Reference Model for IoT. (2011). Project Deliverable D1.2.
139. IoT Device Security: Built-In, Not Bolt-On, NXP Semiconductors, (2018). http://www.digi.com/pdf/digi-IoT-device-security-nxp-wp.pdf.
140. IoT Tutorial for beginners, https://www.guru99.com/iot-tutorial.html

141. I-Scoop, (2018). 5G and IoT in 2018 and beyond: the mobile broadband future of IoT. (Available on line 14 Jan 2018), https://www.i-scoop.eu/internet-of-things-guide/5g-iot/
142. ISO/IEC JTC 1-'Internet of Things (IoT). - ISO/IEC JTC 1 Information Technology, (2014). Preliminary Report.
143. ITU 2020, (2020). ITU-T: Global standards for the Internet of Things. https://www.itu.int/en/ITU-T/techwatch/Pages/internetofthings.aspx
144. Jaiswal, N., Analysys Mason, (2018). 5G: Continuous evolution leads to quantum shift. Available on line 14 Jan 2018. https://www.telecomasia.net/content/5gcontinuous-evolution-leads-quantum-shift.
145. Andrews, J. G. (2013). Seven ways that HetNets are a cellular paradigm shift. *IEEE Communications Magazine, 51*(3), 136–144.
146. Jia, X., Feng, Q., Fan, T., Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). In: 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012. IEEE, pp. 1282–1285.
147. Jia, Yu., & Buyya, R. (2005). A taxonomy of workflow management systems for grid computing. *Journal of Grid Computing, 3*, 171–200.
148. Jithin Jagannath, Nicholas Polosky, Anu Jagannath , Francesco Restuccia , and Tommaso Melodia, (2019). Machine Learning for Wireless Communications in the Internet of Things: A Comprehensive Survey. AdHoc Networks.
149. Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet Things Journal, 1*, 3–9.
150. Jorge G´omez, Juan F. Huete, Oscar Hoyos, Luis Perez, Daniela Grigori, (2013). Interaction System Based on Internet of Things as Support for Education. Proceedings In :The 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2013), Procedia Computer Science 21, pp.132 – 139.
151. Juels Ari, Rivest, R.L., Szydlo, M. (2003). The blocker tag: selective blocking of RFID tags for consumer privacy. Proceedings of the 10th ACM Conference on Computer and Communications Security. ACM, pp. 103–111.
152. Qi, J., Yang, P., Min, G., Amft, O., Dong, F., & Xu, L. (2017). Advanced internet of things for personalised healthcare systems: A survey. *Pervasive and Mobile Computing, 41*, 132–149.
153. Junaid Arshad , Muhammad Ajmal Azad , Roohi Amad , Khaled Salah , Mamoun Alazab and Razi Iqbal, (2020). A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics 2020 9(629).
154. Keoh, S., Kumar, S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. *IEEE Internet of Things Journal, 1*(3), 265–275.
155. Kevin Ashton, (2009). That 'Internet of Things' Thing. RFID Journal, Available at http://www.rfidjournal.com/articles/view?4986.
156. Khattab, A., Jeddi, Z., Amini, E., & Bayoumi, M. (2017). RFID Security A Light Weight Paradigm. *Springer, 2017*, 1–162.
157. Khan Rafiullah, Sarmad UllahKhan, Rifakhat Zaheer, and Shahid Khan, (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT '12), pp.257–260.
158. Kitsos, P., Sklavos, N., Parousi, M., & Skodras, A. N. (2012). A Comparative study of hardware architectures for lightweight block ciphers. *Computers and Electrical Engineering, 38*(1), 148–160.
159. Kim, M., Ahn, H., & Kim, K. P. (2016). Process-aware internet of things: a conceptual extension of the internet of things framework and architecture. *KSII Transactions on Internet and Information Systems (TIIS), 10*(8), 4008–4022.
160. Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, IEEE, 2016, pp. 839–858.
161. Kumar, P., Braeken, A., Gurtov, A. V., Iinatti, J. H., & Ha, P. H. (2017). Anonymous secure framework in connected smart home environments. *IEEE Transactions on Information Forensics and Security, 12*(4), 968–979.
162. Kuyoro, S., Osisanwo, F., Akinsowon, O., (2015). Internet of things (IoT): an overview. In: 3rd International Conference on Advances in Engineering Sciences and Applied Mathematics, pp. 53–58.
163. Lasc, I., Dojen, R., & Coffey, T. (2011). Countering jamming attacks against an authentication and key agreement protocol for mobile satellite communications. *Computers & Electrical Engineering, 37*(2), 160–168.

164. Levis, P., Madden, S., Polastre, J., Szewczyk, R., Whitehouse, K., Woo, A., Gay, D., Hill, J., Welsh, M., Brewer, E., et al. (2005). TinyOS: An operating system for sensor networks. In: Ambient Intelligence. Springer, pp. 115–148, https://doi.org/10.1007/3-540-27139-2_7.
165. Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on industrial informatics, 10*(4), 2233–2243.
166. Da Xligu, Li., & Wang, X. (2013). Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. *IEEE Transactions on Industrial Informatics, 9*(4), 2177–2186.
167. Hsien-Tang, L. (2013). Implementing smart homes with open source solutions. *International Journal of Smart Home, 7*(4), 289–296.
168. Li, J., Shvartzshnaider, Y., Francisco, J.A., Martin, R.P., Raychaudhuri, D. (2012). Enabling internet-of-things services in the mobility first future internet architecture. In: Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM).
169. Li, Jun, Zhang, Y., Chen, Y.F., Nagaraja, K. (2013). A mobile phone based WSN infrastructure for IoT over future internet architecture. In: Proceedings of IEEE International Conference on and IEEE Cyber, Physical and Social Green Computing and Communications (GreenCom), pp. 426–433.
170. Li, L. (2013). Technology designed to combat fakes in the global supply chain. *Business Horizons, 56*(2), 167–177.
171. Luo, H., Wen, G., Su, J., & Huang, Z. (2018). Slap: Succinct and lightweight authentication protocol for low-cost RFID system. *Wireless Networks, 24*(1), 69–78.
172. Lu Tan, Neng Wang, (2010). Future internet: The Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), IEEE, Chengdu, China, pp. 376–380.
173. Madsen, H., Albeanu, G., Burtschy, B., Popentiu-Vladicescu F. (2013). Reliability in the utility computing era: towards reliable fog computing. In: Proceedings of the International Conference on Systems, Signals and Image Processing, 2013, pp. 43–4
174. Noura, M., Atiquzzaman, M., & Gaedke, M. (2018). Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications, 24*(3), 796–809.
175. Fahmideh, M., & Zowghi, D. (2020). An exploration of IoT platform development. *Information Systems, 87*, 101409.
176. Mahdi. H. Miraz, Maaruf Ali, (2018). A Review on Internet of Things (loT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). Internet Technologies and Applications (ITA), pp. 219–224.
177. Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The internet of things: New interoperability, management and security challenges. *International Journal of Network Security and its Applications, 8*(2), 85–102.
178. Mahmud Hossain, M., Fotouhi, Maziar., Hasan, Ragib., (2015). Towards an Analysis of security issues, challenges, and open problems in the Internet of Things. Proceedings In: World Congress on Services, IEEE pp. 21–28.
179. Mainetti, L., Patrono, L., Vilei, A. (2011). Evolution of wireless sensor networks towards the internet of things: a survey. In: Software, Telecommunications and Computer Networks (SoftCOM), 2011, 19th International Conference on. IEEE, pp. 1–6.
180. Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications, 67*, 99–117.
181. Margery Conner, (2010). Sensors empower the Internet of Things. EDN. Available at https://www.edn.com/sensors-empower-the-internet-of-things/
182. Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis, (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. IEEE Communications Surveys & Tutorials.
183. Maria Rita Palattella, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, Latif Ladid, (2016). Internet of Things in the 5G Era: Enablers, Architecture and Business models. IEEE Journal on Selected Areas in Communication, pp. 510–527.
184. Palattella, M. R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L. A., Boggia, G., & Dohler, M. (2012). Standardized protocol stack for the internet of (Important) things. *IEEE Communications Survey and Tutorials, 15*(3), 1389–1406.
185. Marquez, J., Villanueva, J., Solarte, Z., Garcia, A. (2016). IoT In Education: Integration of objects with virtual academic communities. In: New advances in information systems and technologies. Springer, 2016. p. 201–12.
186. Massimo Condoluci, Giuseppe Araniti, Toktam Mahmoodi, and Mischa Dohler, (2016). Enabling the IoT machine age with 5G: machine-type multicast services for innovative real-time applications. IEEE Access, pp.5555–5569.

187. Mbarek, B., Ge, M., Pitner, T. (2019). Self-adaptive RFID authentication for Internet of Things. In: International Conference on Advanced Information Networking and Applications, Springer, pp. 1094–1105.
188. Meddeb, A. (2016). Internet of things standards: Who stands out from the crowd? *IEEE Communications Magazine, 54*(7), 40–47.
189. Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B., & Gupta, B. B. (2018). An Efficient Algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems, 83*, 619–628.
190. Michael Chui, Markus Löffler, Roger Roberts, (2010). The Internet of Things. McKinsey and Company.
191. Michelle Selinger, Ana Sepulveda and Jim Buchan, (2013). Education and the Internet of Everything. Cisco Consulting Services and Cisco EMEAR Education Team.
192. Microsoft Azure IoT. Available from: https://azure.microsoft.com/en-us/services/iot-hub/
193. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future generation computer systems, 82*, 395–411.
194. Mirai botnet adds three new attacks to target IoT devices. (2018). https://www.zdnet.com/article/mirai-botnet-adds-three-new-attacks-to-target-iot-devices/
195. Mohamad Noor, M. B., & Hassan, W. H. (2019). Current research on internet of things (IoT) security: A survey. *Computer Networks, 148*, 283–294.
196. Feki, M. A., Kawsar, F., Boussard, M., & Trappeniers, L. (2013). The internet of things: The next technological revolution. *Computer, 46*, 24–25.
197. Mohamed El Beqqal, M. Azizi, (2017). Classification of major security attacks against RFID systems. International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), IEEE, 2017, pp. 1–6.
198. Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh, Farhad Norouzi, (2020). Towards the internet of things. Springer Innovations in Communication and Computing, pp.9–31.
199. Morchon, O.G., Rietman, R., Sharma, S., Tolhuizen, L., Arce, J.T. (2016). A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO. In: Algorithms for Sensor Systems. Lecture Notes in Computer Science 9536, 112–128.
200. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A Review of smart home applications based on internet of things. *Journal of Network and Computer Applications, 97*, 48–65.
201. Nabil Benamar, Antonio Jara, Latif Ladid, Driss. E. Ouadghiri, (2014). Challenges of the Internet of Things: IPv6 and network management. In: Proc. Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing 1, 328–333.
202. Nagajayanthi, B., Radhakrishnan, R., & Vijayakumari, V. (2015). Healthcare IoT-A Multilayer security mechanism using linear programmable pre-coded matrix decomposition method. *International Journal of Applied Engineering Research., 10*(24), 44554–44563.
203. Nagajayanthi, B, Vijayakumari, V., Radhakrishnan R, (2016) Secured Seamless Broadcasting Using Bluetooth Enabled IoT Cloud. Research Journal of Applied Sciences Engineering and Technology. Maxwell Scientific Publication Corporation. 13(4), 325–330.
204. Nagajayanthi, B. (2019). Energy Efficacious IoT Based Nifty Parking Information System. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9*(3), 3151–3156.
205. Nagajayanthi, B. (2020). Energy efficient light weight security algorithm for low power IoT devices. *International Journal of Engineering and Advanced Technology, 9*(3), 45–50.
206. Naija, Y., Beroulle, V., & Machhout, M. (2018). Security enhancements of a mutual authentication protocol used in a HF full-fledged RFID tag. *Journal of Electronic Testing, 34*(3), 291–304.
207. Nakamoto S. (2008). Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
208. National Intelligence Council, Disruptive Civil Technologies — Six Technologies with Potential Impacts on US Interests Out to 2025— Conference Report CR 2008–07, April 2008, Available at www.dni.gov/nic/NIC_home.html.
209. NIST. Information Technology, Available at https://www.nist.gov/topics/internet-things-iot
210. Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., Gomez, C. (2015). IPv6 over Bluetooth Low Energy. RFC 7668. https://rfc-editor.org/rfc/rfc7668.txt.
211. OASIS Standard. MQTT Specification, (2014). Version 3.1.1.
212. Hahm, O., Baccelli, E., Petersen, H., & Tsiftes, N. (2016). Operating systems for low-end devices in the Internet of things: A Survey. *IEEE Internet of Things Journal, 3*(5), 720–734. https://doi.org/10.1109/JIOT.2015.2505901

213. Oxford Dictionaries, (2017). January (Online). Available http:// www.oxforddictionaries.com/us/definition/American_English/Internet-of-things.
214. Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., Scarfone, K. (2017). Guide to Bluetooth Security. NIST Special Publication 800–121 Revision 2, 2017.
215. Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols and applications. *Journal of Electrical and Computer Engineering, 2017*, 1–25.
216. Parashar, R., Khan, A., & Neha, A. K. (2016). A survey: The internet of things. *International Journal of Technical Research and Applications, 4*(3), 251–257.
217. Kamgueu, P. O., Nataf, E., & Ndie, T. D. (2018). Survey on RPL enhancements: A focus on topology, security and mobility. *Computer Communications, 120*, 10–21.
218. Perez, A. J., Zeadally, S., & Cochran, J. (2018). A Review and an Empirical analysis of privacy policy and notices for consumer Internet of Things. *Security and Privacy, 1*(3), e15.
219. Pethuru Raj, Anupama.C. Raman, (2017). The Internet of Things: Enabling Technologies, Platforms, and Use Cases. Auerbach Publications.
220. de Boer, P. S., Van Alexander, J. A. M., Deursen, T. J. L., & Rompay, V. (2019). Accepting the internet-of-things in our homes: The role of user skills. *Telematics and Informatics, 36*, 147–156.
221. J. Postel, (1980). User datagram protocol. IETF RFC 768 (August) (1980). (Online). Available https://www.ietf.org/rfc/rfc768.txt.
222. Bhoyar, P., Parul Sahare, S. B., & Dhok, R. B. D. (2019). Communication technologies and security challenges for internet of things: A comprehensive review. *International Journal of Electronics and Communication (AEÜ), 99*, 81–99.
223. Haasan, Q. F., Khan, A. U. R., & Madani, S. A. (2018). *Internet of Things –Challenges, Advances and Applications*. CRC Press, Computer and Information Science Series, Taylor and Francis Group.
224. Rappaport, T.S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., Wong, G.N., Schulz, J.K., Samimi, M., Gutierrez, F. (2013). Millimeter wave mobile communications for 5g cellular: It will work! . IEEE Access, pp.335–349, https://ecfsapi.fcc.gov/file/60001013348.pdf.
225. Rasouli, H., Kavian, Y. S., & Rashvand, H. F. (2014). ADCA: Adaptive duty cycle algorithm for energy efficient IEEE 802.15. 4 beacon-enabled wireless sensor networks. *IEEE Sensors Journal, 14*(11), 3893–3902.
226. Ravikiran, H.V. (2018). Security considerations for bluetooth smart devices. http://www.design-reuse.com/articles/39779/security-considerations-for-bluetooth-smart-devices.html.
227. Ray, B. R., Chowdhury, M., & Abawajy, J. (2013). Hybrid approach to ensure data confidentiality and tampered data recovery for RFID tag. *International journal of networked and distributed computing, 1*(2), 79–88.
228. Ray, P. P. (2018). A survey on internet of things architectures. *Journal of King Saud University Computer and Information Sciences, 30*, 291–319.
229. Ray, P.P., Agarwal, S. (2016). Bluetooth 5 and internet of things: Potential and architecture. In: 2016 International conference on Signal Processing, Communication, Power and Embedded System (SCOPES). IEEE; 2016, pp.1461–5.
230. Rayes Ammar, Salam, Samer (2017). Internet of Things—From Hype to Reality-The road to Digitization. River Publisher Series in Communications, Springer, Denmark. pp. 49. https://www.amazon.de/Internet-Things-Hype-Reality-Digitization/dp/3319448587.
231. Rahmani, A. M., Gla, T. N., Negash, B., Anzanpour, A., & Azimi, I. (2018). Exploiting smart e-Health gateways at the edge of healthcare internet-of-things: A fog computing approach. *Future Generation Computer Systems, 78*, 641–658.
232. Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi , Alexis Olivereau , Alexandru Serbanati, Michele Rossi, (2014). Secure Communication for Smart IoT Objects: Protocol Stacks, Use Cases and Practical Examples. World of Wireless, Mobile and Multimedia Networks (WoW-MoM), 2012 IEEE, 1–7.
233. Rimal, B.P., Choi, E., Lumb, I. (2009). A Taxonomy and survey of cloud computing systems. In: Proceedings of the Fifth International Joint Conference on INC, IMS and IDC (NCM'09), IEEE, 2009, pp. 44–51.
234. Robert Lutz, (2014). The Implications of the Internet of Things for Education. Available at http://www.systech.com/systech-blog/384-theimplications-of-the-internet-of-things-for-education.
235. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.
236. Roundup of Internet of Things Forecasts. Available from: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#6a7ab8041480
237. Rustam Pirmagomedov, Yevgeni Koucheryavy, (2019). IoT technologies for Augmented Human: A survey. Internet of Things.
238. Salman Tara, Raj Jain, (2019). A Survey of protocols and standards for Internet of Things. CoRR (2019).

239. Samaniego, M., Deters, R. (2016). Blockchain as a service for IoT. In: Proceedings of the 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), IEEE, 2016 .
240. Samuel, S.S.I. (2016). A Review of connectivity challenges in IoT-smart home. Proceedings of the 3rd MEC International Conference on Big Data and Smart City (ICBDSC), IEEE.
241. Lim, S., Kwon, O., & Lee, D. H. (2018). Technology convergence in the internet of things (IoT) startup ecosystem: A network analysis. *Telematics and Informatics, 35*(7), 1887–1899.
242. Hammoudi, S., Aliouat, Z., & Harous, S. (2017). *Challenges and research directions for internet of things* (pp. 1–19). Springer.
243. Sebastian, S., & Ray, P. P. (2015). Development of IoT invasive architecture for complying with health of home. *Proc International Conference on Computing and Communication Systems (I3CS '15)* (pp. 79–83). Shillong.
244. Severi, S., Sottile, F., Abreu, G., Pastrone, C., Spirito, M., Berens, F. (2014). M2M technologies: enablers for a pervasive internet of things. In: Networks and Communications (EuCNC), European Conference on. IEEE, pp. 1–5.
245. Li, S., Da Li, Xu., & Zhao, S. (2018). 5G internet of things: A survey. *Journal of Industrial Information Integration, 10*, 1–9.
246. Shang, W., Yu, Y., Droms, R., Zhang, L. (2016). Challenges in IoT Networking via TCP/IP Architecture. NDN Technical Report NDN-0038.
247. Shao, C., Hui, D., Pazhyannur, R., Bari, F., Zhang, R. (2015). IEEE 802.11 Medium Access Control (MAC) Profile for Control and Provisioning of Wireless Access Points (CAPWAP). RFC 7494, 2015. https://rfc-editor.org/rfc/rfc7494.txt.
248. Chen, S., Hui, Xu., Liu, D., Bo, Hu., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things Journal, 1*(4), 349–359.
249. Sherali Zeadally, Ashok Kumar Das, Nicolas Sklavos, (2019). Cryptographic technologies and protocol standards for Internet of Things. Internet of Things.
250. Shelby, Z., Hartke, K., Bormann, C. (2014). The Constrained Application Protocol (CoAP). IETF RFC 7252. (Online).
251. Daemin, S., Keon, Y., Kim Jiyoon, P. V., Astillo, J. N., & Kim, I. Y. (2019). A security protocol for route optimization in DMM -based smart home IoT networks. *IEEE Access, 7*, 142531–142550.
252. Shirazi, S. N., Gouglidis, A., Farshad, A., & Hutchison, D. (2017). The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. *IEEE Journal in Selected Areas of Communication, 35*(11), 2586–2595.
253. Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). FogBus: A blockchain-based lightweight framework for edge and fog computing. *Journal of Systems and Software, 154*, 22–36.
254. Sicari, S., Rizzardi, A., Piro, G., Coen-Porisini, A., & Grieco, L. A. (2019). Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the internet of nano-things. *Computer Networks, 162*, 106856.
255. Singh, S., Sharma, P. K., & Park, J. H. (2017). SH-SecNet: An enhanced secure network architecture for the diagnosis of security threats in a smart home. *Sustainability, 9*(4), 513.
256. Singh, S., & Chana, I. (2015). Q-Aware: Quality of service based cloud resource provisioning. *Computers and Electrical Engineering, 47*, 138–160.
257. 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*, 4724–4734.
258. Srinidhi, N. N., Dilip Kumar, S. M., & Venugopal, K. R. (2019). Network optimizations in the internet of things: A review. *Engineering Science and Technology, An International Journal, 22*(1), 1–21.
259. Srinivas, J., Das, A. K., Wazid, M., & Kumar, N. (2018). Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things. *IEEE Transactions on Dependable and Secure Computing, 17*(6), 1133–1146.
260. Stallings, W. (2011). *Cryptography and Network Security: Principles and Practice* (5th ed.). Delhi, India: Pearson.
261. Watson, S., & Tanha, A. D. (2016). Digital forensics: The missing piece of the internet of things promise. *Computer Fraud and Security, 6*, 5–8.
262. Stuart Millar, (2016). Network Security Issues in Internet of Things (IoT). Queen's University Belfast.
263. Su, J., Sheng, Z., Leung, V. C., & Chen, Y. (2019). Energy efficient tag identification algorithms for RFID: survey, motivation and new design. *IEEE Wireless Communications, 26*(3), 118–124.

264. Gill, S. S., Tuli, S., Minxian, Xu., Singh, I., Singh, K. V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U., Pervaiz, H., Sehgal, B., Kaila, S. S., Misra, S., Aslanpour, M. S., Mehta, H., Stankovski, V., & Garraghan, P. (2019). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things, 8*, 100118.
265. Sundevil Lee, (2012). Overview of internet of things. Available at http://www.scribd.com/doc/77110937/Overview-of-Internet-Of-Things.
266. Peddoju, S. K., & Upadhyay, H. (2020). *Evaluation of IoT data visualization tools and techniques*. Springer.
267. Stanciu, A. (2017). Blockchain based distributed control system for edge computing. In: Proceedings of the 21st International Conference on Control Systems and Computer Science (CSCS), IEEE, 2017.
268. Tagra, D., Rahman, M., Sampalli, S. (2010). Technique for preventing DoS attacks on RFID systems. In: International Conference on Software, Telecommunications and Computer Networks, IEEE, 2010, pp. 6–10.
269. Ted, H. S. (2017). Security and privacy for a green internet of things. *IT Professional, 19*(5), 34–41.
270. The Internet of Things, (2018). https://www.ietf.org/topics/iot/.
271. The Tech Wire Asia, The Next Generation of IoT, (2017). Available online 14 Jan 2018. http://techwireasia.com/2017/08/next-generation-iot/
272. Ting, S. L., & Ip, W. H. (2015). Combating the counterfeits with web portal technology. *Enterprise Information Systems, 9*(7), 661–680.
273. Tordera Eva Marín , Masip-Bruin Xavi, García-Almiñana Jordi , Admela Jukan Guang-Jie Ren, Zhu Jiafeng, Farré Josep, (2016). What is a Fog Node a Tutorial on Current Concepts towards a Common Definition. 2016.
274. Transmission control protocol (TCP), IETF RFC 793 (September) (1981). (Online). Available https://tools.ietf.org/html/rfc793.
275. Ubuntu Core, (2018). https://www.ubuntu.com/core, 2018, Accessed: 2018–05–18.
276. Van Deursen, A. J. A. M., & Mossberger, K. (2018). Anything for anyone? A new digital divide in Internet-of-things skills. *Policy and Internet, 10*(2), 122–140.
277. Van Deursen, A. J. A. M., Helsper, E. J., Eynon, R., & Van Dijk, J. A. G. M. (2017). The compoundness and sequentiality of digital inequality. *International Journal of Communication, 11*, 452–473.
278. Van Deursen, A. J. A. M., Helsper, E. J., & Eynon, R. (2016). Development and validation of the internet skills scale (ISS). *Journal of Information Communication and Society, 19*(6), 804–823.
279. Vakulya Gergely, Simon Gyula, (2013). Low-power communication protocol for low duty cycle data acquisition applications. IEEE International Workshop on Measurements and Networking.
280. Valerie Issarny, Mauro Caporuscio, Nikolaos Georgantas, (2007). A Perspective on the Future of middleware-based Software Engineering, IEEE Computer Society, pp. 244–258.
281. Verizon, (2015). State of the Market: The Internet of Things 2015.
282. Vermesan, O., Friess, P., Guillemin, P. (2009). Internet of things strategic research roadmap. The Cluster of European Research Projects, available from http://www.internet-of-things-research.eu/pdf/IoTClusterStrategicResearchAgenda2009.pdf
283. Adat, V., & Gupta, B. B. (2018). Security in internet of things: issues, challenges, taxonomy, and architecture. *Telecommunication Systems, 67*(3), 423–441.
284. Jog, V. V., & Senthil Murugan, T. (2016). A critical analysis on the security architectures of internet of things: The road ahead. *Journal of Intelligent Systems, 27*(2), 149–162.
285. Wang, M., Fan, C., Wen, Z., Li, S. (2011). Implementation Of Internet of Things Oriented Data Sharing Platform Based On Restful Web Service, Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1–4.
286. Wang, Y., Uehara, T., Sasaki, R. (2015). Fog computing: Issues and challenges in security and forensics. In: Proceedings of the 39th IEEE Annual Computer Software and Applications Conference, 3, IEEE, 2015.
287. Weber, R. H., & Weber, R. (2010). *Internet of Things*. Springer.
288. Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., & Borriello, G. (2009). Building the internet of things using RFID: the RFID ecosystem experience. *IEEE Internet Computing, 13*(3), 48–55.
289. Andrew, W., Anurag, A., & Da Li, Xu. (2014). The internet of things —A survey of topics and trends. *Information Systems Frontiers, 7*, 261–274.
290. Wu, M., Lu, T.J., Ling, F.Y., Sun, J., Du, H.Y. (2010). Research on the architecture of internet of things. In the Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10) 5, IEEE, Chengdu, China, August 2010.
291. Xia, C., Maes, P. (2013). The Design of artifacts for augmenting intellect. In: Proceedings of the 4th Augmented Human International Conference, ACM, 2013, pp. 154–161.

292. Xiao, F., Wang, Z., Ye, N., Wang, R., & Li, X. (2018). One more tag enables fine-grained RFID localization and tracking. *IEEE/ACM Transactions on Networking, 26*(1), 161–174.
293. Xiaoqi Li, P. Jiang, T. Chen, X. Luo, Q. Wen, (2018). A survey on the security of blockchain systems, Future Generation Computer Systems , https://arxiv.org/pdf/1802.06993.pdf
294. Xingmei, X., Jing, Z., He, W. (2013). Research on the Basic Characteristics, the Key Technologies, the Network Architecture and Security Problems of the Internet of Things. 3rd International Conference on Computer Science and Network Technology, 2013.
295. George, X., Ververidis, C. N., Siris, V. A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K. V., & Polyzos, G. C. (2014). A survey of information-centric networking. *IEEE Communication Survey Tutorials, 16*(2), 1024–1049.
296. Yang, G., Xie, L., Matti, M., Zhou, X., Pang, Z., Xu, L. D., Walter, S. K., Chen, Q., & Zheng, L. (2014). A health-IoT platform based on the integration of intelligent packaging, unobtrusive Bio-Sensor and intelligent medicine box. *IEEE Transactions on Industrial Informatics, 10*(4), 2180–2191.
297. Yang, B., Nie, X., Shi, H., Gan, W. (2011). M-learning mode research based on internet of things. Proceedings of International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp. 5623–5627.
298. Pundir, Y., Sharma, N., & Singh, Y. (2016). Internet of things (IoT): Challenges and future directions. *International Journal of Advanced Research in Computer and Communication Engineering, 5*(3), 960–964.
299. Yu, Y., Wang, J., Zhou, G. (2010). The exploration in the education of professionals in applied Internet of Things engineering. In Proceedings of the 4th International Conference on Distance Learning and Education (ICDLE). IEEE, 2010, pp. 74–77.
300. Zach Shelby, Carsten Bormann, (2011). 6LoWPAN: The wireless embedded Internet. 43, John Wiley & Sons
301. Abbas, Z., & Yoon, W. (2015). A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects. *Sensors, 15*, 24818–24847.
302. Zhang, M., Sun, F., Cheng, X. (2012). Architecture of internet of things and its key technology integration based-on RFID. In: Computational Intelligence and Design (ISCID), 2012 Fifth International Symposium on 1. IEEE, pp. 294–297.
303. Zhou, Q., Zhang, J. (2011). Research prospect of Internet of Things geography. In Proceedings of the 19th International Conference on Geo informatics. IEEE.
304. Babovic, Z. B., Protic, J., & Milutinovic, V. (2016). Web performance evaluation for internet of things applications. *IEEE Access, 4*, 6974–6992.
305. Zubair, A., Baig, P. S., Valli, C., Rabadia, P., Peacock Hannay, M., Chernyshev, M., Johnstone, P., Kerai, A., Ibrahim, K. S., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cybersecurity and digital forensics. *Digital Investigation, 22*, 3–13.

Dr. B Nagajayanthi is an Associate Professor in Vellore Institute of Technology, Chennai Campus. She is expertized in the field of Wireless Networking, Cryptography, Internet of Things and Network Security. She has ardent interest and real time experience in working with projects.