Review Paper

Security trends in Internet of Things: a survey

Rachit[1] · Shobha Bhatt[1] · Prakash Rao Ragiri[1]

Received: 8 May 2020 / Accepted: 4 January 2021 / Published online: 12 January 2021

Abstract
The Internet of Things (IoT) is a network of embedded devices that are uniquely identifiable and have embedded software required to communicate between the transient states. The purpose of this study is to explore discrete IoT security challenges pertaining to currently deployed IoT standards and protocols. We have presented a detailed review in this study that focuses on IoT's imminent security aspects, covering identification of risks pertaining to the current IoT system, novel security protocols, and security projects proffered in recent years. This work presents an updated review of the IoT architecture in the protocols and standards that are proffered for the next-gen IoT systems. A security-specific comparative analysis of protocols, standards, and proffered security models are presented as per IoT security requirements. This study elicits the need for standardization at the communication and data audit level, which exposes the hardware, software, and data to various threats and attacks. Our study reveals a need for protocols that are competent enough to be accorded for over one threat vector. This paper provides an insight into the latest security research trends, which will prove beneficial in the development of IoT security. The research outcomes can benefit the research community in IoT by integrating IoT-based devices' best security aspects.

Keywords Internet of Things · Lightweight IoT protocols and standards · IoT network security models

1 Introduction

Lately, the entire network domain is undergoing a drastic technological revolution. Automation of networks has been a hot topic that has been trending for quite some time. Supplementing it is Internet of Things (IoT) technology, which paves the way for providing that element. The Internet of Things [1] is defined as the inter-device environment built up by the devices that focus on three important tasks–transmitting data, receiving data, and processing received data. Initially, local physical devices connected to the internet for real-time data analysis were considered being the IoT network. With time-lapse, IoT's scale has extended itself from the local workstation to Industrial IoT frameworks [2]. Research works on IoT depict the proliferation of IoT in the field of–healthcare [3], industrial setup [4], business analytics, education, etc. As of 2019, IoT, which used to work at smaller network spaces, has upgraded for wide area networks, and so have the risks relative to it because of the expected surge in IoT devices in a diversified environment.

1.1 Research challenges

The primary purpose of this research work is to explore the latest security solutions in the IoT. Besides this primary goal, sub-goals comprise identifying and characterizing the latest security risks in the IoT. Before that, it is important to address the recent research challenges in IoT-

(1) Heterogeneity issue
(2) Inter-connectivity

✉ Shobha Bhatt, bhattsho@gmail.com; Rachit, rachit.7rauthan25@gmail.com; Prakash Rao Ragiri, prakashrao@aiactr.ac.in | [1]Department of Computer Science, Ambedkar Institute of Advanced Communication Technologies & Research, (Affiliated to Guru Gobind Singh Indraprastha University), Delhi, India.

(3) Ubiquitous nature
(4) Security standards issue

Trending technical domains like Artificial Intelligence as cluster-based fuzzy logic modules [5, 6], Machine Learning, and Software Enabled Networking [7] have become the new research field for incorporating IoT. A notable development in IoT is the addition of ultra-lightweight protocols [8, 9] deployed for the core functioning and security reasons as well [10].

Research works pertaining to IoT security challenges [11] cover a large area, and it is changing every day, with new loopholes being exposed regularly. Today, when we talk about IoT security, the main emphasis is on the access control methods [12], encryption methodologies used for transient phases [13], and hardware-specific security solutions [14], and SQL related input based attack controls [15]. So, our research emphasizes the ever-changing security perspectives of IoT by giving IoT related security issues, proper definitions, classification, and searching for the solution present in the current scenario against them.

1.2 Research contribution

The work has been motivated to explore security concerns in IoT based devices due to different IoT applications. First, to understand IoT's security aspect, it is important to have prior knowledge about the infrastructure we are dealing with; thus, we have discussed IoT architecture and made a comparative analysis of protocols and standards used in IoT. Our second research contribution includes exploring all possible aspects of recent research being made in IoT security, which will prove beneficial in developing an IoT security framework. A thorough review presented in this survey focuses on prominent threats prevailing in current IoT systems, along with the latest security models proffered for the IoT environment in recent years. The purpose is to define security solutions in IoT's security requirements: confidentiality, integrity, authenticity, and trust management [16]. Our third research contribution comprises the identification and comparative analysis of prevalent protocols and standards in the IoT. We have addressed the updated innovations and standardization practices being used in IoT [17], classification of security issues in IoT based on the levels at which they affect the entire environment, and their relative solutions. Research findings show that IoT security solutions are addressed by using existing encryption techniques and novel security design models. The major security issues recognized are trust and integrity of communication. It was also revealed that IoT security challenges are enhanced by combining IoT with other networks such as SDN [18, 19]. We also discovered a need for standardization at the manufacturing level, which shows the vulnerabilities at the hardware and software levels [20]. Inspections also revealed a need for protocols competent enough to accord for over one threat vector [21, 22]. The research outcomes can help the IoT research community by integrating the safest appropriate security features in IoT-based devices.

The paper is organized as follows. Section 1, as discussed, is a brief introduction to the study. Section 2 presents a literature review of recent developments in IoT. Section 3 discusses IoT architecture along with the trending protocols and standards used in IoT. Section 4 discusses Security trends in IoT in detail. Section 5 states the result and discussion of the entire research study, and Sect. 6 concludes the complete survey work.

2 Literature review

Wireless network with embedded networking capability is the current Industrial trend worldwide. IoT is one of the main gainers of this networking domain. It has undergone a significant development by integrating Cloud services, providing SaaS, IaaS, and PaaS. IoT Commercial sectors have seen a major boom in the market during the last few years, as smart system demands grew manifold because of its rich feature and one-click-away services. Smart systems like Smart Home appliances, AI-based smart devices, smart home automation, smart vehicles, smart labs, etc., offer ease of living but too much dependability on them often leads to high risks. Figure 1 based on statista [23] report gives an estimated graph of the expected surge in IoT devices in the near future.

The technical report suggests IoT devices have become the new source hotspot for intrusion activities for the hackers as the protocols and standards existing on these devices are mainly lightweight protocols [24, 25] and, on the other end, entities constituting it has more accessible access to the server [26]. These pose challenges to the

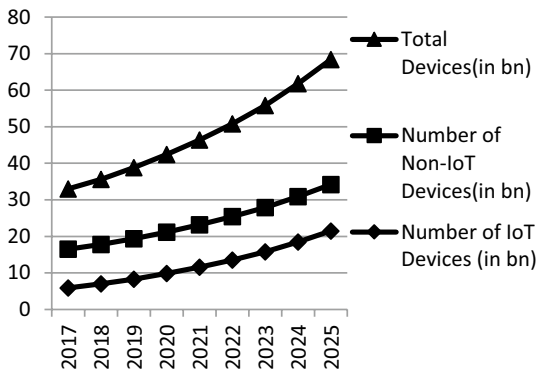

Fig. 1 Estimated census of Wireless Devices [23]

technology as there is no proper addressing of the security for the latter.

It is observed that threat structure is not confined to a particular layer in IoT architecture [27]. Former network practices of integrating network security features in IoT have/had degraded IoT systems' performance. Table 3 comprises a set of recent novel models proposed in the wake of advanced threat reports coming for IoT. We have defined the security parameter concerning which certain research work offers a security model pertaining to conventional security models.

The conventional model issue was—Inter-Compatibility among security tools deployed for IoT devices as they differed in Policy and implementation techniques and lack of Low- Powered device algorithms [28]. Recent research has proposed novel solutions using a different plethora of encryption methods and hardware-based methods [29] to overcome conventional security issues. Table 1 discusses some of these significant security models currently in research.

Xin Zhang and Fengtong Wen [30] proposes a novel anonymous user WSN authentication for the Internet of Things wherein two algorithmic models UDS (user-device-server) and USD (user-server-device), are constructed to ensure valid authentication for resolving trust centric threat models. This is a multi-functional method to provide security during the authentication process with lighter storage overheads, efficient communication costs, and faster computational speed. This work is limited in terms of the extent of the security solution provided, only for the lightweight sensor devices against the prominent network layer and physical layer based attacks. A cluster-based fuzzy logic implementation model is proposed by Mohammad Dahman Alshehri and Farookh Khadeer Hussain [31] and a secure messaging paradigm between IoT nodes where encrypted communication takes place utilizing hexadecimal values to cope with Port Scanning threats and other integrity specific vulnerabilities for AI-based IoT security solutions. This work effectively proffers the detection mechanism against the malicious IoT nodes present in the network, but risks pertaining to the data audit attack surface are not covered in this model. This study also falls short of addressing the performance analysis relative to communication costs and computation costs occurring in operation.

Priyanka et al. [13] propose a multi-stage security model making use of Elliptical curve cryptography (ECC) and fully homomorphic encryption (FHE) against cryptographic attacks, which ensures the integrity of the data transmitted in the IoT environment with less computation power. However, there is a lack of clearance on the increased data overheads generated during the process. Computational cost is another issue concerning this model.

Regarding Industrial IoT, Munkenyi Mukhandi et al. [5] discusses the novel security solution for robotic communication from an Industrial IoT perspective using MQTT and Robot Operating System protocols. Two primary methods–data encryption and authentication have been used for this purpose, which has proved their efficiency in securing communication phases. This work gives valuable insight into the effectiveness of the cryptographic methods in securing communication channels. On the contrary part, this study states the inconsistency between the performance metrics and the cryptographic functions. Deep learning and Machine learning have made their insight in IoT environment with major products being Alexa, Echo, which abject the text commands and takes voice-over commands for action on a real-time basis. But issues have arisen pertaining to the data packet leaks, and thus for that perspective, a voice recognition application is proffered by Pooja Shree Singh and Vineet Khanna [32], which is based on Mel-frequency cepstral coefficients (MFCC) for user identification and authentication deployable in the IoT environment to ensure data integrity, confidentiality, and privacy security. This work is useful for securing voice-enabled IoT applications; however, large dependency on the hardware architecture required for the noise-free and quality input is its major down-point. IoT has struggled with access control-related problems ever since its arrival. To address this problem, Michail Sidorov et al. [10] proposed a novel secure ultra-lightweight RFID protocol targeted for integration in a supply chain management system that uses permissioned blockchain network along with encryption provided at different access levels. Performance analysis depicts promising results with lesser storage costs and high computational speed. This work is believed to impact secure IoT devices significantly; however, the entire setup cost is uncertain. Chen et al. [33] proffers a novel Low scale Denial-of-Service attack detection approach that encompasses Trust evaluation with Hilbert-Huang Transformation in Zigbee WSN to resolve security issues pertaining to a plethora of low energy devices becoming the target of the attacks. This work is useful in refining the attack surface due to its low rate signal detection method. It features scalable architecture as it covers both cloud computing and edge computing IoT devices, which is an advantage, but larger storage overheads remain an issue. Intrusion Detection Systems (IDS) are tasked with detecting and monitoring threat activities in the conventional network security domain [34]. Extension of which in IoT perspective is some proposed model like Snort [35], Suricata [36], and Bro [37]. Roesch [35] and Paxson [37] talks about the model resulting from pattern-matching monitoring. Suricata [36] is modeled on the semantic level matching of the network activities. Paradoxically, such models are designed for professional use and are not explicitly aimed

Table 1 Review of latest IoT related Security Models

S. No	Year	References	Description	Security aspect affected
1	2018	Xin Zhang and Fengtong Wen [21]	Proposes a novel anonymous user WSN authentication for the Internet of Things wherein two algorithmic models UDS and USD are constructed	Authentication
2	2018	Mohammad Dahman Alshehri and Farookh Khadeer Hussain [22]	Proposes a cluster-based fuzzy logic implementation model along with a secure messaging paradigm between IoT nodes using hexadecimal values	Confidentiality and trust management
3	2019	Priyanka Anurag Urla, Girish Mohan, Sourabh Tyagi and Smitha N. Pai [23]	The model proffered here is a multi-stage security model that utilizes Elliptical curve cryptography (ECC) and fully homomorphic encryption (FHE) for mitigating cryptographic attacks	Integrity
4	2019	Hongsong Chen, Caixia Meng, Zhiguang Shan, Zhongchuan Fu and Bharat K. Bhargava [24]	Proposes a novel Low scale Denial-of-Service attack detection approach that encompasses Trust evaluation with Hilbert-Huang Transformation in Zigbee WSN	Availability and trust management
5	2019	Michail Sidorov, Ming Tze Ong, Ravivarma Vikneswaran, Junya Nakamura, Ren Ohmura and Jing Huey Khor [20]	Proffers a novel security model devised for ultra-lightweight RFID protocol, which focuses on the supply blockchain management system. It utilizes a valid blockchain network having encryption implied at different access levels	Authentication
6	2019	Munkenyi Mukhandi, David Portugal, Samuel Pereira and Micael S. Couceiro [26]	Proffers novice security model encompassing robotic communication in Industrial IoT using MQTT and Robot Operating System. Two primary methods implemented are–data encryption and authentication	Authentication and integrity
7	2019	Pooja Shree Singh, Vineet Khanna [27]	proffers a voice recognition application based on Mel-frequency cepstral coefficients (MFCC) for user identification and authentication deployable in an IoT environment to ensure data integrity, confidentiality, and privacy	Confidentiality, Integrity, and Privacy

SN Applied Sciences (2021) 3:121 | https://doi.org/10.1007/s42452-021-04156-9

at the IoT environment in terms of protocol analysis availability. It targets such advancements for expert users but not a regular citizen who lacks knowledge of the whole framework technology's technical know-how. GHOST [38] is a Development project (Safeguarding home IoT environments with personalized real-time risk control) that challenges the conventional network security solutions for the IoT by proposing novel reference architecture. This model's feature is–embedded network environment in an adequately adapted smart home network gateway and is vendor-independent. The issues regarding this integrated model are many attacks like impersonation attacks, offline password attacks, and hardware-based anomaly attacks still pertain to pose a threat to the whole architecture.

3 Internet of Things: architecture

The Internet of Things covers a vast range of industries and uses cases that scale from uni-constrained node devices to large cross-platform deployments of embedded technologies and cloud systems connecting in real-time [39]. As discussed earlier, IoT operations are constructed out of three major functions, for example, transmitting, retrieving, and processing data. IoT is a technology comprising data exchange between heterogeneous devices that continuously stream information data among other peripheral devices.

3.1 Layered architecture

Internet of Things has a multi-layer and multi-plane architecture, as shown in Fig. 2. It comprises the following component sections—Device Management section, Application Interface section, and Communication plane.

Application Interface Layer—Devices interact with underlying architecture via certain embedded interface modules like Arduino IDE, Raspberry Pi, sensors, actuators, etc., present in this architecture section.

Device Management Plane manages the device i/o functionalities by identifying the data's source and destination. For instance, Aggregator—is a centralized component that aggregates the data in fluxed from the devices.

Communication Layer—this layer is the intermediary layer that comprises switches and similar network units that define the communication protocols and standards

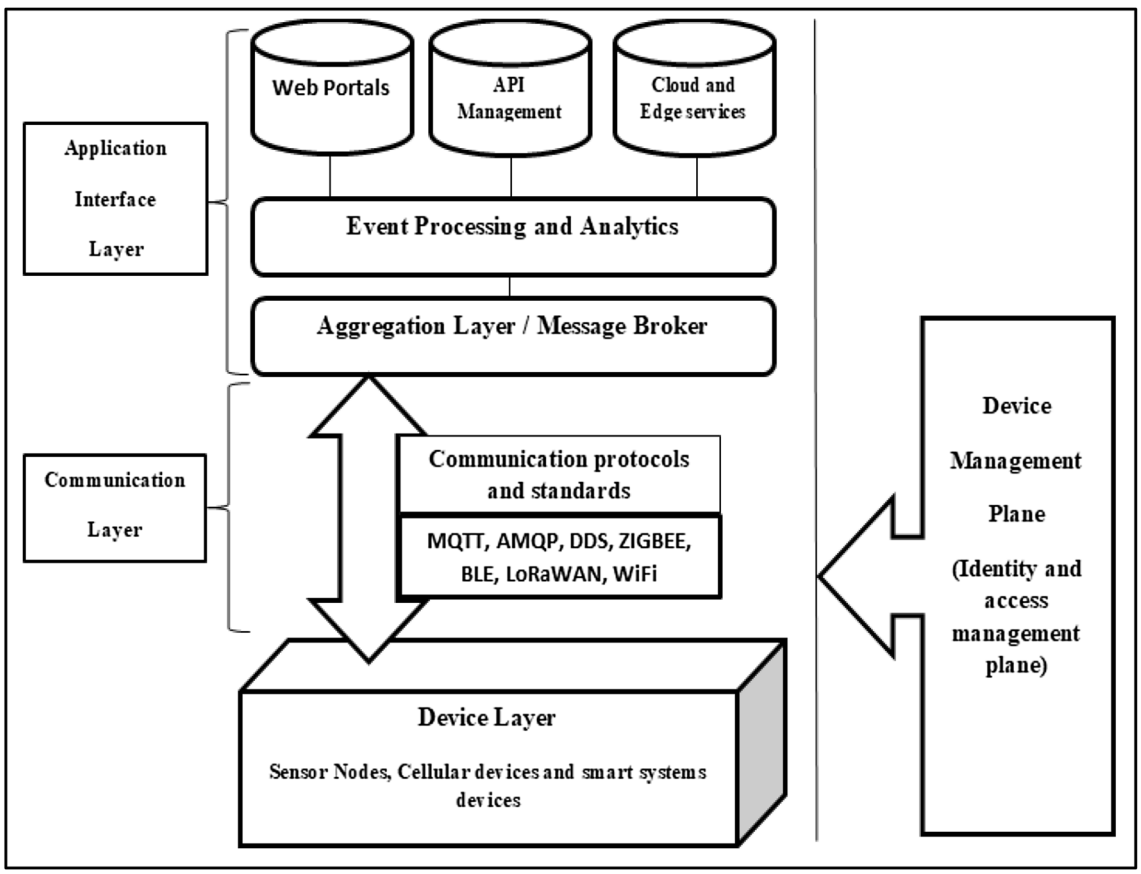

Fig. 2 Layered Internet Of Things Architecture

for the IoT network traffic. This layer consists of protocol stacks of the latest protocols and standards implemented to direct network traffic in the entire system. New diversified communication protocols used in embedded IoT environments are energy efficient, have better congestion control properties, and have improved QoS features.

3.2 Communication protocols

Communication between the IoT devices is made feasible with certain standard protocols like MQTT (Message Queueing Telemetry Transport), AMQP, DDS, ZigBee, and LoRaWAN [40], etc. Such an environment needs to have some sort of standardized set of rules which initialize easier and is compatible enough for info sharing. Notably, the communication protocols of IoT are:

1) *Bluetooth Low Energy (BLE) Protocol* [41]—one of the vastly used protocols in the IoT environment. Its low energy consumption capability makes it suitable for low energy devices. This protocol is based on Generic Attributes, and it operates via services and characteristics.
2) *Message Queueing Telemetry Transport (MQTT) Protocol* [42]—it is the messaging protocol devised for lightweight IoT devices for transmitting and receiving data between sensor nodes. This protocol working is based upon three major components, namely—Publisher, Broker, and Subscriber. The publisher is the one that only transmits the data; the Broker is the intermediary MQTT server that analyzes the data being sent, and the request is identified for certain resources, and last, the subscriber, these components are the receiver of message coming from the broker.
3) *Advanced Message Queueing Protocol (AMQP)* [43]—major features of AMQP protocol are—this is efficient, portable, multichannel, and secure. This binary protocol ensures authentication through SASL or TLS and relies on TCP. It is better suited for working in multi-client environments, as it supports multi-functions by making servers handle immediate requests faster.
4) *Constrained Application Protocol (CoAP)* [44]—as the name suggests, it is a constrained based environment protocol. This protocol's significant characteristics are—based on the REST API structure, designed for smart system applications, well-designed congestion control, cross-protocol integration, and many more.
5) *Data Distribution Service (DDS) protocol* [45]—It is an IoT protocol developed for M2M (Machine to Machine) Communication. Data exchange is possible via the publish-subscribe method, as in MQTT and CoAP protocols, the only difference being that it is broker less architecture, unlike the latter ones. It uses multicasting to bring high-quality QoS to the applications. DDS protocol can be deployed from low footprint devices to the cloud.

Some other Protocols relative to the Internet of Things are specified in Table 2, highlighting the features and issues related to protocols' security. As observed, IoT protocols have provided frameworks for enabling easier adaptation of IoT in other existing wireless technology like cloud, edge computing, lightweight embedded systems. Although scalability, performance, and applicability are bettered with innovative protocols, security loopholes are left in the process, which will be discussed in the next section of this paper.

4 Security trends in Internet of Things

IoT, as seen in the above sections, is not confined to limited resources. New trending technologies like 5G [47, 48], Block chaining [49], Quantum computing, and edge computing getting emulsified with the IoT have broadened the IoT's operational perspective. Figure 3 showcases the practical aftermath that each new technology brings and how it can affect IoT functionary. Heterogeneous physical devices like sensor nodes, actuators, gateways, switches, and other embedded system devices constitute this volatile environment. It does not confine the Internet of Things to networking principles; a major impact is made by the engineering behind the smart devices, which is the whole concept's backbone. Self-configuring devices that feature the M2M communication paradigm are the new invention in IoT. This setup makes nodes intelligent enough through algorithms and supplementary technology to self-decide the course of action in any condition [50, 51]. It is beneficial in an emergency condition, rescue operations where it is a tedious task to configure the network for a particular region with little or no support from damaged nodes. But too much dependency on machines makes it vulnerable also, as machines are not foolproof. Today, specifically, adversaries exploit weak authentication, unpatched firmware, and credentials pertaining to authenticity that is vulnerable over the internet [52].

4.1 Security challenges

1) As observed from the table referring to the protocols and standards of IoT, the paradigm is most vulnerable in accessing requests, identifying third-party indulgence, and weak scalability compliance with security management. Various security challenges in IoT today pertaining to conventional network architecture are pointed out as—*Heterogeneous Device Configura-*

Table 2 Protocols and Standards in IoT

S. No	Protocol	Features	Major security issue
1	Bluetooth low energy (BLE) [38] (2019)	1. Low energy consumption 2. Provides the same range as that of conventional Bluetooth 3. Mesh networking topology is implied 4. Is incorporated for low energy consuming devices like sensors, home appliances, cameras, etc	Open to interception and attacks during transmitting and receiving data
2	Zigbee [24] (2019)	1. The network paradigm is flexible 2. Improved mesh networking provided along with low cost, multi-hop data transmission, and power efficiency 3. Power consumption is relatively low	Malicious node based sinkhole and wormhole attacks, Distributed Denial of Service (DDoS)
3	Message queueing telemetry transport (MQTT) [18] (2008)	1. Provides lightweight protocol for the transmission of data among machines over TCP 2. Simplified protocol 3. Processing and energy consumption rate is less 4. The requirement of bandwidth is less	Exposed MQTT servers over the internet, third party malicious subscription to MQTT messages
4	Constrained application protocol (CoAP) [40] (2019)	1. Developed for the constrained network device environment 2. Specifically uses for homogeneous restricted device community 3. Comprises various end node devices, restrained smaller networks connected over the internet 4. RESTful architecture based	The DDoS attack involving a third party actor that simultaneously sends forged IP packets to target IP Addresses during CoAP reflection/ amplification
5	Data distribution service (DDS) [37] (2018)	1. Communication protocol for the machine to machine exchange of data 2. Scalability and high performance are the key features 3. Proficient in data transference between low-footprint devices and other cloud platforms	Due to the expandability feature, weak implementation and management of devices can lead to DDoS or Man in the middle attacks
6	Near Field Communication (NFC) [46] (2018)	1. Ensure secured 2-way communication linking 2. Smartphones are the end nodes 3. A major application is a contactless payment transaction between electronic devices, utilizing digital contents	Malicious node based wormhole attack
7	EnOcean [35] (2020)	1. User-driven self-powered wireless sensor network which processes and accumulates data in smart intelligent systems 2. Less idle current thus less energy consumption close or less than 100 Nano amperes (nA) current	Being a user-driven or self-prepared IoT protocol, optional blocking, pre-shared security keys, undefined re-synchronization of rolling codes are often missed or neglected
8	SigFOX [33] (2019)	1. It brings the best out of both Cellular and Wifi network with a low power consumption of nearly 50 microwatts 2. Supports dense node network with star network topology 3. Has cloud access and restricted endpoint access control	Poor IoT payload encryption

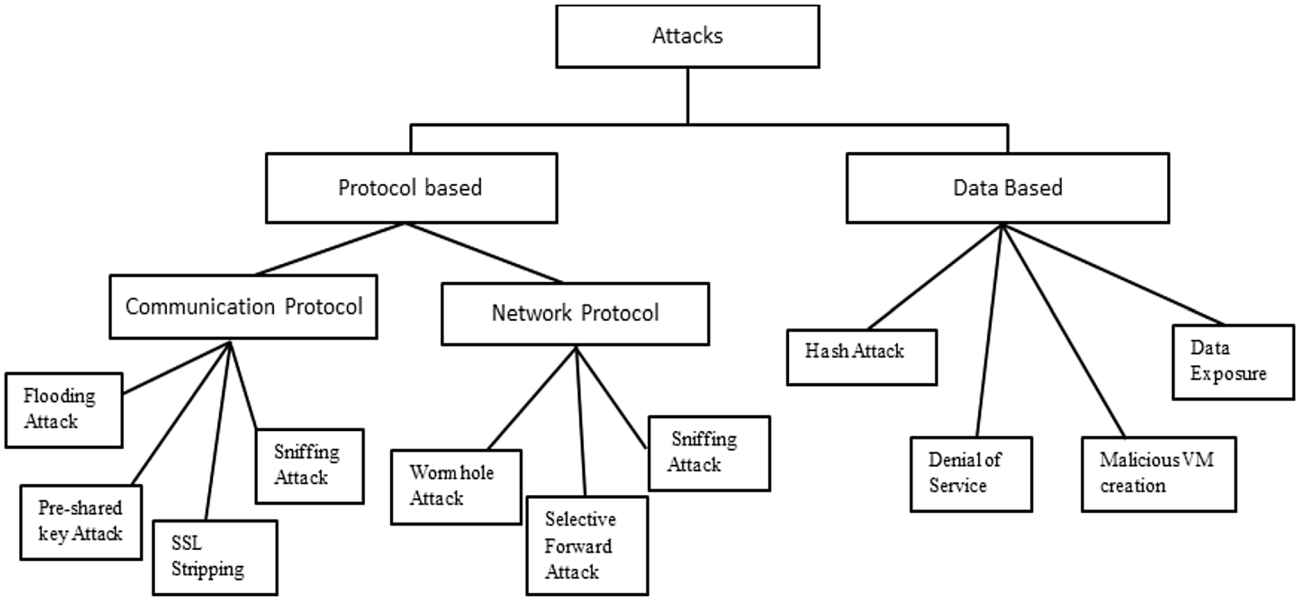

Fig. 3 IoT Attacks Classification [14]

tion—IoT devices' way of interaction with the physical world varies from the way conventional network devices used to do. Heterogenous nature IoT devices, while performing operations, ramify other networking components. As per NIST, they emphasized that IoT-specific privacy policies [53] and cyber controls must consider the fact relative to the ramifications made by IoT devices, which brings about changes to physical systems [54], eventually affecting the physical world. Thus, heterogeneity characteristics are a form of security issue [55].

2) *Dispersive Network Update Policy*—IoT devices worldwide, be it in an organization or personal workspace, are managed through commonly distributed servers. Such IoT devices are accessed, managed, or monitored via a separate form of a rule engine, and security policy is also different for each device in the system. So, in regularization, all the devices need to be updated, which is a tedious, complex task for the organization. Issues faced are in the form of non-uniform rate of updation, additional switch leave behind some non-updated devices, or weakly configured nodes as keeping a check on millions of nodes requires time. Intervention from a third party for support in the discussed issue can jeopardize the system's access control. Organizations that have geographically dispersed locations suffer cost-prohibitive and time-consuming issues and must be protected and updated.
3) *Add-Ins Security Policy*—Because IoT was never modeled out for the provision of the security features. Additional plugins and security controls are appended over the IoT layered architecture for providing secure solutions. Thus, unlike the conventional network paradigm, the efficiency of security characteristics depends on the functioning capability of additional resources over IoT architecture. Client actions like how they opt for certain available security options also affect the IoT's security effectiveness.
4) *Physical IoT threats*—Physical security threats are real in physical IoT setups in industrial units, network-integrated healthcare systems, and network enterprise domains. Two main threat vector points are—Communication channels and the data audit functionaries [56]. Security challenges prevailing in the communication channel comprises trust management issues and authentication issues among the stakeholders, network entities, and the network mode itself through which the communication is taking place. Data Audit specific security challenges expose the weak security points prevailing during an enormous amount of data transmittance over the network and the IoT architecture's aggregator layer. Other physical security challenges involve manual or natural destruction to the sophisticated network components. In industrial systems, physical threats lie in the malfunctioning of the IoT equipment like robotics, sensors, and hardware devices that might adversely affect the physical entities [29].
5) *Exposure threat*—End devices in IoT, like sensors and IP cameras that are installed in open environments, are the threat points that are not so hard for the adversary to get access to. This leads to physical-based attacks

and proximity attacks, which compromise the user's authentication and integrity [57]. Security challenges pertaining to this issue lie in how architectural modification we can make in the protocol or the communication mechanism to secure such devices against the adversaries.

4.2 Classification of attacks in IoT

Recognizing potential threats in architecture based on behavior and target set is extremely important to devise security solutions. Many commercial firms have invested a vast amount of assets in securing their IoT-based network in recent development.

Attacks on IoT are divided into two modules, as shown in Fig. 3 as:

(1) Protocol Based Attacks—These types of attacks exploit the internal protocol-based structure of the IoT components that impact the communication medium and the embedded system's forwarding channels. These are further classified in other subsections. Protocol-based has two:

   (a) Communication protocol-based attacks—This explains the forms of exploitations occurring during the transient phases among nodes. These include–Flooding attacks, Pre-shred key attacks, and sniffing attack.
   (b) Network protocol-based attacks—This explains the exploitation occurring in the connection establishment. Attacks include—Wormhole attacks, Selective Forward attacks, and Sniffing attacks.

(2) Data-Based Attacks—Data based attacks include threats pertaining to the original data packets and messages traveling at node sites. Hash collision, DoS, Malicious Node VM creation, and Data exposure are some of its most afflicted security exploitations.

4.2.1 Classification of IoT attacks based on active and passive forms

Some prominent attacks based on active and passive forms are depicted in Table 3 shown below. The significance of such attacks in IoT security is that specific security solutions applied over the IoT environment for active and passive attacks tend to affect the network performance differently. Active attacks require state-of-the-art responsive security mechanisms to thwart the risk and impact network performance. On the other hand, defense mechanisms deployed for passive attacks are limited to monitoring tactics and thus have relatively less impact on the network's performance.

Table 3 Active/passive IoT attacks

Attack	Active	Passive
Denial of service/distributed denial of Service	✓	
Traffic sniffing		✓
Masquerade attacks	✓	
Message replay	✓	
Port scanning		✓

1) Denial of Service/Distributed Denial of Service attack [58]—In terms of IoT, DDoS is the prominent one as it affects the network's availability security parameter. Botnets are created to implement a DDoS attack that targets the sensor nodes or any weakly configured nodes in a physical environment. Gaining access from these weak points, infected packets from various sources traverses network data paths that finally congest the whole link architecture and make servers unavailable in the process. It is highly dangerous in energy transmission sectors, military communication, emergency operations, and finally, the worst affected is healthcare facilities.
2) Traffic sniffing attacks [59]—Traffic sniffing attack comes under the threat activity of active data gathering in which critical system info is captured and later utilized for attacks like botnet attack. Information assets like usernames, passwords, unencrypted data info, authentication type, and hardware details are scrutinized with advanced tools' assistance during such a penetration attack. Most IoT devices currently in the market are not so intelligent enough to mitigate such threats and easily become the target of such threats.
3) Masquerade attack [60]—this attack uses a fake network ID to gain unauthorized access to target node information via a legitimate access identification process. Devices with weak authorization processes are at high vulnerability risk. Such attacks perpetrate utilizing stolen passwords and user credentials by locating logical spaces within programs or finding alternatives to the existing authentication process. Access levels through masquerade attacks depend on the level of authorization the penetrator attains.
4) Message Replay attack [61]—A replay attack can be organized in three steps–eavesdropping on the secure communication link between IoT devices or Gateway, Interception of the acknowledgments or connection

establishment components, and fraudulent misdirection or delays through the replay of the message. It affects the normal working of the devices in the network, making them implement functions that they are not supposed to, or the result is directed in the way an attacker wants them to. It is easier to implement as, after packet seizing, further steps do not need advanced skills for message decryption because the entire message can be replayed to gain access to the server.

5) Port Scanning–Port scanning has the following components–SYN requests, target port, source, firewall, packets, open nodes, and listening nodes [62]. The commonly used method is SYN scans, which involve establishing a partial connection to the host node present on the target port by transmitting an SYN packet for the host system's initial response evaluation.

Case 1 when the request packet is not scrutinized properly by firewall policies, then an SYN/ACK packet is transmitted from the host.
Case 2 otherwise, an RST packet is sent by the host if the port is closed.

4.3 Security solutions

The latest IoT security solutions are more directed towards software-centric security methods [63] than conventional security, which was tool-centric. Authentication, trust, and integrity of the communication channel among IoT devices are the critical security parameters pertaining to which modern solutions are addressed. Though still at the current level, IoT lacks in supporting high-powered devices and is not compatible enough for coping up with increasing heterogeneous entities.

4.3.1 Comparative analysis of IoT protocols

Protocol analysis is shown in Table 4. Integrating IoT with other future budding technology like SDN for better scalability, node management, security policy, and reliability poses new security challenges to IoT.

As depicted in Table 4, the protocols reviewed are low on energy consumption, but the security issue varies on different parameters. Of course, these protocols' performance factor has improved, but that has exposed the weak loopholes in the rules flows.

CoAP protocol supports the DTLS security mechanism and has spontaneous support in the form of IPSec. The transient phase remains secure in this, but the load based attacks like a botnet and DDoS attacks remain the security issues [64, 65].

MQTT protocol provides Transport layer-based security support or the Secured Socket security layer for safe transient phases. Issues arise in malicious node subscription attacks and, again, the botnet attacks [62].

EnOcean [66] secures the nodes in their environment by providing a unique rolling code key encryption technique.

Cons are problems in the synchronization of codes and the privacy of the key used.

SigFOX [9] gives security support via several security solutions like tough firewall, hardware security module, public key infrastructure, and on-the-go security dispatching security solution, which proves beneficial for the dynamic IoT setup environment. It is a Virtual Security paradigm. Issues lie in weak Payload encryption. In terms of energy consumption, almost every novel protocol has

Table 4 Latest IoT protocol properties

Protocols	Energy consumption	Topology provided	Threat issues	Security support
COAP	Low	Chain, grid, cross, dumbbell, and random	DDoS, Botnet, and malicious node attacks	Datagram transport layer Security (DTLS), IPSec
MQTT	Low	Distributed and multi-broker	Malicious node subscription attack, Botnet attacks	TLS or SSL Security
BLE	Low	Piconet	Interception attacks, Man in the Middle attack, and identity tracking	Generic Access Protocol (GAP)
DDS	Relatively High	Random	DDoS and Man in the Middle attacks	DTLS
EnOcean	Low	Mesh	Loose privacy, undefined synchronous code definitions	Encryption Methodology with rolling code key distribution
SigFOX	Low	One-hop star	Weak Payload Encryption attacks	Hardware Security Module, Public Key Infrastructure along with OTA (Over the Air) security dispatching facility

low energy consumption values, which is a promising feature as it will perform better in a high-density network and thus enhance network performance.

4.4 Comparative analysis of IoT security models

As discussed earlier in Sect. 2, security models have proposed a unique plethora of securing IoT environments. A comparative analysis is done to determine their effectiveness in satisfying the IoT network's basic security requirements, as depicted in Table 5. In this analysis, we investigate the parameters of the technique used and the security requirements satisfied by each one of them.

Security requirements adjudged here are the basic Confidentiality (C), Integrity (I), and Availability (A) and Trust management (T) among nodes and Authenticity (Ay). The dual authentication model proposed by Xin Zhang and Fengtong Wen [30] excels in satisfying authentication and trust security requirements via the usage of UDS and USD WSN authentication models but lacks in CIA requirements, which exposes it to botnet attacks and DDoS attacks, sniffing attacks, and tracking.

Security solution proffered by Mohammad Dahman Alshehri and Farookh Khadeer Hussain [31] satisfies CT security requirements. Still, it has weak immunity towards A, I, Ay sans security exploitations like Relay attacks, Man in the Middle Attacks, DDoS, and viruses.

Security methods implied by Priyanka et al. [13], Munkenyi Mukhandi et al. [5], and Pooja Shree Singh and Vineet Khanna [32] have security provisions for Integrity security requirements, but the model proposed by Munkenyi Mukhandi et al. [5] having additional provisions for authenticity in Industrial IoT environment robotic setups where encryption mechanisms are integrated using MQTT protocols. Priyanka et al. [13] has proposed strong cryptographic securing methods to avert the Integrity based attacks. Security solution proffered by Pooja Shree Singh and Vineet Khanna [32] implies MFCC security coefficients to ensure the confidentiality and integrity security requirements. In Hongsong Chen et al. [33] proffered model, availability and trust security requirements are satisfied by Hilbert-Huang transformation but are exploitable in C, I, and Ay security parameters.

5 Result and discussion

The result derived from the aforementioned comparative analysis states that protocol-based security solutions cover up most of the IoT attack surfaces. Protocols like COAP and DDS protocols provide effective immunity against the prominent attack like DDoS attack and botnet attacks through secured means applied over Data Link and Transport layers. Novice methods are derived in the case of SigFOX and EnOcean novel protocols that avert new threat issues like unsynchronous code definition and weak payload encryption threats through a unique encryption method. MQTT and BLE, the lightweight protocols, have also emerged to provide an effective solution against the threats relative to malicious node and Man in the middle attacks. To avert the modifications brought in the IoT devices through physical attacks, there is a provision of Physically Unclonable Function [67] protocols that are imbibed in the specially designed PUF chip mounted on the IoT devices. Its unique authentication mechanism based on the PUFs makes it a formidable option against threats borne out of physical attacks. Similarly, based on these protocols and standards, the comparative analysis is projected for the security models. Security models depict the novel usage of encryption methods, machine learning methods [68], blockchain [69], and socket programming to ensure the confidentiality, integrity, authenticity, availability, and trust-based security requirements in the IoT environment. Divisive security management proves to be beneficial for easier management of the security methods,

Table 5 Security models with respect to security requirements

Proposed security model	Technique used	Confidentiality (C)	Integrity (I)	Availability (A)	Trust (T)	Authenticity (Ay)
[21]	Data encryption method				✓	✓
[22]	Fuzzy-logic based algorithmic method	✓			✓	
[23]	A multi-level data encryption method	✓	✓			
[24]	Mathematical evaluation method			✓	✓	
[20]	Block chain-based authentication method					✓
[26]	Cryptographic based data encryption method		✓			✓
[27]	Socket programming	✓	✓			✓

as well as enhances the effectiveness in most of the proffered solutions.

6 Conclusion

This work highlighted the recent security trends in the IoT network domain by surveying the newly proffered models, protocols, and encryption methods implied in securing the IoT network. Our research findings on security risks in IoT emphasize the extension of the attack surface of the IoT threats and vulnerabilities in protocol-based and data-based attacks, which conveys the fact that conventional means are no longer as efficient as they were earlier against dynamic attacks prevalent in heterogeneous IoT environments like malicious node, DDoS attack, and botnet attacks. Investigations of contemporary research models show that majority of security solutions are sought through the implication of alternative forms of encryption methods, which have proved to be effective in securing communication channel attack surfaces in IoT and promoting lower energy consumption in the process. Integration of technologies like machine learning, artificial intelligence-based fuzzy logic methods, elliptical cryptographic functions, and blockchain has assisted in firming the security of the IoT networks. On the negative side, it has increased the complexity factor of the entire system. Because of the high level of abstraction of such complex solutions, the transparency in the intent of security provisions has decreased. In this work, efforts have been made to address the evolution of existing communication technologies, protocols, and internationally accepted worldwide standards, relentless efforts that have been (and are being) made by the scientific researchers globally in antecedent discussed topics. Still, there is always a scope of exploration.

Author contributions Rachit has done the major work under the supervision of—SB and PRR.

Code availability Not applicable.

Compliance with ethical standards

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

Availability of data and material Not applicable.

References

1. Ashton K (2009) That Internet of Things thing. RFID J 22:97–114
2. Wan J, Tang S, Shu Z, Li D, Wang S, Imran M, Vasilakos AV (2016) Software-defined industrial internet of things in the context of industry. IEEE Sens J 16(20):7373–7380
3. Mavrogiorgou A, Kiourtis A, Perakis K, Pitsios S, Kyriazis D (2019) IoT in healthcare: achieving interoperability of high-quality data acquired by IoT medical devices. Sensors 19(9):1978
4. Lemayian JP, Al-Turjman F (2019) Intelligent IoT communication in smart environments: an overview. In: Artificial Intelligence in IoT. Springer, Cham, pp 207–221
5. Mukhandi M, David P, Pereira S, and MS Couceiro (2019) A novel solution for securing robot communications based on the MQTT protocol and ROS. In: IEEE/SICE International Symposium on System Integration (SII), pp 608–613
6. Rutten E, Marchand N, Simon D (2017) Feedback control as MAPE-K loop in autonomic computing. Software engineering for self-adaptive systems III Assurances. Springer, Cham, pp 349–373
7. Sinh D, Le LV, Lin BSP, Tung LP (2018) SDN/NFV—a new approach of deploying network infrastructure for IoT. In: Wireless and optical communication conference (WOCC), IEEE, 27th, pp 1–5
8. Safkhani M, Bagheri N (2017) Passive secret disclosure attack on an ultralightweight authentication protocol for internet of things. J Supercomput 73(8):3579–3585
9. Coman FL, Malarski KM, Petersen MN, Ruepp S (2019) Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In: 2019 Global IoT Summit (GIoTS), IEEE, pp 1–6
10. Sidorov M, Ong MT, Sridharan RV, Nakamura J, Ohmura R, Khor JH (2019) Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. IEEE Access 7:7273–7285
11. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M (2020) Internet of Things (IoT) enabling technologies, requirements, and security challenges. Advances in data and information sciences. Springer, Singapore, pp 119–126
12. Wang Li, Dinghao Wu (2019) Bridging the gap between security tools and SDN controllers. ICST Trans Secur Saf 5(17):156242
13. Urla PA, Mohan G, Tyagi S, Pai SN (2019) A novel approach for security of data in IoT environment. In: Computing and network sustainability. Springer, Singaporem, pp 251–259
14. Abdul-Ghani Hezam A, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Comput Sci Appl 9:355–373
15. Sharma K, Bhatt S (2019) SQL injection attacks-a systematic review. Int J Inf Comput Secur 11(4–5):493–509
16. Jaiswal S, D Gupta (2017) Security requirements for internet of things (IoT). In: Proceedings of International Conference on Communication and Networks, Springer, Singapore, pp 419–427
17. Radanliev P, De Roure DC, Nurse JRC, Montalvo RM, Cannady S, Santos O, Burnap P, Maple C (2020) Future developments in

standardisation of cyber risk in the Internet of Things (IoT). SN Appl Sci 2(2):169
18. Sood K, Shui Yu, Xiang Y (2016) Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review. IEEE Internet Things J 3(4):453–463
19. Li Y, Chen M (2015) Software-defined network function virtualization: a survey. IEEE Access 3:2542–2553
20. Bhattacharjya A, Zhong X, Wang J, and Li X (2019) Security challenges and concerns of Internet of Things (IoT). In: Cyber-Physical Systems: architecture, security and application, Springer, Cham, pp 153–185
21. Capellupo M, Liranzo J, Bhuiyan MZA, Hayajneh T, Wang G (2017) Security and attack vector analysis of IoT devices. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, pp 593–606
22. Vervier PA, Shen Y (2018) Before toasters rise up: a view into the emerging iot threat landscape. In: International Symposium on Research in Attacks, Intrusions, and Defenses, Springer, Cham, pp 556–576
23. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
24. Wang K-H, Chen C-M, Fang W, Tsu-Yang Wu (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. J Supercomput 74(1):65–70
25. Singh S, Sharma PK, Moon SY, Park JH (2017) Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Humaniz Comput. https://doi.org/10.1007/s12652-017-0494-4
26. Grooby S, Dargahi T, Dehghantanha A (2019) A bibliometric analysis of authentication and access control in IoT devices. Handbook of big data and IoT security. Springer, Cham, pp 25–51
27. Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. Digital twin technologies and smart cities. Springer, Cham, pp 123–149
28. Bembe M, Abu-Mahfouz A, Masonta M, Ngqondi T (2019) A survey on low-power wide area networks for IoT applications. Telecommun Syst 71(2):249–274
29. Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint
30. Zhang X, Wen F (2019) An novel anonymous user WSN authentication for Internet of Things. Soft Comput 23(14):5683–5691
31. Alshehri MD, Hussain FK (2019) A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101(7):791–818
32. Singh P S, and V Khanna (2019) A MFCC based Novel approach of User Authentication in IOT. In: 2nd International Conference on Emerging Trends in Engineering and Applied Science, ISSN: 2454-4248, 5(1)
33. Chen H, Meng C, Shan Z, Zhongchuan Fu, Bhargava BK (2019) A Novel low-rate denial of service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang transformation and trust evaluation. IEEE Access 7:32853–32866
34. Aldaej A (2019) Enhancing cyber security in modern Internet of things (IoT) using intrusion prevention algorithm for IoT (IPAI). IEEE Access. https://doi.org/10.1109/ACCESS.2019.2893445
35. Roesch M (1999) Snort: lightweight intrusion detection for networks. In: 13th Systems Administration Conference on LISA, pp 229–238
36. (OISF), Open information security foundation: Suricata. https://suricata-ids.org/
37. Paxson V (1999) Bro: a system for detecting network intruders in real-time. Comput Netw 31(23–24):2435–2463
38. Collen A, Nijdam NA, Augusto-Gonzalez J, Katsikas SK, Giannoutakis KM, Spathoulas G, Gelenbe E, Votis K, Tzovaras D, Ghavami N, Volkamer M (2018) Ghost-safe-guarding home IoT environments with personalised real-time risk control. International ISCIS Security Workshop. Springer, Cham, pp 68–78
39. Gubbi J, Buyya R, Marusic S, Palaniswami M (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. Futur Gener Comput Syst 29(7):1645–1660
40. Gresak E, Voznak M (2018). Protecting gateway from abp replay attack on lorawan. In: International Conference on Advanced Engineering Theory and Applications, Springer, Cham, pp 400–408
41. Pallavi S, Anantha Narayanan V (2019) An overview of practical attacks on BLE Based IOT devices and their security. In: 2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, pp 694–698
42. Hunkeler U, Truong H L, Stanford-Clark A (2008) MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. In: 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08), IEEE, pp 791–798
43. McAteer IN, Malik MI, Baig Z, Hannay P (2017) Security vulnerabilities and cyber threat analysis of the AMQP protocol for the internet of things. In: Valli C (Ed). The Proceedings of 15th Australian Information Security Management Conference, 5–6 December 2017, Edith Cowan University, Perth, Western Australia, pp 70–80
44. Randhawa RH, Hameed A, Mian AN (2019) Energy efficient cross-layer approach for object security of CoAP for IoT devices. Ad Hoc Netw 92:101761
45. Beckman K, Reininger J (2018) Adaptation of the DDS security standard for resource-constrained sensor networks. In: 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), IEEE, pp 1–4
46. Sethia D, Gupta D, Saran H (2018) NFC secure element-based mutual authentication and attestation for IoT access. IEEE Trans Consum Electron 64(4):470–479
47. Li S, Da Li X, Zhao S (2018) 5G Internet of Things: a survey. J Ind Inf Integr 10:1–9
48. Arfaoui G, Bisson P, Blom R, Borgaonkar R, Englund H, Félix E, Klaedtke F, Nakarmi PK, Näslund M, O'Hanlon P, Papay J, Suomalainen J, Surridge M, Wary JP, Zahariev ANDA (2018) A security architecture for 5G networks. IEEE Access 6:22466–22479
49. Mohanty SN, Ramya KC, Sheeba Rani S, Gupta D, Shankar K, Lakshmanaprabu SK, Khanna A (2020) An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. Futur Gener Comput Syst 102:1027–1037
50. Chatterjee S, Mukherjee R, Ghosh S, Ghosh D, Ghosh S, Mukherjee A (2017) Internet of Things and cognitive radio—Issues and challenges. In: 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), IEEE, pp 1–4
51. T Leppänen, J Riekki, M Liu, E Harjula, T Ojala (2014) Mobile agents-based smart objects for the internet of things. In: Internet of Things Based on Smart Objects. Springer, Cham, pp 29–48
52. Ahmad M, Younis T, Habib MA, Ashraf R, Ahmed SH (2019) A review of current security issues in Internet of Things. Recent trends and advances in wireless and IoT-enabled networks. Springer, Cham, pp 11–23
53. Dabbagh M, Rayes A (2019) Internet of Things security and privacy. Internet of Things from hype to reality. Springer, Cham, pp 211–238
54. A Soni, R Upadhyay, A Jain (2017) Internet of Things and wireless physical layer security: a survey. In: Computer Communication Networking and Internet Security Springer, Singapore, pp 115–123

55. Yıldırım G, Tatar Y (2017) On WSN heterogeneity in IoT and CPSs. In: 2017 International Conference on Computer Science and Engineering (UBMK), IEEE, pp 1020–1024
56. Hou J, Leilei Qu, Shi W (2019) A survey on internet of things security from data perspectives. Comput Netw 148:295–306
57. Xu H, Sgandurra D, Mayes K, Li P, Wang R (2017) Analysing the resilience of the internet of things against physical and proximity attacks. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, pp 291–301
58. Salim MM, Rathore S, Park JH (2019) Distributed denial of service attacks and its defenses in IoT: a survey. J Supercomput. https://doi.org/10.1007/s11227-019-02945-z
59. Stiawan D, Idris M, Malik RF, Nurmaini S, Alsharif N, Budiarto R (2019) Investigating Brute Force attack patterns in IoT network. J Electr Comput Eng. https://doi.org/10.1155/2019/4568368
60. Shen H, Shen J, Khan MK, Lee J-H (2017) Efficient RFID authentication using elliptic curve cryptography for the internet of things. Wireless Pers Commun 96(4):5253–5266
61. Na SJ, Hwang DY, Shin WS, Kim KH (2017) Scenario and countermeasure for replay attack using join request messages in lorawan, In: 2017 International Conference on Information Networking (ICOIN), pp 718–720
62. Om Kumar CU, Bhama PRKS (2019) Detecting and confronting flash attacks from IoT botnets. J Supercomput 75(12):8312–8338
63. Flauzac O, Gonzalez C, Nolot F (2016) Developing a distributed software defined networking testbed for IoT. Procedia Comput Sci 83:680–684
64. Sonar K, Upadhyay H (2014) A survey: DDOS attack on Internet of Things. Int J Eng Res Dev 10(11):58–63
65. Kolias C, Kambourakis G, Stavrou A, Voas J (2017) DDoS in the IoT: mirai and other botnets. Computer 50(7):80–84
66. Khursheed F, Sami-Ud-Din M, Sumra IA, Safder M (2020) A Review of Security Mechanism in internet of Things (IoT). In: 2020 3rd International Conference on Advancements in Computational Sciences (ICACS), IEEE, pp 1–9
67. Babaei A, Schiele G (2019) Physical unclonable functions in the Internet of Things: state of the art and open challenges. Sensors 19(14):3208
68. Mohamed T, Otsuka T, Ito T (2018) Towards machine learning based IoT intrusion detection service. In: International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Springer, Cham, pp 580–585
69. Miraz MH, Ali M (2018) Blockchain enabled enhanced IoT ecosystem security. International Conference for Emerging Technologies in Computing. Springer, Cham, pp 38–46