

## Internet of Things (IoT) applications security trends and challenges

Asif Ali Laghari<sup>1</sup> · Hang Li<sup>1</sup> · Abdullah Ayub Khan<sup>2</sup> · Yin Shoulin<sup>1</sup> · Shahid Karim<sup>3</sup> · Muhammad Adnan Kaim Khani<sup>4</sup>

Received: 8 August 2024 / Accepted: 17 December 2024

Published online: 24 December 2024

© The Author(s) 2024 OPEN

### Abstract

The idea behind layered design is the foundation of the Internet of Things. Each tier uses a variety of technologies for capacity, preparation, and information transmission. With regard to the risks and vulnerabilities related to IoT-enabled devices, as well as potential assurance mechanisms in light of equipment constraints and novel information transfer techniques, this study attempts to analyze the current architecture of the Internet of Things. After that, we talk about IoT architecture and applications. The following is a list of effective real-time IoT applications that are now in use: Self-driving cars, traffic management systems, smart grids, logistic management hierarchies, environment monitoring, building safety applications, and many more are examples of emerging technologies. Specifically, we highlight the latest improvements and challenges associated with IoT security. Finally, we discuss the state-of-the-art research and its conclusions, as well as the outstanding problems for future IoT security research.

### Highlights

1. This research provides details of IoT architectures comparison and applications and its security.
2. Further, this work is based on the category's security attacks according to layers of IoT.
3. Challenges and limitations with solutions to previous work provided and open research issues are discussed for future research.

**Keywords** Internet of Things (IoT) · Privacy and security · Cloud computing (CC)

### 1 Introduction

The Internet of Things is poised to fundamentally alter how businesses generate and how individuals spend money on goods and management in every industry [1, 2]. Similar to internet services and personal computers before it, the Internet of Things promises to drastically alter how we create. IoT devices promise to reduce asset utilization and increase flexible chain productivity while simultaneously fine-tuning the nature of the goods sold and the benefits are given when combined with global broadband communication systems and massive information research [3]. The

---

✉ Asif Ali Laghari, asiflaghari@synu.edu.cn; ✉ Hang Li, lihang@synu.edu.cn; ✉ Yin Shoulin, yslin@synu.edu.cn; Abdullah Ayub Khan, abdullahayub.bukc@bahria.edu.pk; Shahid Karim, sk@eurasia.edu; Muhammad Adnan Kaim Khani, adnankk12@gmail.com |

<sup>1</sup>Software College, Shenyang Normal University, Shenyang, China. <sup>2</sup>Department of Computer Science, Bahria University Karachi Campus, Karachi 75000, Pakistan. <sup>3</sup>School of Information Engineering, Xi'an Eurasia University, 710065, Shaanxi, Xian, China. <sup>4</sup>Department of Computer Science, Ilma University, Karachi, Pakistan.



economic and operational structures of emerging industries like farming and assembly are beginning to be disrupted by the Internet of Things [4]. Given the broadness of expected applications and device types from basic sensors that inactively screen a situation too complex arranged frameworks, for example, self-ruling vehicles navigating the world's interstates, the IoT is ready to carry new requests and consistency to a regularly confusing world [5, 6]. The IoT empowers better approaches to connect the advanced and physical universes; the cybersecurity hazard scene is growing [7]. The digital threat is not, at this point, limited to critical business information or frameworks, where associations have generally centered their cyber-security ventures; programmers are likewise focusing on devices outside conventional edges [8]. The precipitate volume of IoT devices, combined with their range of capacities, enormously increments expected weaknesses [9]. Add to this the effect numerous undermined devices can go live on the Internet, or solo instruments can also go on the physical world, and it gets more noticeable the developing test to cybersecurity practices [10]. Now is the ideal time for associations to rethink conventional threats and the executive's procedures and techniques regarding this growing threat scene [11].

IoT is a process or system of connected devices which can control through the network [12, 13]. The device can be mechanical or digital machines, which can run with the help of the internet without human interaction. In the broad term, it encompasses everything which runs through the internet through means of sensors and passes data by using the concept of cloud networking. However, with the emergence of Blockchain Technology provide a in-depth solution regarding infrastructure security. Recently, most of the organizations are moving on the mentioned platform in order to protect their data, even though the intercommunications [8–21].

The working IoT is connected to the cloud [14]. An IoT system consists of sensor-based devices that can talk to the cloud through connectivity. When the data has been taken, the software process it and perform the action which the user wants and hand if there is any user input is needed so through the user interface, the system gets user input by the user and for changes, the data is sent to the cloud for specific changes by the user and then back to the sensors or devices which are capable of performing an action which the user wanted [15].

The IoT based on 4 main components on which the IoT mechanism works, as shown in Fig. 1:

- Sensors devices
- Connectivity
- Data processing
- User interface

## 1.1 Sensor devices

A sensor is a small microchip embedded in devices that sense or collect environmental data [16]. It could be as simple as reading the temperature or collecting a bundle of information as collecting video data. For example, let us consider the mobile you use daily. The mobile contains sensors like a GPS controller, camera, gesture reader, etc.

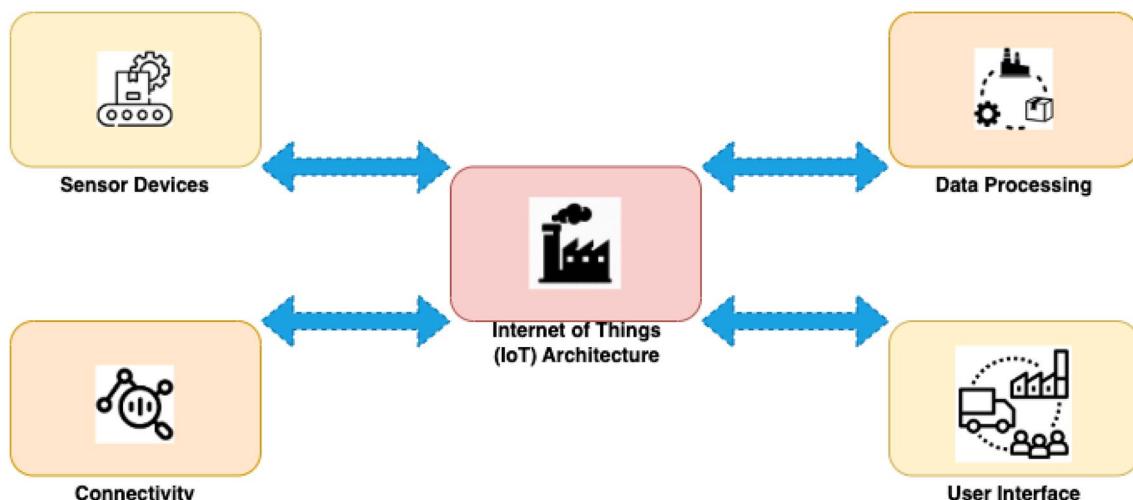


Fig. 1 Major Components of IoT Architecture

## 1.2 Connectivity

The second thing comes, which is essential, which is connectivity. The sensor needs a connection to the cloud for communication, like 5G. For this, several methods have been used depending on the hardware and the types of devices the user sets [17]. They can include cellular, Wi-Fi, GPS, satellite, LAN, WAN, or any connection. Each connection has limitations and bandwidth, so the user has to choose one of the better options for their relationship.

## 1.3 Data processing

The data gets to the cloud, so the software in the application performs some kind of processing on it, such as checking the temperature in a reasonable range and the house activity through cameras [18].

## 1.4 User interface

In the IoT framework, the user interface is crucial in managing IoT applications. Some rules are defined for the user [19]. For example, if the temperature is too high, an alert or message is sent to the user to check the temperature and set the environment. But in some contexts, there is also an automatic system available that checks the temperature, and on high alert, it automatically performs some actions and controls the condition, and it depends on the applications used in the IoT framework [20].

The main contribution of this paper is to give a comprehensive review of IoT security and challenges. The research work is based on the IoT architecture, applications and security. Additionally, security attacks categorize according to layers of IoT, and the paper explains several types of attacks in security challenges. Further, this research provides currently available security solutions for IoT systems, which are most important for secure IoT. Additionally, this research produces important challenges and open issues that need to consider for future research proposals for IoT security.

The rest of the paper is organized as follows. Section 2 explains the IoT architecture, and Sect. 3 provides details of popular IoT applications. Section 4 is based on the security categories, and Sect. 5 includes the security challenges IoT faces. Various solutions related to IoT security are discussed and analyzed in Sect. 6. Section 7 discusses the research challenges posing as the main hindrance to IoT security and their possible solutions before concluding the paper in Sect. 8.

## 2 IoT architecture

IoT is not just an internet-connected device; it is the technology IoT is the technology that builds a system capable of sensing and responding to the world without any human intervention. The IoT is generally working into four stages given in Fig. 2 (also discussed in Table 1); these stages are:

- i. Sensors and Actuators Devices
- ii. Internet Gateway and Data Acquisition System
- iii. Pre-Processing Edge IT
- iv. Cloud and Data center

### 2.1 Sensors and actuators devices

The first layer of these four stages is called Sensors and actuators [21]. The sensor collects data from an environment and converts it into usable data [22]. Smartphones are an example of this stage. Smartphones contain sensors that detect the earth's gravitational, allowing them to orient their screen depending on your position. Actuators are devices that can intervene in the physical reality that generates data—for example, shutting off an engine, switching off the light, and adjusting the room temperature.

These Senses and actuating stages help to adjust everything in the physical world and for information that requires deeper insight for more analysis. The data must be collected in a cloud-based system, as mentioned in Table 1. There is some sensors type applied in IoT.

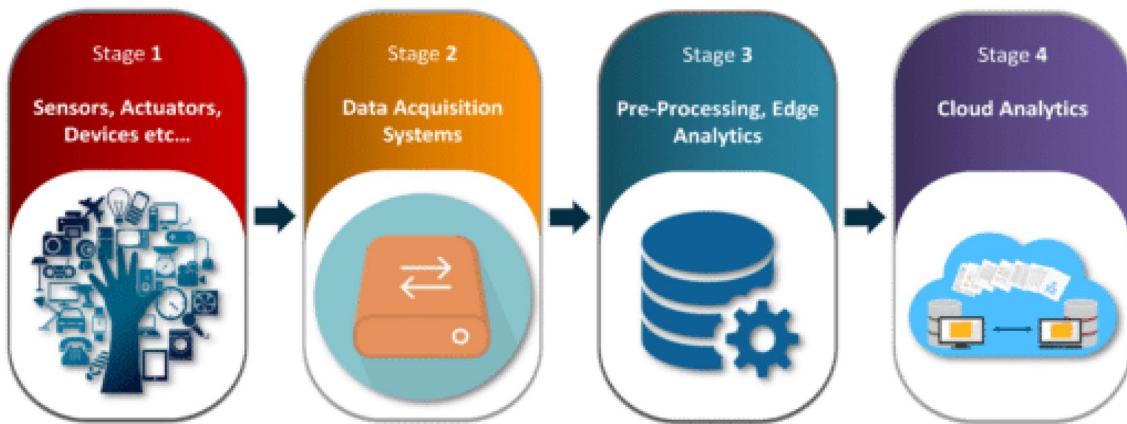


Fig. 2 Stages of IoT working

- Temperature Sensors
- Moisture IoT Sensors
- Light IoT Sensors
- Water Level IoT Sensors
- Image IoT Sensors

### 2.1.1 Temperature sensors

These sensors are found in every IoT case keeping track of the thermal condition of air, environment, machines, and other objects [23]. Temperature sensors are helpful in manufacturing warehouses, plantations, weather reports, and agriculture, where the soil temperature is highly monitored to balanced and provide maximum growth [24].

- *Thermistors*: Its resistance depends on the temperature. It's mostly used in electronics like an electronic thermometer.

### 2.1.2 Moisture IOT sensors

Widespread uses in the metrology station to report forecast weather, moisture, and humidity sensors are also employed in agriculture, food supply chain, and health monitor system [25].

- *Hair tension Moisture System* It is the oldest type of moisture sensor based on human and horsehair or cotton fibre. The fibre or hairs change their length upon contact with moisture. Pointer the reading on scale and connect with hair and fibre. These moisture sensors are cheap construction [26].

### 2.1.3 Light IOT sensors

Light sensors depend on the light intensity, and these are easily found in smart TV, Mobile phones, and Computer LEDs through up and down the brightness [27].

- *Photoresistors*: Its resistance changes through radiation because it's a photosensitive element. It is easily connected via analog light sensors. Lamps are an example of a photoresistor it turns automatically turn after Dark.

### 2.1.4 Water level monitoring sensors

Water level monitoring sensors are used in flood warning system for prediction and environmental protection in case any natural disaster is coming so it can send a warning [28].

**Table 1** The Usage of IoT Architecture to Build Different Run-Time Applications

| Major contribution(s)  | Method/methodology   | Gap analysis   | Similarity and difference with the proposed model  |
|--|--|--|--|
| The integration of Internet of Things (IoT), machine learning, and intelligent sensors for remote sensing data of agriculture [18] | This paper classified the role of sensors and their suitable usage in the field using a support vector machine (SVM). In this manner, the authors separated assessment according to the operational condition, such as soil quality, crop monitoring, harvesting, weeding, and sowing as follows: <ul style="list-style-type: none"> <li>• ESP-32</li> <li>• DHT-11</li> </ul> | <ul style="list-style-type: none"> <li>• Interoperable cross-chaining limitations</li> <li>• Scope of data protection issues</li> </ul>                                  | <ul style="list-style-type: none"> <li>• Public chain</li> <li>• Hash-encryption SHA-256 mechanism used</li> <li>• Wireless sensor inter-connectivity</li> </ul>                     |
| Spectral convolution network for hyperspectral image classification and remote sensing [19]  | The author of this paper proposed a model named "HRSIC", a novel spatial feature information classification using ResNet connections. However, the aim of this is to reduce the cause of degradation and increase depth  | <ul style="list-style-type: none"> <li>• Outsource computation is required</li> <li>• High resource consumption</li> <li>• Complex deep network structure</li> </ul>     | <ul style="list-style-type: none"> <li>• No security features are discussed</li> <li>• Permissionless network</li> <li>• Image-based remote sensing classification</li> </ul>        |
| An efficient prediction from remote sensing data by transfer learning mechanism [20]   | A new paradigm called YieldNet, a customized convolutional model based on neural networks, utilized that objective to transfer learning between a large-scale crop yield prediction using the share weight of the backbone feature extractor   | <ul style="list-style-type: none"> <li>• No standard is used to schedule transactions of remote sensing</li> <li>• A local data preservation strategy is used</li> </ul> | <ul style="list-style-type: none"> <li>• Real-time decision-making platform for stakeholder to maximize yield potential</li> <li>• Unsecure channel for data transmission</li> </ul> |

- *Optical Sensors*: a sensor that detects water level by the reflection of light in the prism.

### 2.1.5 Image sensors

Image IoT Sensors are used whenever the need for the smart devices to look the happening in the surrounding it used in security systems and military equipment, and other things [29].

- *Active Pixels Sensor*: DSLR, webcams, Digital X-Ray is an example of active pixels sensors.

Actuators are separated in four categories.

- *Linear*: Motion of object and element in straight line.
- *Motors*: Rotational Components and whole object
- *Relays*: Electromagnet Based Actuators
- *Solenoids*: used in home appliances.

## 2.2 Internet gateway and data acquisition system

Data from the sensor come in analogue form, so it must be converted into digital form; the Data acquisition system (DAS) is the tool to aggregate and convert it into digital format. It could happen in the 2nd stage of IoT architecture, called internet gateway [30, 31]. Data acquisition devices help machines more innovative analyze actual data. It is used in industrial and commercial electronics and environmental and scientific equipment to capture signals and environmental conditions.

Data acquisition consists of:

- Signal Condition
- Recorder and Display Devices
- Data handling
- Multiplexing
- Transmission and storage
- *Signal Condition*: Output signals of transducers are very weak signals which cannot be used for further processing [32]. Various types of signals conditioner are used to make the signals strong, like filters AND Modifiers.
- *Multiplexing*: Accept multiple analog inputs and provide a single output signal according to the requirement.
- *Display Devices*: Data is displayed in a suitable form to monitor the input signals like Oscilloscopes, Numerical Display, and Panel Meter. Data can be permanently or temporarily stored and recorded in Optical or ultraviolet recorders.

## 2.3 Edge IoT

It is the 3rd Stage of IoT Architecture. The prepared data is transferred to the IT World [33, 34]. This stage is closely linked to the previous Phases of IoT Architecture stages, sensors and actuators, because the location of the edge system is located where sensors and actuators are located. Edge devices in IOT can also benefit from high-class IoT projects. It provides high speed in data transfer cloud platforms and performs faster response time and extra flexibility in data processing. There are Some Components of Edge Computing in IoT, as mentioned in Table 1.

- Machine learning (ML) and Artificial Intelligence
- Complex Event Processing (CEP)
- Machine Learning (ML) and Artificial Intelligence:

The Idea of Machine learning Models are built by Using complicated, so it turns into artificial intelligence AI. Most edge IoT devices support machine learning ML models [35]—some Edge devices are Delivered directly to IoT Devices.

- Complex Event Processing:

Complex and Event Processing (CEP) Services and Software are used in several Operational technologies [36]. CEP takes data from multiple sensors and acts on a specific platform. CEP and Pattern Models push edge devices. The most common technology is the Apache storm.

## 2.4 Cloud and data centre

It is the 4th stage of IoT architecture. The primary process happens in the data center and cloud [37]. It makes the system more secure and robust IT System. There are some stages in the cloud.

- *Cloud Discovery*: it helps data stored inside the on-premise or data warehouse.
- *Cloud Data Migration*: In this system, you need to decide on what type of data load into the cloud, how more efficient is.
- *Cloud Data Maturity*: At this point, you are ready to make the harder cloud work and hone your cloud data management strategy. Cloud data Maturity technology is the second nature of data professionals [38]. But right now, you have made solid type cloud data use in cases, improved analytics, and reporting for part of the business.

## 3 IoT applications

IoT's motive is to bring changes to our life for the betterment. With new wireless networks, revolutionary computing capabilities, and superior sensors, the IoT will hope to become a frontier in the race and share of the wallet. At the same time, some needless about the current hype about IoT is the biggest. Nowadays, many companies announce prediction IoT-based devices, and we discuss a significantly trending IOT app right now [39] and also given in type in Fig. 3.

Now, we will try to think about intelligence devices, for example, traffic cameras. Well, the work of the camera is to monitor the street for accidents, weather, and other stuff, and the data will communicate with a standard gateway [40, 41]. This gateway receives information from the camera, depending on the info extended comprehensive traffic monitoring system. The application of IoT is given below:

### 3.1 Smart home

A smart home is one of the best examples of an IoT application [42]. Smart home searches on the Internet are around 60 k monthly [43]. Well, nowadays, more than 256 companies are active in the term smart home than any other app

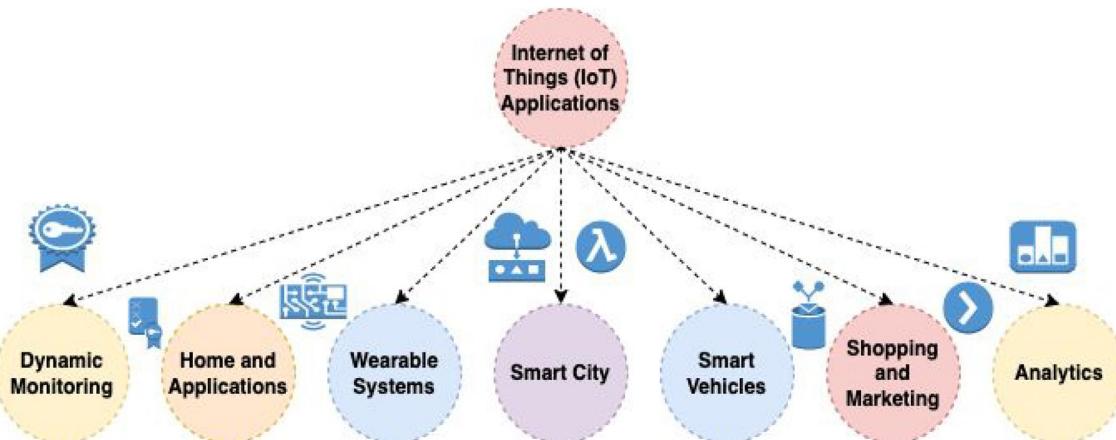


Fig. 3 IoT applications

in the field of the IoT is enormous [44]. Well, the investment is around \$2.5bn in intelligent home startups. Some of the names in the list are Alert Me or Nest, as well as several Multinational Corporation as Samsung or Apple.

### 3.2 Smart city

A smart home is also one of the best applications in the field of application of IoT. This term has a wide variety, from waste management and traffic management environmental monitoring to water distribution. The popularity of this term is it promises to solve all the major problems the city is facing right now [45]. It also helps reduce noise and pollution and will do their part in the help of towns.

### 3.3 Smart Grid

A smart grid is also one of the best apps for IoT [46]. The coming smart grid has promised to collect data on related behaviors of electricity consumers and suppliers in an automated fashion to improve efficiency and reliability [47]. We can also highlight the concept of popularity will be around 41 k on Google searches [48]. Well, on the other endless number of a tweet, around 100/month, that Indicates people don't want to say or don't have anything to say about it.

### 3.4 Car connected

The evolution of the car connected is coming slowly. We at the current progress suggest that the cycle of the automotive industry typically takes around 3–4 years; however, we have not seen anything related to car connection. Some risk-taker startup is working on car connected project, and this is a good sign for this project. Some well-known giants have announced connected cars like Apple, Microsoft, and Google [49–51].

### 3.5 Health connected

Connected health remains the sleeping giant of IoT applications [52]. Well, when we talk about the concept of intelligent medical devices and connected healthcare systems, they have tremendous potential not just in terms of the firm but as an individual. Till now, this has been done sparingly with the help of the use case and startup; the scale is still to be seen.

### 3.6 Supply smart chain

We all know the supply chain has already been more intelligent for years. The record of tracking goods from the road and getting the supplier to exchange inventory information in the market for many years. It's a prediction that with the help of IoT, it will take a boost. So far, it shows that its popularity is similar to an intelligent home [53].

### 3.7 Industrial net

It is also a great application of the IoT. While many market types of research, such as Cisco, see the industrial internet as an IOT concept with huge potential, its popularity only reaches the masses as wearable's does [54].

#### 3.7.1 Wearable

The wearable is a significantly trending topic too. As a customer, you waited for the new release of Apple's new smart-watch. We can see a vast wearable innovation to be excited about, like the Looksee bracelet [44]. One of the best startups, wearable maker Jawbone is one of the hugely funded till now. I have approximately 500 million US dollars! [55].

### 3.7.2 Personal assistance

We have been familiar with smartphone assistance for many years; now, this system is available in smart homes, and as we know, there is Amazon's famous home personal assistant, Alexa [56]. This individual assistance lets us control our smart home digitally and virtually [57].

### 3.7.3 Video doorbells

Another advanced technology of IoT is the video doorbell. Video doorbells allow the user to access the call from the video doorbells when a person is reached at the door. It also enables users to access when they want to lock and unlock their homes by a smartphone app. One additional feature of that is when some are continuously walking around the house video doorbell notifies the homeowner, and we can also set a time on that video; any notification or bell is not allowed at that particular time [58].

### 3.7.4 Smart locks

In today's world crime ratio is increasing day by day due to poverty and thief, and many more reasons. At that time, smart locks were one of the advanced technologies of smart homes. Through this, we easily lock the lock by our mobile app, even sitting in the office, car, or anywhere [59].

### 3.7.5 Traffic monitoring

IoT in traffic monitoring and management is helpful for us because it manages the traffic in smart cities [60]. When we are on the sensor of our smartphone during the trip, it retrieves the data and forwards data to our car through an app like Google map; this will give us the information and show all the different routes with the present traffic; after observing all the route, it will provide us with the best route with minimum traffic and also tell us the time of arrival, distance and destination.

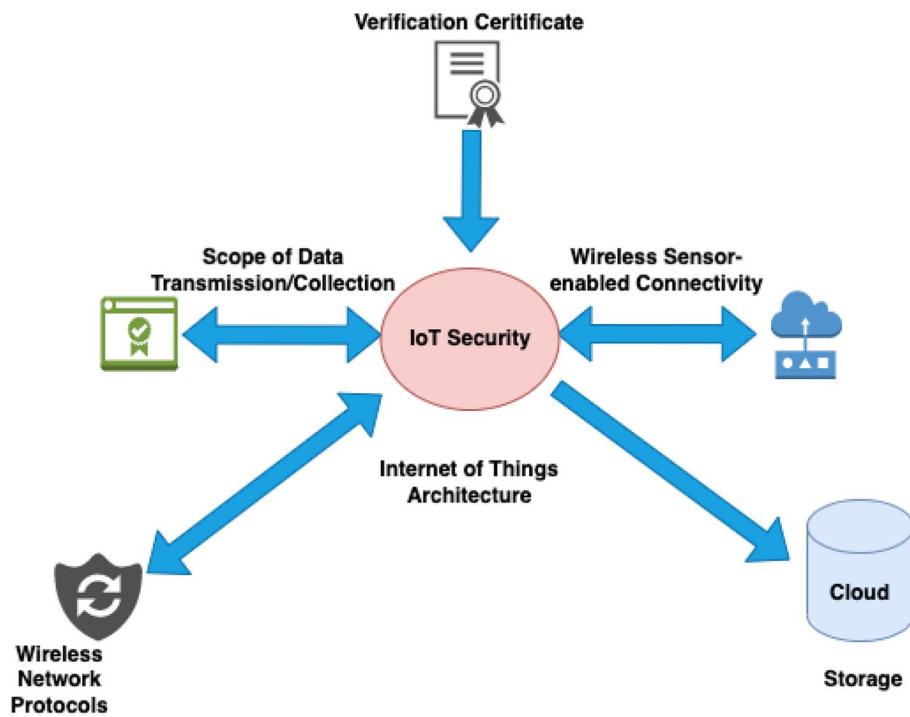
### 3.7.6 Smart watches

Smart is one another example of the IoT, smartwatch not only shows the time, it shows your heartbeats, pulse time, calories burned, timer, and the steps you run and walk; it will tell us all these things, but for smartwatch, we also need a smart mobile in which we install an app that comes in our watch, through the mobile application we also have the access of our watch, it works on the sensors and the relationship between the IoT [61–63].

## 4 Categories of IoT security

The number of applications connected through the Internet over the year and the ratio is very high. The report says that almost 30 billion devices connected will mark through the Internet and 75 billion onwards to 2025 [64]. So, the ratio of the number of devices is more than we expected, so for a better experience by the user, we have to do our best in security for the application. Thus, to protect these devices and to reduce cyber-attacks and hacking problems, as shown in Fig. 4; we must build some mechanism or use some better system for protecting our devices from unauthorized access or stealing of data from devices [65], (some of the major IoT security state-of-the-art methods are discussed in Table 2 as well).

**Fig. 4** Working Hierarchy of IoT Security



#### 4.1 Categorizing risks

Deciding the proper degree of security limitations for a given item or administration is subject to its related risk arrangement. For evident reasons, a threat with a likely death toll sway requires a more substantial degree of security than the threat presented by an undermined resource following a tag on a bed of toothpaste [66]. Be that as it may, instead of spotlighting exclusively on inconsistent results, it's smarter to consider explicit IoT devices concerning use cases and management [67]. To run security level Utilizing threat classifications, conversations, and choices assist with wiping out the limit of security system irregularities. It additionally gives a way to create layouts and instruments that associations could utilize to form the use of IoT security limitations, strategies, and techniques repeatable. Threat classifications can diminish the mystery included while making security prototypes for an undeniably differing and associated scene of items and management [68]. A significant initial phase in ordering the IoT chances is to characterize it. In wide terms, the IoT change is controlled by the expected effects of an undermined device, be they execution, managerial, physical (wellbeing and security), or substantial. IoT chance fluctuates extraordinarily by sending and contrasting somewhat from conventional Information Technology threats, which has concentrated on avoiding system interruption and information exfiltration from past the corporate firewall. The IoT likewise varies largely from traditional Information Technology due to its network model [69]. Numerous corporate IT foundations are planned as semi-private systems with negligible to the outside-the-touch points world, explicitly, the Internet. The network's system security is commonly authorized at the system edges and on the inner system end focuses, for example, Personal Computers and associated printers, by observing for and halting inbounds assaults [70]. Stable accepted procedures and advancements are promptly accessible to assist associations with countering these dangers.

Several security intrusions are associated with the layers of IoT; each layer is weak against various security attacks [71]. These attacks are frequently unique or separated and are regularly produced by an inside or external source [72]. The dynamic attack will instantly prevent the organization, while an inactive attack can take information from the IoT mastermind discreetly without interfering with the organization. DoS trap can impact each layer of IoT, making the organizations of the framework unavailable [73]. During this fragment, we will notice security concerns associated with every layer of the IoT.

**Table 2** Discussion Regarding IoT Architectural Security

| Major contribution (s)   | Method/methodology   | Gap analysis   | Similarity and difference with the proposed model  |
|--|--|--|--|
| Fractional crops remote sensing data classification using convolutional deep network [21]  | This paper proposed FGCN, a predefine convolutional network involve with fractional Gabor features, which is an efficient fusion method that comprehensively extracted multi-features in the remote sensing data | <ul style="list-style-type: none"> <li>Semantic change features problem</li> <li>Light detection and ranging data processing limitations</li> <li>Cost of data optimization</li> </ul>                                   | <ul style="list-style-type: none"> <li>A multi-sensor platform is proposed</li> <li>Consume more computation because of complex network structure while training</li> </ul>                  |
| Risk assessment of futuristic disaster in smart cities using remote sensing data classification with multicriteria approach [22] | The importance of remote sensing data in risk assessment and futuristic developments is presented by E. Psomiadis et al. The main objective of this study is highlighted as follows:                             | <ul style="list-style-type: none"> <li>Upstream and downstream of data transmission via the centralized network related problem</li> <li>Cost of network bandwidth</li> <li>No data privacy mechanism follows</li> </ul> | <ul style="list-style-type: none"> <li>Fog-enabling computation is required for high-resolution orthophoto images</li> <li>Leak of record keeping and preservation mechanism used</li> </ul> |
| Scene classification by remote sensing data classification using deep learning network for dynamic monitoring [23]               | Remote sensing data utilized to create geographical information system for efficient classification of flooded areas, impacts, and related disasters   | <ul style="list-style-type: none"> <li>Computational complexity</li> <li>Performance errors in terms of search network and balance particle choices</li> </ul>   | <ul style="list-style-type: none"> <li>Hierarchical extraction processes</li> <li>Scene classification</li> <li>A complex data structure is presented</li> </ul>                             |

## 4.2 Perception layer

The perception layer of IoT is the most sensitive, where most attacks are launched; the centers on this layer by and massive include external conditions, which makes it the most adored attacking region in IoT orchestration [74]. Distant development is used to send the sign between the centers of IoT; like this, its adequacy is typically reduced by waves disrupting impact. Recognitions to the surface sending of the IoT sensors, an attacker can adjust the gear of the devices [75, 76]. Also, the devices on the perception layer include sensors, scanner label peruses, or RFID, whose estimation limit and power use are extraordinarily low, which makes them attackable. Evaluating is regularly used to abuse the mystery of this layer, which may exchange character information about IoT devices. The center catch attack can be prepared on this layer, during which the attacker expects command over the center point and focuses all the data from the center point. Moreover, the attacker can change center points on this layer.

## 4.3 Network layer

DoS attacks are frequently executed viably on the network layer [77]. Inactive watching and framework inspecting are furthermore ordinary on the network layer. Transferring data from devices and a neighborhood of remote access offers an increase in those sorts of attacks [78]. Just in case a spy can grow the entering material of IoT devices, secure correspondence is getting to tend up around then. An appropriate segment of crucial exchange should be guaranteed for the secure communication of IoT devices [79]. The communication between the IoT devices is almost the same because of the web; the rationale is that it's not confined to machines but to humans. The likeness is that the significant issue for the security of IoT devices, as a consequence of the heterogeneity of the IoT devices at these available shows, cannot be used. The range limits need to, in like manner, be extended to shape IoT devices sufficiently prepared to influence any particular condition which may impact their security.

## 4.4 Application layer

There are no overall standards and courses of action for advancing IoT applications; there are various security issues related to IoT applications [80]. There are multiple applications, and every application has a unique procedure for approval, making it hard to ensure affirmation and security. The growing number of related attackers sharing knowledge will cause an overhead. This overhead will cause the unavailability of IoT organizations. Throughout the application development pattern, another problem must be seen as that's who is getting to be the machine's customer and thus the way they accompany the devices. There should be a few expenses for the purchasers that they are getting to be used to control the knowledge and to infer what data should be revealed and who are getting to be the customer of knowledge once they go to use the knowledge.

# 5 IoT security challenges

As more actions handle the IoT, an enormous gathering of new security faults will arise. The extended risk can be recognized to create restrictions and failed opportunities to improve security. Here are driving IoT security challenges that try must address.

## 5.1 The rise of botnets

In recent years, there has been an arose of botnets between IoT devices; when botnet exits when hackers remotely control IoT devices by accessing through a vulnerable port and then controlling them, and then they are for illegal purposes, the decentralized organization could enable and choose them as part of a botnet. Still, the main problem is that many companies need more -real-time security to track the hacker [81, 82].

## 5.2 More IoT devices

In the recent 2000 or a few years ago, the professional was mainly focused on completely protecting mobile devices or computers, but now there is a conflict of IoT devices. well, a recent survey tells that there are over 7 billion devices across

the world and that number is increasing day by day and is going towards 20 billion by 2020, so that main problem is that more IoT devices mean more security issue and that why it challenges for the security professional [83].

### 5.3 Brute forcing/default password

The Mirai bot is mostly used in some of the biggest and most distributed DDoS attacks, and because of that some issues arises when shipping devices with default passwords and intentionally not telling the consumer to change the password as soon as they receive it, there some government which do not permit manufacturers to sell devices with default password like admin as username and same as password [84]. Why Mirai vulnerability was so in working because it identifies the vulnerable devices and uses default credentials and then infects them.

### 5.4 Malware and ransomware

As you know, the number of IoT-connected devices is rising, so malware and ransomware use to exploit them; ransomware entirely relies on encryption and locks out the user of gadgets. A merge of malware and ransomware creates a wholly new type of attack and hybridization [85]. Ransomware attacks could focus on limiting the traffic flow, disabling device functionality, and stealing user data.

### 5.5 Botnets aiming at cryptocurrency

Due to the popularity of cryptocurrency, there is also an increase in the craze of hacking to get crypto cash; new technology such as blockchain has been launched to avoid hacking, but there is still a problem in app development using blockchain, which is running itself [86]. Different methods are used to extract credentials, but social engineering is common. Many users use VPN to divert IP and video cameras to mine crypto, such as the open-source monero, which is a digital currency mined with IoT devices.

### 5.6 Home invasions

The scariest is that IoT is mainly installed in houses, and it causes home invasions because of web connectivity and its use in home automation. The security of these IoT devices is a big problem as they can expose your IP address and pinpoint it; the most precious information cans old to hackers on the dark web, and they use it to blackmail another when you are using IoT in your security system. There is a chance that it will leave houses at the exploitable level [87].

### 5.7 Remote vehicle access

Apart from home threats, there is a chance hijack of your car is a threat. Some car technologies are on the verge of becoming a reality by connecting to IoT devices, and it is associated with IoT; hackers can have control of your car by accessing it, and it is a lethal vulnerable [88].

### 5.8 Lack of encryption

Ignoring the way that encryption is an extraordinary strategy to shield developers from getting to data, it is, moreover, one of the primary IoT security challenges [89]. These devices do not have the limit and deal with capacities that would be found on a standard PC. The result is a development in traps where software engineers can, without a remarkable stretch, control the estimations expected for protection. But encryption won't be a security asset if an undertaking settles this issue.

### 5.9 Outdated legacy security

Despite the shortcomings of the IoT devices, the other worry is with interconnected legacy systems. In an undertaking with many IoT devices, legacy advances may give off an impression of being bizarre [90]. An entrance of an IoT device could, like a manner, realize a break of a legacy structure that needs current security standards.

## 5.10 Unreliable threat detection methods

Endeavors have different procedures for distinguishing data breaks, including spotting standard pointers, watching customer activity, and other security shows [91]. Regardless, due to the number of IoT devices and the complications of each device's usual danger, commitment systems could be less trustworthy yet, instead, even more of a test.

## 5.11 Small scale attacks in IoT

Regardless of how security specialists are revolved around hindering massive degree attacks, the little extension ambushes could be among the more certifiable IoT security challenges. Little extension attacks are all the more difficult to distinguish and could, without a doubt, occur without endeavoring to observe them [92]. Developers can infiltrate common undertakings, for instance, printers and cameras.

## 5.12 Phishing attacks

Phishing starts with security stresses and overall endeavor advancements, and IoT gadgets address the latest ambush vector [93]. Developers could give a sign to an IoT device that triggers different troubles. Regardless of how it is one of the most broadly perceived kinds of security ambushes, and it might be ended, various affiliations disregard to set up their workers about the latest phishing threats fittingly.

## 5.13 Inability to predict threats

Security specialists must be proactive in hindering IoT security breaks before they happen. Regardless, a couple of tries may need to improve on a solid organizational structure that could screen activity and give pieces of information about likely threats [94]. With this sort of game plan, an undertaking will have the ability to spot probably breaks early.

## 5.14 Infrequent updates

Programming updates are one way that IT experts guarantee that PCs and cell phones are as sure as anyone might imagine. Some IoT devices may need more than the measure of programming updates that different advances may get [95]. Likewise, ventures battle to give essential security updates to IoT devices in the field.

## 5.15 User privacy

Actions must ensure client information (that goes for both an organization's outside and inner clients). It is a worry because numerous specialists are utilizing IoT devices given by their managers [96]. At the point when a threat occurs, and private information is undermined, an endeavor's notoriety would endure a top dog, which is the reason this is one of the best IoT security challenges that cannot be disregarded.

## 5.16 Weak default password

Several IoT devices have unique default passwords that are weak [97]. Even though it is recommended that you modify the passwords, a few IT managers ignore to make this essential step. A powerless, simple-to-figure secret word could leave an IoT device helpless against a savage power attack.

# 6 IoT security solutions

Technological advancement also produces security solutions as some people use it to spread negativity. The increase in the demand for IoT applications makes sense because it has a vast concept, as it has raised many security issues related to privacy issues, unauthorized access, cyber-attack, and data hacking [98]. Many security experts use strong

passwords and other tricks to save IoT devices. However, hackers can exploit many loopholes to gain remote access and steal the data of the user or the device.

The increase in cyber threats in the IoT application and devices gives importance to and highlights the issue that some essential practices should be made to solve these problems [99]. The DoS attack and many server attacks open the window that security issue is more accurate for IoT applications. So many solutions are provided by experts and other security agencies to protect user identity and data.

## 6.1 LWPAN security

IEEE 802.15.4, Specification for Low-Rate Wireless Networks, is the basis for Low-Power Wireless Personal Area Networks. The standard is introduced with many systems, including LWPAN, ZigBee, Z-Wave, EnOcean (State Protocols for Building and House Automation) and SNAP [100]. IPv6 and IEEE 802.15.4 merge the concept of LWPAN. The home automation systems thread protocol even reaches LWPAN [101]. One or more of the LWPAN networks, the edge router, which regulates the entry and performance of the LWPAN, are linked to the Internet. In the configuration of the RPL, routing problems in 6LoWPAN are discussed by the IETF-ROLL task force. The protection in the LWPAN networks must only restrict access to records for approved users, maintain data integrity, and prevent malicious intruders. To track traffic on both sides, an intrusion detection system is needed. The lack of encryption at the 6LoWPAN layer, optimum semiannual effort on fracture connections, and restricted networked system memory make LWPAN's packet fragmentation framework vulnerable.

## 6.2 Security in RPL

In low-power networks deployed over 6LoWPANs with high or inconsistent packet loss mounts, IPv6 Routing Protocol for LLN (RPL) is designed for routing IPv6 traffic [102]. A "Security" field after the ICMPv6 message header is used for RPL protection. In this area, information indicates the security level and encryption algorithm used for message encryption. LDR provides data authentication support, somaticized security, replay protection, and critical management. The selective transmission, sinkhole, Sybil, hello-inundations, hyperspace, black hole, and denial of service attacks are used in RPL attacks.

## 6.3 Security in bluetooth low energy

### 6.3.1 BLE protocol

BLE is a low-performance version of wireless Bluetooth 2.4 GHz. Although classic Bluetooth BLE signal strength and radio range are smaller than specific metrics, BLE is designed to run on a copper battery (e.g. the common CR2032) for high-power applications [103]. BLE sensor devices can run for several years without needing a new battery, thanks to their low power and long battery life. The latest BLE Secure Connections model is implemented in BLE version 4.2 to improve protection. Review the main security issues of BLE: passive rescue.

### 6.3.2 Eavesdropping

Passive eavesdropping defence can be used by encryption [104]. BLE 4.2 uses Elliptic Curve Diffie-Hellman (ECDH) algorithm for data encryption. In contrast, earlier versions of the BLE (Bluetooth 4.1 or older) apps used the easily guessed partial key for the first time to crypt a connection.

## 6.4 Identity tracking

Third-party devices that are connected with addresses and provide device authentication of the devices that transmit the information and monitor the users. A regular change of private addresses to defend against this threat only the trusted parties can overcome them [105].

## 6.5 Zigbee security

Zigbee security requires the presumption of safe stocking of keys and the pre-loading of computers with symmetrical keys so that they will not be transmitted unencrypted. This unique unprotected critical transmission provides a short operating time frame, during which an assailant can sniff the key [106].

## 6.6 RFID security

The classification of radiofrequency is the way to classify the “people” uniquely by using radio waves to transmit their identity (usually a serial number). At least one RFID device is composed of a tag, an antenna, and a scanner. RFID tags are connected to read devices using the RFID reader to store identifications and data. Active, passive, or passive-aided RFID tags may be. Active RFID tags can be distributed with readings ranging up to 100 m. Battery-free devices can use passive tags, as the ID is read by the reader passively. You have a read distance of up to 25 m from close touch and use the strength of an interrogating reader for all responses [107].

## 6.7 LoRa and LoRaWAN security

The network layer authenticity NwkSkey is used from the LoRa system to the LoRa network server [108]. The AppSkey is used for the end-to-end AES-128 protection of the application layer from LoRa to the application server. An authentication process of the LoRaWAN network joining protocol is provided between the system and the LoRaWAN network [109]. LoRa devices can be linked to the grid in two ways: through over-the-air activation or customized activation. Use the mixture of NwkSKey and AppSKey Session Keys to provide LoRa devices to encrypt and sign all future messages after a node joins into the LoRaWAN network.

Since the Network Server only identifies those keys and the actual node, no other node or man can recover the plain text data during a mid-assault. You will store the same session keys on the LoRa computer and the network server. Where data is shielded in transit from LoRaWAN networks or terminals, nodes are susceptible to physical attacks, particularly in remote and unmonitored areas where devices are mounted. A computer can be befriended on the web if encrypted keys are removed. LoRa's long-term air time can be abused in attacks like targeted jamming.

## 6.8 IoT security in azure

The Azure IoT Network of the Azure IoT Suite provides a truly managed interface that enables secure two-way communication with Azure's IoT tools [110]. Azure IoT Suite Security can be divided into three main areas: supplying and authenticating devices, secure connectivity, and secure network processing and storage. The registry for identity Azure IoT Hub ensures secure storage of IoT IDs and identification keys. Azure IoT Hub or Gateways and Azure IoT Hub provide the connectivity between devices and the Azure IoT Hub through an Azure IoT Hub authenticated by the X framework.

## 6.9 IoT security in AWS

An AWS IoT message broker or Thing Stones Service is required for each connected computer [111]. AWS has recently released a professionally controlled IoT protection program, AWS IoT App Defender. 45 AWS IoT Device Defender reviews and defines the security policy of customer devices against a collection of established best IoT security practices. AWS IoT System Defender security warnings are created when security policy audits fail, or enforcement violations are found in the AWS IoT Console, Security warnings, Amazon CloudWatch and Amazon SNS. Besides, AWS IoT App Defender provides customers with tools to help them analyze and resolve security issues, including contextual details.

## 6.10 Use IoT security analytics

Analytics is one method by which we can identify the loophole in IoT devices by applying security analytics [112]. Analytics helps to find loopholes in the application or IoT devices. It can collect data from multiple sources that can provide IoT security. The malicious and normality in the behavior of IoT devices can also be reduced if we do security analytics monitoring

on IoT devices from the IoT gateway alone. It will help security experts to recognize this abnormality in the data that harms IoT devices.

### 6.11 Use public key infrastructure

The most trustable method and many companies are used public key infrastructure. This process creates, manages, and distributes digital data in IoT devices. PKI ensures data protection from both ends, the user and the sender, because the data is encrypted and decrypted at the user's end [113]. The secret keys are used to transfer or communicate to prevent the changing of data and cyber-attacks.

### 6.12 Ensure communication protection

The communication level is the main bridge between the IoT devices, and the cloud provides strong communication to ensure security safety and prevent cyber-attacks and other issues. First of all key step of communication is encryption. The information must be encrypted, and then the protocols that are used for communication are secure and powerful. Mostly AES 256, HTTP, HTTPS, AES 128, and many other protocols are used to protect the communication level between the IoT devices and the cloud [19, 114].

### 6.13 Secure the network

The IoT devices are direct to the system, which is connected to the network, so there must be protection for this system which is connected to the IoT devices [115]. So there must be endpoint security for this system and features like anti-malware, antivirus, intrusion prevention, and firewalls, which protect the network and prevent them from cyber-attacks.

### 6.14 Ensure device authentication

There also another method by which we can strengthen our security is by using the authentication method for IoT devices. The authentication method is to reduce unauthorized access to someone's data. In this regard, the attacker needs some information to access someone's device and get the information you verify, so this is a better option than a user authentication method for our IoT devices [116]. There are many authentication methods, which are the following:

- Two way authentication
- Digital certificates
- Biometric

The described solutions are not more for those attacks because we don't know our exact enemy, so we should be aware and always have proper security in IoT devices and on servers connected to the internet.

## 7 Open research issues

The IoT technology is in the development phase and needs to mature more, so less user knowledge, poor maintenance, and updates and development standards are problems for security [117]. IoT devices have weak security, or user unaware of security measures that a hacker will easily control by using malware for ransom [118]. The control of IoT devices harms wearable devices, smart homes, and health-related applications. If the ransom is not paid to the hacker, then IoT-based vehicles will not start, or the locked homes will not open, so still, research is required in this area to make more secure IoT devices from this type of attack.

Software update is another major issue of IoT security [119]. To compete in the market, organizations launched the product quickly and took a long time to release an update of that software, which will also open doors for hackers to attack IoT devices to gain access. Sometimes the user of an IoT device is updated software from the cloud, and the link will break during the update so that it will unencrypt, and the hacker can gain access from unencrypted to control devices [120]. Future research requires a blocked port and access immediately if the cloud link is broken, and the organization is also required to release software updates as per due time to make IoT devices secure.

Lack of knowledge of clients is also a problem for IoT security because this is a new technology. Hence, future research also provides precautions, tutorials, and guidelines for users to secure their IoT devices [121]. Connecting plug-and-play devices to the IoT system also makes it insecure. However, these lessons learned for personal computer and credit card users still need to be aware of IoT [65]. The research required in the field of IoT, such as early prediction of attacks of hackers in IoT systems and detection of threats, the security of cloud in IoT, cloud to IoT or server to client security models, the secure and standard architecture of IoT systems, IoT system design and implementation with consideration of security and privacy issues and IoT device security with data privacy techniques. IoT security is still complex; organizations and users seek proper solutions [122].

## 8 Conclusion

The main worry when using IoT devices is security rather than any problems with the devices themselves. However, the primary factor bringing attention to the problem of security lapses—the reason we encounter attacks on a daily basis—is the data on the internet. IoT gadgets, on the other hand, will be the most important technological innovation in 2020 and beyond since they make things easier by using the internet and efficiently completing household tasks. In this work, we review and classify security vulnerabilities based on their type and frequency of occurrence, such as malicious attacks, malicious insiders, etc. We also go over the available solutions and how they help secure IoT devices. Additionally, we offer open research topics for future advancement in order to help organizations and researchers address security-related problems.

**Author contributions** A.A.L, A. A. K, Y. S wrote the main manuscript, S.K and A. K. K draw figures and tables and H.L supervised the work.

**Funding** Shenyang Normal University.

**Data availability** No datasets were generated or analysed during the current study.

## Declarations

**Competing interests** The authors declare no competing interests.

**Open Access** This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

## References

- Yin S, Li H, Laghari AA, Gadekallu TR, Sampedro GA, Almadhor A. An anomaly detection model based on deep auto-encoder and capsule graph convolution via sparrow search algorithm in 6G Internet-of-everything. *IEEE Internet Things J.* 2024. <https://doi.org/10.1109/JIOT.2024.3353337>.
- Fatima Z, Rehman AU, Hussain R, Karim S, Shakir M, Soomro KA, Laghari AA. Mobile crowdsensing with energy efficiency to control road congestion in internet cloud of vehicles: a review. *Multimed Tools Appl.* 2023;83:1–26.
- Sony M. Industry 4.0 and lean management: a proposed integration model and research propositions. *Prod Manuf Res.* 2018;6(1):416–32.
- Yahya N. Agricultural 4.0: its implementation toward future sustainability. In: Green Urea. Singapore: Springer; 2018. p. 125–45.
- Jeong YN, Son SR, Jeong EH, Lee BK. An integrated self-diagnosis system for an autonomous vehicle based on an IoT gateway and deep learning. *Appl Sci.* 2018;8(7):1164.
- Gao J, Li P, Laghari AA, Srivastava G, Gadekallu TR, Abbas S, Zhang J. Incomplete multiview clustering via semidiscrete optimal transport for multimedia data mining in IoT. *ACM Trans Multimed Comput Commun Appl.* 2023;20:1–20.
- Jardine E. Mind the denominator: towards a more effective measurement system for cybersecurity. *J Cyber Policy.* 2018;3(1):116–39.

8. Khan AA, Laghari AA, Elmennai H, Shaikh AA, Bourouis S, Hadjouni M, Alroobaee R. GAN-IoTVS: a novel Internet of Multimedia Things-enabled Video Streaming Compression Model Using GAN and Fuzzy Logic. *IEEE Sensors Journal*. 2023.
9. Khan AA, Laghari AA, Baqasah AM, Alroobaee R, Almadhor A, Sampedro GA, Kryvinska N. Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing.
10. Khan AA, Chen YL, Hajjej F, Shaikh AA, Yang J, Ku CS, Por LY. Digital forensics for the socio-cyber world (DF-SCW): a novel framework for deepfake multimedia investigation on social media platforms. *Egypt Inf J*. 2024;27:100502.
11. Samie F, Bauer L, Henkel J. IoT technologies for embedded computing: a survey. In *2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ ISSS)*, IEEE, 2016. pp. 1–10.
12. Khan Z, Lehtomaki JJ, Iellamo SI, Vuohtoniemi R, Hossain E, Han Z. IoT connectivity in radar bands: a shared access model based on spectrum measurements. *IEEE Commun Mag*. 2017;55(2):88–96.
13. Firouzi F, Farahani B. Architecting IoT Cloud. In: Intelligent Internet of Things. Cham: Springer; 2020. p. 173–241.
14. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S. Internet of Things (IoT) Security with Blockchain Technology: a State-of-the-Art Review. *IEEE Access* (2022).
15. Khan AA, Laghari AA, Baqasah AM, Alroobaee R, Gadekallu TR, Sampedro GA, Zhu Y. ORAN-B5G: a next generation open radio access network architecture with machine learning for beyond 5G in industrial 5.0. *IEEE Transactions on Green Communications and Networking*. 2024.
16. Khan AA, Laghari AA, Alroobaee R, Baqasah AM, Alsafyani M, Bacarra R, Alsayaydeh JAJ. Secure remote sensing data with blockchain distributed ledger technology: a solution for smart cities. *IEEE Access*. 2024.
17. Ammar M, Russello G, Crispo B. Internet of Things: a survey on the security of IoT frameworks. *J Inf Secur Appl*. 2018;38:8–27.
18. Kesavan G, Sanjeevi P, Viswanathan P. A 24 hour IoT framework for monitoring and managing home automation. In *2016 international conference on inventive computation technologies (ICICT)*, IEEE, 2016. vol. 1, pp. 1–5.
19. Navani D, Jain S, Nehra MS. The Internet of Things (IoT): a study of architectural elements. In *2017 13th international conference on signal-image technology & internet-based systems (SITIS)*, IEEE, 2017. pp. 473–478.
20. Mehmood, F., Khan, A. A., Wang, H., Karim, S., Khalid, U., & Zhao, F. (2024). BLPAC-Ledger: A Lightweight Plenum Consensus Protocols for Consortium Blockchain Based on the Hyperledger Indy. *Computer Standards & Interfaces*, 103876.
21. Khan AA, Dhabi S, Yang J, Alhakami W, Bourouis S, Yee L. B-LPoT: a middleware lightweight Proof-of-Elapsed Time (PoET) for efficient distributed transaction execution and security on Blockchain using multithreading technology. *Comput Electr Eng*. 2024;118:109343.
22. Gusev M. A dew computing solution for IoT streaming devices. In *2017 40th international convention on information and communication technology, electronics and microelectronics (MIPRO)*, IEEE, 2017. pp. 387–392.
23. Santos C, Jiménez JA, Espinosa F. Effect of event-based sensing on IoT node power efficiency. Case study: air quality monitoring in smart cities. *IEEE Access*. 2019;7:132577–86.
24. Alonso RS, Sittón-Candanedo I, García Ó, Prieto J, Rodríguez-González S. An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario. *Ad Hoc Netw*. 2020;98:102047.
25. Placidi P, Gasperini L, Grassi A, Cecconi M, Scorzoni A. Characterization of low-cost capacitive soil moisture sensors for IoT networks. *Sensors*. 2020;20(12):3585.
26. Padwal SC, Kumar M, Balaramudu P, Jha CK. Analysis of environment changes using WSN for IOT applications. In *2017 2nd international conference for convergence in technology (I2CT)*, IEEE, 2017. pp. 27–32.
27. Ronen E, Shamir A. Extended functionality attacks on IoT devices: the case of smart lights. In *2016 IEEE European symposium on security and privacy (EuroS&P)*, IEEE, 2016. pp. 3–12.
28. Siddula SS, Babu P, Jain PC. Water level monitoring and management of dams using IoT. In *2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, IEEE, 2018. pp. 1–5.
29. Laghari AA, Li H, Karim S, Hyder W, Shoulin Y, Khan AA, Laghari RA. Internet of multimedia things (IoMT): A review. *The Review of Socionetwork Strategies* 2024; 1–29.
30. Kazi R, and Tiwari G. IoT based Interactive industrial home wireless system, energy management system and embedded data acquisition system to display on web page using GPRS, SMS & E-mail alert. In *2015 International Conference on Energy Systems and Applications*, IEEE, 2015. pp. 290–295.
31. Patil A, Deokar SA, Banderkar A. GRID TIE solar power plant data acquisition System using Internet of Things. In *2018 International conference on information, communication, engineering and technology (ICICET)*, IEEE, 2018. pp. 1–4
32. Sun J. Design and Development of the fire sensor system of fitness club based on the Internet of Things. In *The international conference on cyber security intelligence and analytics*, Springer, Cham, 2020. pp. 617–624.
33. Marah BD, Jing Z, Ma T, Alsabri R, Anaadumba R, Al-Dhelaan A, Al-Dhelaan M. Smartphone architecture for edge-centric iot analytics. *Sensors*. 2020;20(3):892.
34. HaddadPajouh H, Khayami R, Dehghantanha A, Choo KKR, Parizi RM. AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things. *Neural Comput Appl*. 2020;32:1–15.
35. Mrozek D, Koczur A, Malysiak-Mrozek B. Fall detection in older adults with mobile IoT devices and machine learning in the cloud and on the edge. *Inf Sci*. 2020;537:132–47.
36. Rahmani AM, Babaei Z, Souri A. Event-driven IoT architecture for data analysis of reliable healthcare application using complex event processing. *Clust Comput*. 2020;24:1–14.
37. Sharma PK, Chen MY, Park JH. A software defined fog node based distributed blockchain cloud architecture for IoT. *ieee Access*. 2017;6:115–24.
38. Tyagi S, Agarwal A, Maheshwari P. A conceptual framework for IoT-based healthcare system using cloud computing. In *2016 6th international conference-cloud system and big data engineering (Confluence)*, IEEE, 2016. pp. 503–507.
39. Vermesan O, Friess P. *Internet of things: converging technologies for smart environments and integrated ecosystems*. River publishers, 2013.
40. Liu L, Shi Q, Lee C. A novel hybridized blue energy harvester aiming at all-weather IoT applications. *Nano Energy*. 2020;76:105052.
41. Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y. A survey of IoT applications in blockchain systems: architecture, consensus, and traffic modeling. *ACM Comput Surv (CSUR)*. 2020;53(1):1–32.

42. Qiu C, Fan W, Lee C, Yuce MR. Self-powered control interface based on Gray code with hybrid triboelectric and photovoltaics energy harvesting for IoT smart home and access control applications. *Nano Energy*. 2020;70:104456.
43. Pathan MA, Deval N. IOT based smart office using wireless sensor Area Network."
44. Sami N, Mufti T, Sohail SS, Siddiqui J, Kumar D. Future Internet of Things (IOT) from cloud perspective: aspects, applications and challenges. In: *Internet of Things (IOT)*. Cham: Springer; 2020. p. 515–32.
45. Kumar H, Singh MK, Gupta MP, Madaan J. Moving towards smart cities: solutions that lead to the smart city transformation framework. *Technol Forecast Soc Change*. 2020;153:119281.
46. Mishra, Ravi, Anjali Pandey, and Jhalak Savariya. Application of Internet of Things: Last meter smart grid and smart energy efficient system. In *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*, IEEE, 2020. pp. 32–37.
47. Zheng W, Sun K, Zhang X, Zhang Q, Israr A, Yang Q. Cellular communication for ubiquitous Internet of Things in smart grids: present and outlook. In *2020 Chinese Control And Decision Conference (CCDC)*, IEEE, 2020. pp. 5592–5596.
48. Humaira F, Islam MS, Luva SA, Rahman MB. A secure framework for IoT smart home by resolving session hijacking. *Glob J Comput Sci Technol*. 2020;20:9–20.
49. Kansal P, Sharma D, Kumar M. Introduction to fog data analytics for IoT applications. In: *Fog data analytics for IoT applications*. Singapore: Springer; 2020. p. 19–38.
50. Kerber W. Data sharing in IoT ecosystems and competition law: the example of connected cars. *J Compet Law Econ*. 2019;15(4):381–426.
51. Dev R. Connected cars & IoT—emerging trends and predictions. *Auto Tech Rev*. 2016;5(2):12–3.
52. Suryawanshi K, Pandharkar M. The application scenario and dependence with IoT. In: *Internet of Things in smart technologies for sustainable urban development*. Cham: Springer; 2020. p. 91–105.
53. Shahzad A, Zhang K, Gherbi A. Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain. *Sensors*. 2020;20(13):3760.
54. Yang H, Alphones A, Zhong W-D, Chen C, Xie X. Learning-based energy-efficient resource management by heterogeneous RF/VLC for ultra-reliable low-latency industrial IoT networks. *IEEE Trans Industr Inf*. 2019;16(8):5565–76.
55. Turck M. Growing pains: the 2018 internet of things landscape. *Mattturck Com* 2018.
56. Somesh S, Senthilnathan N, Sabarinath M, Santhosh Kumar A, Rishikeshan R, Bala V. Real time implementation of home appliance control using ALEXA. In *IOP Conference Series: Materials Science and Engineering*. IOP Publishing, 2020. vol. 937, no. 1, p. 012008
57. Srivastava S, Babu MR. Generic architecture for ubiquitous IoT applications. In *Emerging research in data engineering systems and computer communications*, Springer, Singapore, 2020. pp. 131–143.
58. Jain A, Lalwani S, Jain S, Karandikar V. IoT-based smart doorbell using Raspberry Pi. In *International conference on advanced computing networking and informatics*, Springer, Singapore, 2019. pp. 175–181.
59. Thakur P, Shetty A, Pokharkar O, Shinde S. IoT Based portable smart lock. In *Proceedings 2019: conference on technologies for future cities (CTFC)*. 2019.
60. Zahid IM, Hasib MHH, Rahaman I, Islam MZ, Rashid MM. Smart vehicle protocol monitoring system by the internet of things platform. In *2019 4th international conference on electrical information and communication technology (EICT)*, IEEE, 2019. pp. 1–4.
61. Becirovic S, S Mrdovic. Manual IoT forensics of a samsung gear S3 frontier smartwatch. In *2019 international conference on software, telecommunications and computer networks (SoftCOM)*, IEEE, 2019. pp. 1–5.
62. Takiddeen N, Zualkernan I. Smartwatches as iot edge devices: a framework and survey. In *2019 fourth international conference on fog and mobile edge computing (FMEC)*, IEEE, 2019. pp. 216–222.
63. Kim JE, Bessho M, Ken S. Towards a Smartwatch application to assist students with disabilities in an IoT-enabled campus. In *2019 IEEE 1st global conference on life sciences and technologies (LifeTech)*, IEEE, 2019. pp. 243–246.
64. Martins SS, Wernick C. Regional differences in residential demand for very high bandwidth broadband internet in 2025. *Telecommun Policy*. 2021;45(1):102043.
65. Abdalrahman GA, Varol H. Defending Against Cyber-Attacks on the Internet of Things. In *2019 7th international symposium on digital forensics and security (ISDFS)*, IEEE, 2019. pp. 1–6.
66. Hodo E, Bellekens X, Hamilton A, Dubouilh PL, lorkyase E, Tachtatzis C, Atkinson R. Threat analysis of IoT networks using artificial neural network intrusion detection system. In *2016 International symposium on networks, computers and communications (ISNCC)*, IEEE, 2016. pp. 1–6.
67. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. *IEEE Access*. 2019;7:82721–43.
68. Ferrando R, Stacey P. Classification of device behaviour in internet of things infrastructures: towards distinguishing the abnormal from security threats. In *Proceedings of the 1st international conference on internet of things and machine learning*, 2017. pp. 1–7.
69. Kiel D, Arnold C, Voigt K-I. The influence of the Industrial Internet of Things on business models of established manufacturing companies—A business level perspective. *Technovation*. 2017;68:4–19.
70. Wang T, Zhang G, Anfeng Liu Md, Bhuiyan ZA, Jin Q. A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing. *IEEE Internet Things J*. 2018;6(3):4831–43.
71. da Costa KAP, Papa JP, Lisboa CO, Munoz R, de Albuquerque VHC. Internet of Things: a survey on machine learning-based intrusion detection approaches. *Comput Netw*. 2019;151:147–57.
72. Elrawy MF, Awad AI, Hamed HFA. Intrusion detection systems for IoT-based smart environments: a survey. *J Cloud Comput*. 2018;7(1):21.
73. Chifor BC, Bica I, Patriciu VV. Mitigating DoS attacks in publish-subscribe IoT networks. In *2017 9th international conference on electronics, computers and artificial intelligence (ECAI)*, IEEE, 2017. pp. 1–6.
74. Khattak HA, Shah MA, Khan S, Ali I, Imran M. Perception layer security in Internet of Things. *Future Gener Comput Syst*. 2019;100:144–64.
75. Mirzamohammadi S, Chen JA, Sani AA, Mehrotra S, Tsudik G. Ditio: trustworthy auditing of sensor activities in mobile & IoT devices. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, pp. 1–14. 2017.
76. Morgner P, Pfennig S, Salzner D, Benenson Z. Malicious IoT implants: tampering with serial communication over the Internet. In *International Symposium on Research in Attacks, Intrusions, and Defenses*, Springer, Cham, 2018. pp. 535–555.

77. Maleh Y, Ezzati A, Belaissaoui M. An enhanced DTLS protocol for Internet of Things applications. In *2016 International conference on wireless networks and mobile communications (WINCOM)*, IEEE, 2016. pp. 168–173.
78. Jaafar GA, Abdullah SM, Ismail S. Review of recent detection methods for HTTP DDoS attack. *J Comput Netw Commun*. 2019;2019:1283472.
79. Belghazi Z, Benamar N, Addaim A, Kerrache CA. Secure Wifi-Direct using key exchange for IoT device-to-device communications in a smart environment. *Future Internet*. 2019;11(12):251.
80. Balaji S, Nathani K, Santhakumar R. IoT technology, applications and challenges: a contemporary survey. *Wirel Pers Commun*. 2019;108(1):363–88.
81. Majumdar P, Singh A, Pandey A, Chaudhary P. A deep learning approach against botnet attacks to reduce the interference problem of IoT. In: Intelligent computing and applications. Singapore: Springer; 2021. p. 645–55.
82. Yin M, Chen X, Wang Q, Wang W, Wang Y. Dynamics on hybrid complex network: botnet modeling and analysis of medical IoT. *Secur Commun Netw*. 2019;2019:6803801.
83. Ali O, Ishak MK, Wuttisittikuljij L, Maung TZB. IoT Devices and Edge gateway provisioning, realtime analytics for simulated and virtually emulated devices. In *2020 international conference on electronics, information, and communication (ICEIC)*, IEEE, 2020. pp. 1–5.
84. Kumar A, Lim TJ. Early detection of Mirai-like IoT bots in large-scale networks through sub-sampled packet traffic analysis. In *Future of Information and Communication Conference*, Springer, Cham, 2019. pp. 847–867.
85. Zahra SR, Chishti MA. Ransomware and Internet of Things: a new security Nightmare. In *2019 9th international conference on cloud computing, data science & engineering (Confluence)*, IEEE, 2019. pp. 551–555.
86. Lu Y. Security and privacy of internet of things: a review of challenges and solutions. *J Cyber Secur Mobil*. 2023;12(06):813–44.
87. Hameed A, Alomary A. Security issues in IoT: a survey. In *2019 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, IEEE, 2019. pp. 1–5.
88. Al-Turjman F, Lemayian JP. Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: an overview. *Comput Electr Eng*. 2020;87:106776.
89. King J, Awad AI. A distributed security mechanism for resource-constrained IoT devices. *Informatica*. 2016;40(1):133–43.
90. Tedeschi S, Emmanouilidis C, Farnsworth M, Mehnen J, Roy R. New threats for old manufacturing problems: Secure IoT-Enabled monitoring of legacy production machinery. In *IFIP International Conference on Advances in Production Management Systems*, Springer, Cham; 2017 pp. 391–398.
91. Yen IL, Bastani F, Solanki N, Huang Y, Hwang SY. Trustworthy computing in the dynamic iot cloud. In *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, IEEE, 2018. pp. 411–418.
92. Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 2015. pp. 336–341.
93. Naqvi B, Perova K, Farooq A, Makhdoom I, Oyedeleji S, Porras J. Mitigation strategies against the phishing attacks: a systematic literature review. *Comput Secur*. 2023;132:103387.
94. Ashraf QM, Habaebi MH. Autonomic schemes for threat mitigation in Internet of Things. *J Netw Comput Appl*. 2015;49:112–27.
95. Markowsky L, Markowsky G. Scanning for vulnerable devices in the Internet of Things. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, IEEE, 2015. vol. 1, pp. 463–467.
96. Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and security: challenges and solutions. *Appl Sci*. 2020;10(12):4102.
97. Yu D, Zhang L, Chen Y, Ma Y, Chen J. Large-scale IoT devices firmware identification based on weak password. *IEEE Access*. 2020;8:7981–92.
98. Kraijak S, and P Tuwanut. A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends. 2015; 6–6.
99. Zhao S, Li S, Qi L, Da Li X. Computational intelligence enabled cybersecurity for the internet of things. *IEEE Trans Emerg Top Comput Intell*. 2020;4(5):666–74.
100. Turk Y. A Self-Organizing management architecture for low powered wireless personal area networks. In *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, IEEE, 2020. pp. 1–6.
101. Gajewski M, Batalla JM, Mastorakis G, Mavromoustakis CX. Anomaly traffic detection and correlation in Smart Home automation IoT systems. *Trans Emerg Telecommun Technol*. 2020;33: e4053.
102. Almusaylim ZA, Alhumam A, Jhanjhi NZ. Proposing a secure RPL based Internet of Things routing protocol: a review. *Ad Hoc Netw*. 2020;101:102096.
103. Basu SS, Haxhibeqiri J, Baert M, Moons B, Karaagac A, Crombez P, Camerlynck P, Hoobeke J. An End-To-End LwM2M-based communication architecture for multimodal NB-IoT/BLE devices. *Sensors*. 2020;20(8):2239.
104. Yu S, Zhang X, Huang P, Guo L, Cheng L, Wang K. AuthCTC: defending against waveform emulation attack in heterogeneous IoT environments. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, 2020. pp. 20–32.
105. Gu K, Zhang WB, Lim SJ, Sharma PK, Al-Makhadmeh Z, Tolba A. Reusable mesh signature scheme for protecting identity privacy of IoT devices. *Sensors*. 2020;20(3):758.
106. Sadikin F, van Deursen T, Kumar S. A hybrid Zigbee IoT Intrusion detection system using secure and efficient data collection. *Internet Things*. 2020;12:100306.
107. Safkhani M, Rostampour S, Bendavid Y, Bagheri N. IoT in medical & pharmaceutical: designing lightweight RFID security protocols for ensuring supply chain integrity. *Comput Netw*. 2020;181:107558.
108. Sanchez-Iborra R, Sánchez-Gómez J, Pérez S, Fernández PJ, Santa J, Hernández-Ramos JL, Skarmeta AF. Enhancing lorawan security through a lightweight and authenticated key management approach. *Sensors*. 2018;18(6):1833.
109. You I, Kwon S, Choudhary G, Sharma V, Seo JT. An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system. *Sensors*. 2018;18(6):1888.
110. Al-Qaseemi SA, Almulhim HA, Almulhim MF, Chaudhry SR. IoT architecture challenges and issues: lack of standardization. In *2016 Future Technologies Conference (FTC)*, IEEE. 2016. pp. 731–738.
111. Mrabet H, Belguith S, Alhomoud A, Jemai A. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*. 2020;20(13):3625.

112. Mohsin M, Anwar Z, Zaman F, Al-Shaer E. IoTChecker: a data-driven framework for security analytics of Internet of Things configurations. *Comput Secur.* 2017;70:199–223.
113. Marino F, Moiso C, Petracca M. PKIoT: a public key infrastructure for the Internet of Things. *Trans Emerg Telecommun Technol.* 2019;30(10): e3681.
114. Tsai K-L, Huang Y-L, Leu F-Y, You I, Huang Y-L, Tsai C-H. AES-128 based secure low power communication for LoRaWAN IoT environments. *IEEE Access.* 2018;6:45325–34.
115. Rekha S, Thirupathi L, Renikunta S, Gangula R. Study of security issues and solutions in Internet of Things (IoT). *Mater Today Proc.* 2023;80:3554–9.
116. Tewari A, Gupta BB. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *J Supercomput.* 2017;73(3):1085–102.
117. Srivastava A, Gupta S, Quamara M, Chaudhary P, Aski VJ. Future IoT-enabled threats and vulnerabilities: state of the art, challenges, and future prospects. *Int J Commun Syst.* 2020;33: e4443.
118. Waqas M, Kumar K, Laghari AA, Saeed U, Rind MM, Shaikh AA, Hussain F, Rai A, Qazi AQ. Botnet attack detection in Internet of Things devices over cloud environment via machine learning. *Concurr Comput Pract Exp.* 2022;34(4): e6662.
119. Solomon G, Zhang P, Brooks R, Liu Y. A secure and cost-efficient blockchain facilitated IoT software update framework. *IEEE Access.* 2023;11:44879–94.
120. Siwakoti YR, Bhurtel M, Rawat DB, Oest A, Johnson RC. Advances in IoT security: vulnerabilities, enabled criminal services, attacks and countermeasures. *IEEE Internet Things J.* 2023;10:11224–39.
121. Narwani K, Liaquat F, Laghari AA, Awais Khan Jumani, Junaid Jamshed, and Muhammad Ibrar. Design and Implementation of an Internet of Things-Based Real-Time Five-Layer Security Surveillance System. *International Conference on Artificial Intelligence and Communication Technology*, Singapore: Springer Nature Singapore, 2023. pp. 307–323.
122. Laghari AA, Khan AA, Alkanhel R, Elmannai H, Bourouis S. Lightweight-biov: blockchain distributed ledger technology (bdlt) for internet of vehicles (iovs). *Electronics.* 2023;12(3):677.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.