IoT Commercial and Industrial Applications and AI-Powered IoT

Khaled Ahmed Nagaty

1 Introduction

Internet of Things is a disruptive technology that is commonly available and easily accessible. It connects heterogeneous devices with each other through sending and receiving information in different formats to reach a common goal [1]. The main goal of IoT devices is to sense data and interact with the environment [2]. Companies use IoT to gather information about customers to understand customers' needs and preferences, and in the same time IoT personalizes customer's products and services and customizes them to the user's needs and preferences. Therefore, many companies and industries in various fields in our daily lives adopt IoT because it helps them automate processes, reduce labor costs, and "increase productivity, save time, optimize cost, optimize human resource, predict maintenance, and provide a lot of comfort to human life." The IoT also reduces waste of resources by monitoring the utilization of these resources, hence improving the quality of products and service delivery. The IoT is composed of physical objects called things. Sensors, software, and communication technologies connect devices and exchange information over the Internet. The devices of IoT systems may range from ordinary devices such as home appliances to complex sensor networks in various industries such as weather forecast, or military. The sensors and devices in IoT systems collect data from the environment and send the data to the cloud through the Internet. When the data gets to the cloud, data processing could be done and finally the information is sent to the end user, which could be another IoT device. IoT systems are characterized by heterogeneity, dynamism, autonomy, extensiveness, privacy, and security [2]. For heterogeneity, an IoT system may be composed of different

K. A. Nagaty (✉)
The British University in Egypt, El-Sherouk City, Cairo, Egypt
e-mail: khaled.nagaty@bue.edu.eg

A. Iranmanesh (ed.), *Frontiers of Quality Electronic Design (QED)*,
https://doi.org/10.1007/978-3-031-16344-9_12

hardware devices, network infrastructure, and processing applications, and they need to connect and exchange information. For dynamism, IoT systems need to keep their correct behavior independent of changes occurring in the environment. For autonomy, IoT devices must be capable of making decisions without human intervention. For extensiveness, as the number of devices estimated to connect to the Internet in 2021 is 35 billion devices, an infrastructure and platform are required to manage such large number of connections. As IoT systems are connecting to the Internet to exchange information, this may let them vulnerable to cyberattacks especially if these systems are collecting sensitive data such as military sensor networks or healthcare systems. Therefore, IoT systems must guarantee privacy and security to protect their collected data. The global market for IoT can be segmented based on technologies, components, applications, end users, and geography. In this chapter, we will consider the IoT market segment based on applications. There are many applications of IoT technologies in our real lives; this is because IoT can be customized to almost any field of applications that can produce data about monitoring the environment, its operations, and activities. IoT applications can be commercial or industrial. The most important commercial applications of IoT are wearables, healthcare, traffic monitoring, hospitality, retail, maintenance management, and digital marketing. The most important industrial applications are manufacturing, agriculture, water supply, smart cities, financial services, energy, supply chain, transportation, telematics, and building automation. Figure 1 shows the IoT global market from 2018 to 2023. According to global data, IoT technology global market reached 130 billion dollars in 2018. It is estimated to reach 318 billion dollars in 2023, at a 20% compound annual growth rate [3].

This chapter is organized as follows: Sect. 2 is dedicated for IoT commercial applications, Sect. 3 is dedicated for industrial IoT applications, Sect. 4 is dedicated for IoT data analytics, Sect. 5 is dedicated for IoT security risks and threats, Sect. 6 is dedicated AI-powered IoT, and finally Sect. 7 is dedicated for conclusion.

2 IoT Commercial Applications

Commercial IoT applications improve experiences of customers, patients, and guests in different places such as hospitals, markets, hotels, and restaurants through more efficient monitoring of operations in smart buildings and smart offices. It improves company's insight into retail business and allow them to make real-time decisions to target potential customers with appropriate messages. The most common commercial IoT applications are the following.

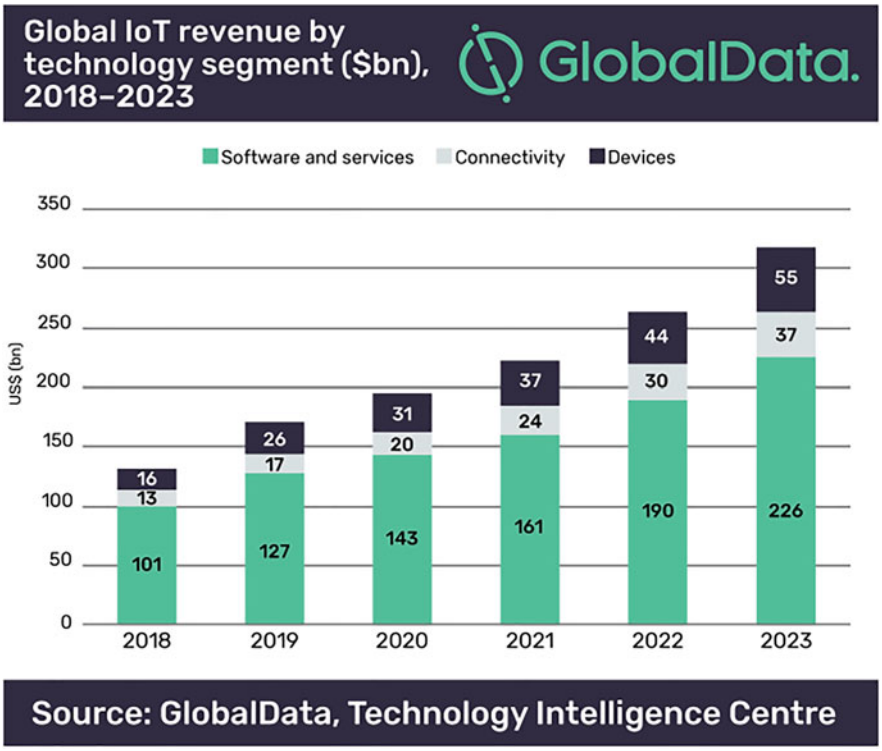

Fig. 1 Forecast End-user Spending on IoT Solutions Worldwide from 2017 to 2025 (in billions of dollars)

2.1 Healthcare

IoT healthcare systems provide flexibility and save much time than traditional healthcare systems [4]. Families, patients, hospitals, physicians, and insurance companies can benefit from the applications of IoT in healthcare. Lives of healthcare providers become safer and easier, costs are reduced, and healthcare services for patients are ultimately improved. IoT enables medical providers to detect patients' commitment to medical plans and provide them immediate help in case of emergency. For instance, monitoring noncritical patients, providing assisted ambient living (AAL) for elderly persons, and rehabilitation after physical injury save hospital resources for patients that are more critical. Patients who live far away from hospitals could not reach the hospital on time, so providing them medical advice using the IoT healthcare system could be a lifesaver. However, Internet disconnection is one of the major risks of IoT healthcare systems [5]. On the other side, patients can learn about their health records and can communicate with their medical providers. This section discusses the major components of IoT

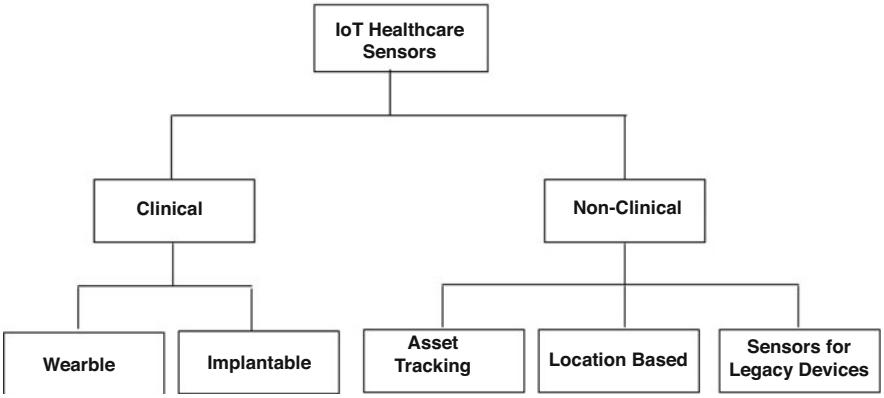

Fig. 2 Classification of IoT healthcare sensors. (As adapted from [6])

healthcare systems, services and applications, challenges, and opportunities. IoT healthcare systems are composed of many components that communicate with each other to collect and analyze data to help patients and healthcare providers. Sensors are an important component of IoT healthcare systems. Sensors must be recalibrated regularly to ensure their measurement efficiency. They are divided into two categories: clinical and nonclinical sensors. The clinical sensors are divided into wearable sensors and implantable sensors. Nonclinical sensors are divided into asset/equipment tracking sensors, location asset sensors, and legacy device sensors. Figure 2 shows the classification of healthcare sensors.

2.1.1 Clinical Sensors

2.1.1.1 Wearable Sensors

They are useful within healthcare for monitoring the bodies of patients and collecting physiological and movement data. Wearable sensors are deployed on parts of medical interest on the patient's body.

Pulse Sensors

It reads heart pulse of a patient. The pulse sensor can be placed on the patient's wrist, chest, earlobe, or fingertips. Figure 3 shows a pulse sensor.

Respiratory Rate Sensors

Respiratory sensors measure respiratory rate by detecting variations in chest movement per minute. The sensing system can be placed around the chest with a

Fig. 3 Pulse sensor

Fig. 4 Respiratory rate sensor [7]

strap. Figure 4 shows a respiratory rate sensor composed of an oxygen mask and a respiratory rate device.

Body Temperature Sensors

An accurate body temperature depends on how far the sensor position from the human body. Infrared (IR) body temperature sensors are noncontact sensors and can be placed close to the patient's forehead, earlobe, or skin. Figure 5 shows a body temperature sensor.

Blood Pressure Sensors

IoT blood pressure monitoring system (IBPMS), for example, Raspberry Pi, can remotely monitor patient's blood pressure [8]. The IBPMS reads the data and sends it to both Telegram and Gmail applications [8]. Figure 6 shows blood pressure sensor.

Fig. 5 Body temperature sensor

Fig. 6 Blood pressure sensor

Fig. 7 Pulse oximetry sensor

Pulse Oximetry Sensors

Oxygen saturation in the patient's blood can be measured using pulse oximeter sensors. This noninvasive device is composed of a red light source, infrared source, photo detectors, and a probe to transmit light through a translucent, pulsating arterial bed, typically an earlobe or fingertip. Figure 7 shows a pulse oximetry sensor.

2.1.1.2 Implantable Sensors

These sensors are inserted into the patient's body for diagnosis, treatment, and long-term monitoring. Such implantable sensors allow health monitoring systems to detect changes in the health conditions of the patients whether they are conscious or not to provide them with immediate treatment. For example, to design better prosthetics, implantable strain sensors can be incorporated into orthopedic prosthetics to specify the forces acting on those joints. Patients with high risk of excessive clotting or impeded blood flow implantable cardiovascular flow and pressure sensors can provide early warning of excessive clotting or impeded flow, and implantable neurostimulators can treat muscular and neurological damage [9].

2.1.2 Nonclinical Sensors

IoT devices can help track physician's location and people inside hospitals, find the nearest ambulance in case of emergency, track assets to achieve operational efficiency and compliance with hygiene standards, and provide real-time information for logistics [6].

2.2 Tourism and Hospitality

The tourism industry is highly affected by digital transformation and diffusion of disruptive technologies such as IoT. IoT technologies help increase customers' satisfaction in tourism and hospitality while reducing operational costs at the same time. IoT devices provide guests with automated guest check-in, smart hotel rooms with IoT-enabled door locks, motorized curtains, smart TVs which have positive impact on customers' satisfaction. IoT security and safety enable safer hotel stays and increased peace of mind for guests. Housekeeping staff can gain from IoT hotel systems to know when a guest room is occupied and when it is ready to be cleaned. Maintenance department can receive quick reports on malfunctioning gadgets such as burned-out lightbulbs or plumbing leaks to fix them as quickly as possible to minimize costs to fix problems and increase guests' satisfaction. The staff can detect vacant rooms and minimize electricity by dimming lights, turning off lights and A/C units, and tracking equipment with asset tracking systems.

2.3 Retail Industry

IoT technologies can play a fundamental role in retail industry. RFID is one of the most common forms of IoT used in retailing [12]. Data obtained from reading the tags attached to items and products by radio-frequency identification (RFID) is

analyzed via IoT data analytics tools which allow retailers to obtain more valuable information on sales update and customers' purchasing patterns. Retailers can enhance customer experience by creating ideal shopping atmosphere using smart self-checkout cart where customers pick an item off a shelve, scan barcode of the item, drop it in the cart, and, when shopping is finished, pay directly on the cart. IoT reduce costs by tracking lost carts and baskets, tracking shipments in real time to prevent spoilage, keep products protected in transit, prevent theft or loss, adjust the air conditioning based on how many people are coming and going, and dim light switches when a store is less occupied. IoT retail uses sensors to monitor customer satisfaction, food safety, and sales opportunities in real time. IoT technologies allow retailers to have deep insight in the supply chain and track assets. Based on customers' behavior and demographics collected by IoT systems, customized products can be delivered to customers and placed in the right places. IoT inventory systems eliminate downtime at warehouse and uphold timely deliveries, and using smart shelves, retailers can monitor stock levels and guarantee products' availability on shelves.

2.4 Digital Marketing

IoT technology provides marketers with more insights on customer's usage of products. IoT technology finds patterns in product usage which allow digital marketers to predict exact demand and understand the daily lifestyle of customers and may read the customer's mind set. This makes 100% of advertisements are aligned with the customers' needs, interests, behaviors, buying patterns, individual preferences, and past purchases. Digital marketers can better understand their audience, determine the elements affect purchasing patterns, analyze customers' behavior in real time, determine markets where a particular product will sell best, and target potential customers with promotion messages and personalized advertisements. For example, if the milk in a customer's smart fridge in his/her smart home is about to end, then the connected smart fridge will record for buying a new bottle of milk and sends a purchasing order to the store. As IoT technology becomes more advanced, it learns the customer's behavior in consuming milk and calculate the number of days the bottle of milk will be consumed. Such smart fridge can warn the customer when the milk is approaching to an end through a text message to the customer's smartphone before sending a purchasing order to the store. As a result, advertisers can predict when customers will replace products, which type of products they want to accurately target potential customers, determine the type of marketing campaign, determine potential messages that will actively engage customers, and improve the marketing campaign. IoT in social media allows digital marketers to automate market data gathering, creating posts with contents they are sure that the audience will want to see and sharing them with potential customers.

3 IoT Commercial Applications

3.1 Agriculture

IoT in agriculture uses remote sensors embedded into plants and fields to collect data about the physical properties of soil and environment to help make decisions for increasing crop production which is essential for sustainable food security. Data analysis helps farmers monitor their crops, organize the irrigation process, promptly diagnose plant diseases to minimize the use of pesticides, help decision-makers to have better insights, and develop management plans to save time and money. Using IoT in agriculture is one step closer to smart agriculture where farms will be self-dependent, thus making the right decisions to increase productivity [10]. IoT sensors used in smart agriculture are classified into two categories: field and climate sensors. The IoT agriculture system is composed of three layers: the first layer is data collection layer that collects field data and climate data and send over the Internet to the data analysis layer. The data analysis layer contains tools to analyze the collected data and historic stored data to predict the parameters required for making decisions in the upcoming days. For example, in rescheduling field irrigation, data about soil moisture is collected from sensors inserted into the soil closer to the root zone of the plants. Climatic data such as temperature and wind speed collected from wind speed sensors, sunshine data, and field data is sent to a dedicated server in the cloud to be analyzed and decision is made based on a threshold value [11]. The decision on whether to start or stop the water pump or increase or reduce the amount of water served to the field is sent to the water pump regulator. The framer or human expert can override the decisions of the IoT agriculture system. Figure 8 shows IoT agriculture sensors which can be categorized into field sensors and climate sensors.

3.1.1 Field Sensors

3.1.1.1 Soil Temperature

It is the measure of warmth in the soil, i.e., how hot or cold the soil is, the air may be warm, but the soil may be cool. So, soil temperature is necessary because it is a very important physical property that affects the germination of seeds and plant growth. It controls the speed of chemical reactions and biological activities in the soil; most soil organisms work better at warm soil temperature. Factors that influence soil temperature are climate, season, water levels, soil color, plant cover, compost and manure, and soil moisture. An instant-read thermometer used for cooking is used to measure soil temperature by putting the thermometer's probe as deep as possible into the soil to get a precise reading of the soil temperature. Figure 9 shows a soil temperature sensor.

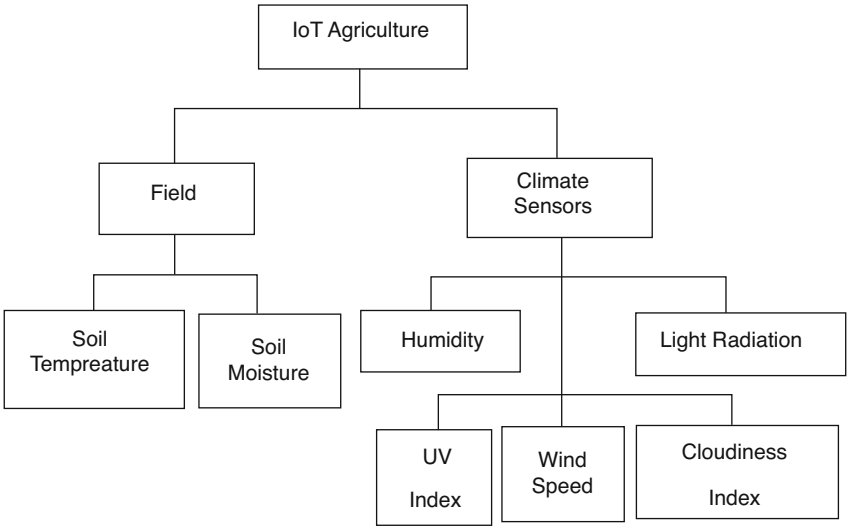

Fig. 8 Classification of IoT agriculture sensors

Fig. 9 Soil temperature sensor

3.1.1.2 Soil Moisture

Soil moisture is the water between the spaces of soil particles; it dissolves minerals and nutrients the plants need and absorb to grow. Soil moisture controls water exchange and heat energy between land surface and atmosphere through evaporation and plant transpiration. Precipitation, temperature, and soil characteristics affect soil moisture. Soil moisture sensors measure the volumetric water content at the root zone in the soil to manage the irrigation systems to use less water. Soil moisture is measured using tensiometers that measure soil moisture tension. Capacitive soil moisture sensor determines the amount moisture in the soil by measuring changes in capacitance to determine the water content of soil. Soil moisture sensors are inserted deep in the soil at the plants' root zone. Figure 10 shows a soil moisture sensor.

Fig. 10 Soil moisture sensor

Fig. 11 Humidity sensor

3.1.2 Climate Sensors

3.1.2.1 Humidity

Humidity sensors or hygrometers measure moisture in the air. They combine relative humidity (RH) measurement and air temperature (T) to provide accurate measurement of dew point and absolute humidity (AH). Relative humidity is an important factor for comfort, it measures the ratio of moisture in the air to the highest amount of moisture at a particular air temperature. Humid air is subject to less daily temperature variation than dry air because humid air takes longer to heat up and cool off. Under high humidity maximum shade temperature rarely exceeds 38 °C, while under dry condition, a maximum of 54 °C is possible. Minute changes in the atmosphere are monitored using humidity sensors to calculate humidity in the air. Humidity sensors are placed in home heating, ventilating, and air conditioning systems. In addition, they are also used in offices, cars, industrial spaces, museums, greenhouses, and meteorology stations to forecast weather. Figure 11 shows a humidity sensor.

3.1.2.2 Ultraviolet (UV) Index

UV index sensor provides an accurate measurement of the ultraviolet radiation index (UVI) from sunlight. UV radiation boosts the intensity of photosynthesis processes and facilitates the production of chlorophyll and nutrient which strengthens the

Fig. 12 Ultraviolet sensor

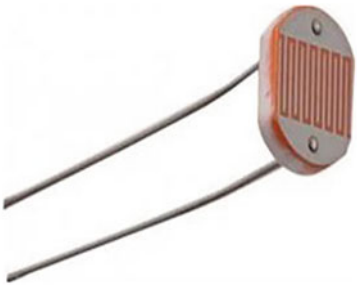

Fig. 13 Photo-resistor sensor

plants. UV affects the life cycle of plants as it can speed up the germination process for starting seeds when grown indoors. UV sensors help identify risks associated with different levels of UV exposure. UV index may be different from one place to another; it is affected by a number of factors including time of day, cloud cover, altitude, and more. Monitoring UV radiation in agricultural field allows farmers to take better precautions to improve the growth of agricultural crops and increase productivity. Figure 12 shows an ultraviolet sensor.

3.1.2.3 Light Radiation

A light sensor measures the radiant energy or illuminance that exists in a very narrow range of frequencies basically called "light." It outputs an electric signal which indicates the intensity of daylight or artificial light. Illuminance decreases as the distance from light source increases, so light sensors can be used to gauge relative distance from the source. Photo-resistors, photodiodes, and phototransistor are types of light sensors. Figure 13 shows a photo-resistor sensor.

3.1.2.4 Cloudiness Index

Cloudiness or cloud cover index refers to the part of the sky covered by clouds when observed from a specific location. Sunshine duration is inversely proportion to cloud cover, i.e., the least cloudy locales are the sunniest ones and vice versa. Variations in daily temperature are affected by cloud cover buffering which lowers

Fig. 14 Ceilometer

the daytime high but raises the nighttime low. Growth and yields are adversely affected by high daytime temperatures which cause pollen sterility and blossom drop, while hot nights can reduce crop yields. Cloudiness is estimated in terms of how many eighths of the sky are covered in cloud. This measure rates from 0 Oktas which is complete clear sky to 8 Oktas which is completely overcast. Figure 14 shows a ceilometer.

3.2 Oil and Gas Mining

Smart personal protective equipment (PPE) embeds tracking devices, sensors, and monitors in clothes worn by workers who may face specific hazards because of their working environment. PPEs provide better safety and long-term cost savings in mining fields through early prevention of health issues, hazardous situations, or the exposure to danger zones. Data collected by these sensors and monitors is analyzed to provide insights on any harms a worker may be susceptible to. PPE sensors can be infused or interwoven in the fabric so that they cannot be removed by laundering or they have built-in electronic devices. In oil and field mining, these PPEs monitor worker's temperature to ensure they are not overheating or developing hypothermia and monitor air toxicity in mine fields to provide real-time safety for the workers. Personal protective equipment includes items such as safety glasses, gloves, earplugs, shoes, muffs, respirators, hard hats or coveralls, vests, and full body suits.

3.2.1 Smart Pipelines

Engineers and operators of oil and gas pipelines must ensure optimal performance of pipelines for continuous flow operations 24 × 7. We need to ensure cost-effective

maintenance of old pipelines network that covers thousands of kilometers across international borders to mitigate risk of flow disruption. Old pipelines operate inefficiently, are vulnerable to damages due to environmental reasons, and require more labor to inspect each kilometer of the pipeline on regular basis that make the cost to maintain high. IoT sensors, meters, and diagnostic devices such as lasers and ultrasonic and acoustic sensors can contribute to networks of smart pipelines. They collect data on pressure, flow, and compressor conditions and report movement, corrosion, leakage, or impact to the pipelines. Data collected from pipelines are analyzed using advanced analytical tools to enhance the existing engineering capabilities of the operating teams and allow them to formulate maintenance and repair options on-demand, with the help of potential risk probability and impact calculators. Accurate and timely information allows the operating teams to be more proactive and ensure better pipeline management.

3.2.2 Lone Worker Monitoring

IoT lone worker tracking system offers an easy way to monitor workers in hazardous environment to ensure safety of the workers, tracking them via GPS to show where they are and to which direction they are heading. Moreover, workers can report emergency situations and talk to emergency professionals.

3.2.3 Safety and Security

Safety is the set of protective measures that must be taken to detect risks, assess safety, and prevent accidents at the workplace. Safety IoT devices collect data that is required to assess health hazards in the work field and identify, evaluate, and prioritize risks. Safety IoT devices include systems like door locks, surveillance cameras, smart safes, access control systems, fire alarm systems, and similar devices mostly used to secure a location or prevent a hazard.

3.3 Wearables

IoT wearables, also known as "wearables," is a category of network-connected devices that can be implanted in the user's body, embedded in clothing, tattooed on the skin, or worn as accessories. Wearables are disruptive technologies that can collect data, track activities, and customize experiences to users' requirements and desires. Wearable technologies are growing fast and expect to influence our social, economic, and legal norms. Wearable devices track employees' performance and monitor their health and location inside the premises. Besides, the wearables can also report collisions and falls, thereby improving the safety of the operations. Fitness trackers and body-mounted sensors such as accelerometers, gyroscopes,

Fig. 15 Fitness tracker

Fig. 16 Smartwatch

magnetic sensors, and their combinations, smart jewelries and smartwatches, are the prevailing trends in today's wearable market.

3.3.1 Fitness Trackers

They are devices that are worn typically as wristbands to measure vital parameters such as heart beat rate and monitor the number of steps taken each day, how long you spent sleeping in each sleep stage, how much calories you have burned, and how long you spent working out. Gathered data can be sent to your smartphone to help you monitor changes over time. Some trackers have GPS to track user's locations during running, biking, or walking especially for old people who may have Alzheimer's disease. Figure 15 shows a typical fitness tracker.

.

3.3.2 Smartwatches

They are watches with computer capabilities such as calculations, translations, digital media playing, and game playing. They have mobile operating systems with apps similar to mobile apps that include digital maps, schedulers, calculators, personal organizers, Wi-Fi, and Bluetooth connectivity. Figure 16 shows a typical smart watch.

Fig. 17 Tri-axial accelerometer

3.3.3 Accelerometers

They are devices that can measure the acceleration of an object. Figure 17 shows a tri-axial accelerometer, which provides simultaneous measurements in three orthogonal axes *x*, *y*, and *z* to analyze all vibrations being experienced by a structure. Tri-axial accelerometers have three crystals that are placed so that each one reacts to vibration in a different axis. The output has three signals; each one represents the vibration for one of the three axes. In IoT, tri-axial accelerometers detect shake, orientation, tap, double tap, tilt, fall, positioning, motion, shock, or vibration.

3.4 Smart Cities

The main components of smart cities are data collection, data exchange, data storage, and data analysis [13]. A huge amount of information is collected daily through millions of connected IoT devices such as sensors and meters that collect and analyze data to better monitor and use the infrastructure and improve maintenance. IoT technology can develop efficient methods to minimize operational costs of public utilities and services, manage traffic, reduce pollution, maintain people safety and city cleanness, increase productivity, and allow quick response to people's needs [14]. Collected data is transmitted to the cloud through Wi-Fi networks, 4G or 5G technologies for storage. Data is stored in the cloud in formats that make it usable for data analysis. In the data analysis stage patterns are extracted and inferences are obtained from the stored data to guide decision-makers. Simple analysis for basic decision-making could be enough, while more detailed and deep analysis for heterogeneous data is required for more complex decisions. Smart city contains smart homes, smart schools, smart hospitals, smart power plants, smart wastewater management, smart agriculture, smart transportation, smart health, smart environment, smart governance, and more. IoT technology uses smart device and sensor networks to collect and analyze data to eliminate risks, avoid damages, and reduce costs. Traffic authorities can use this information to build safe road strategies and predict the outcomes and efficacy of specific measures and precautions that promote optimal safety. IoT technologies collect data and provide

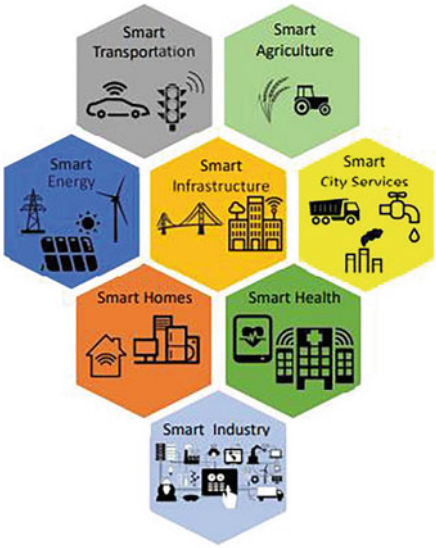

Fig. 18 Smart city components

deep insight on what drivers do to hold them accountable and encourage them to adopt safer habits to reduce road accidents and protect them from collisions and casualties that can happen. Figure 18 shows smart city components [13].

3.4.1 Environmental Monitoring

IoT sensors are deployed at many points in the cities to collect accurate data on the environment to guide us on how to interact with the environment and put plans to improve the quality of life in cities. Major applications of IoT in environmental monitoring include weather monitoring, endangered species protection, water quality, air quality, waste monitoring, and more.

3.5 Smart Buildings

They are digitization of buildings to provide people living in buildings a safe, efficient, comfortable, and convenient environment. Billions of devices are now installed and connected all over the world, thus enabling smart buildings to communicate with their owners, tenants, occupants, and maintenance teams. Smart buildings use IoT sensors to monitor, maintain, and control everything in the building such as lighting, humidity, occupancy, smart elevators, ventilation, shading, security, Co_2 monitoring to identify poorly ventilated areas in the building, and more. Smart buildings use integrated systems to share, exchange information to

facilitate collaboration in order to manage resources in cooperative way to improve building efficiency, optimize resource use, enhance security, reduce operating costs, and monitor and troubleshoot easily. Monitoring smart building 24×7 registers events such as abnormal activities, fire breakouts, or security breaches and helps management take proper care of the building for now and in the future. To build a smart building, the property owner should consider having a powerful wireless networking infrastructure. Distributed antenna system is the key component of building IoT systems as it allows emergency responders such as police or firefighters to interact with each other in case of building fires, earthquakes, or natural disasters. Cellular phone networks enhance the mobility of cellular devices to increase coverage of the whole building. A data analytics software can help the management team understand the data collected by IoT sensors and let them be more flexible to make the right decisions in certain conditions and cost constraints.

3.6 Maintenance Management

IoT-based predictive maintenance keeps track of the operating conditions of equipment and machines which make it easier and more efficient to monitor, maintain, and optimize asset utilization for better availability and performance especially in remote locations. Attaching IoT sensors to assets and service items excludes human errors and unnecessary visits to remote locations, ensure accuracy and availability of usable data, and gain better visibility into assets through real-time monitoring and receiving automatic alerts, notifications, and reports on time between failures, when operating conditions are out of specification, mean time to repair, and key performance indicators. Instead of waiting for a failure, technicians and mechanics can see equipment failures in real time during the breakdown and determine the object's exact location that needs maintenance; this helps technicians to predict machine failure and identify which parts to be replaced. Technicians can receive problem description, list of spare parts needed to fix the asset, options for repairs, and recommended actions to take which make them effective decision-makers. Maintenance will only be performed if it is required, thus reducing the costs of labor and spare parts. This will empower managers to keep productivity at maximum and the cost of repairs and downtime at minimum. Predictive maintenance reports contain failure data, system operating conditions at the time of failure in addition to previous repair data from the enterprise asset management (EAM). These allow manufacturers improve the quality of their products, optimize spare parts stocks, reduce downtime, control maintenance budgets, and increase customers' satisfaction.

3.7 Water Supply

IoT water supply systems monitor water quality in real time, conserve water supplies, and enable cities to function efficiently. An IoT smart water sensor tracks water quantity in the storage reservoir to turn on the water pump to refill the reservoir and switch off the water pump when it reaches the maximum level. IoT technology monitors water flow across the building to optimize water distribution among tenants and monitors water pressure to detect water leakage or wear of water pipes or equipment to reduce water wastage and maintain acceptable water pressure [15]. IoT smart water sensors track water quality by measuring the physical and chemical properties of the water such as temperature, pH, and turbidity [16]. Managers at different points of water supply chain use data collected by IoT water sensors to receive key insights into the changing conditions of water resources and equipment and become able to take on-demand data-driven corrective measures.

3.8 Manufacturing

IoT technology automatically connects machines, tools, and sensors on floor of the factory to provide production engineers and managers with the information they produce to monitor equipment and track parts in real time during the assembly and supply chain processes. With a granular visibility into the production process, managers can make more informed and smarter decisions to ensure reliability, compliance, and safety to optimize productivity. IoT technology provides data on how products are used that could be fed back in real time to manufacturers who can iteratively correct and rapidly design improvement, which improves prediction of demand, enables faster time to market, and enhances customer satisfaction. Implementing IoT in manufacture allows for more efficient energy saving as sensors can help managers determine places of waste, boost equipment efficiency, predict failures, and detect issues of compliance with quality assurance. Equipment failure is the main reason for poor production and poor-quality products, which result in more sales return, poor customer satisfaction, and reduced customers' trust in the products and finally damage the brand reputation. Moreover, repairing defective products consumes more resources and increases the production costs. High-quality products reduce costs and wastes, enhance customer experience, and increase product sales. Maintenance can be done based on machine needs at an exact time not on historical data or guessing because manufacturers may not know about machine faults which may cause production problems.

3.9 Transportation

IoT-based transportation has improved the conventional operations of transportation through embedding sensors, actuators, and other IoT devices. IoT devices collect data about the environment and transmit it for predictive analysis to make decisions within real time. A telematics device is an instrument that can be installed in a vehicle to record accurate up-to-date real-time information about location, idling time, tire pressure, fuel consumption that has better impact on the environment, vehicle activity, and driver behavior including driving style, alerts for harsh acceleration, how fast you brake, and the distance you drive. With telematics data, the operation managers can ensure that a vehicle is on its route. The managers can take adjustment actions if a vehicle has drifted from the optimal route based on a specific threshold. IoT-based systems help managers to better plan for journeys, monitor traffic congestion and vehicle's load, react quickly to traffic accidents, and improve safety by tracking vehicle location in case the vehicle has been stolen. Traffic management is a main application of IoT-based transportation. Traffic management includes smart parking, traffic lights, and smart accident assistance. An IoT-based smart parking system sends data through web/mobile application about free and occupied parking places. An IoT-based real-time traffic monitoring system dynamically handles traffic signals based on traffic density. Smart accident assistance automatically detects an *accident* and notify the nearest emergency unit. IoT technology facilitates tolling and ticketing processes where modern vehicles are equipped with IoT devices and can be sensed a kilometer away from the tolling station, which is correctly identified, and the barrier lifted for the vehicle to pass through. Smart vehicles are connected to the Internet and communicate with each other to prevent collisions and allow smooth traffic. In public transport management, IoT smart transportation can be widely used in automated ticketing and fare collection. It helps public transport operators and transit agencies to monitor vehicles routes, waiting times, and schedules, estimate the overall fleet performance, and provide tools to analyze and interpret the real-time data collected over short time periods. The IoT technology allows public transport systems to better serve its customers and create better customer satisfaction that leads to increased ridership. IoT devices installed in the buses of a fleet provide passengers in digital bus stops with accurate real-time arrival information to decrease passengers' average waiting time. IoT technologies allow for better communication with passengers through text messages on their mobile phones, which increases customers' satisfaction. Transit agencies can monitor passengers' behavior and travel patterns and send them personalized information on their mobile phones with updates on routes, closure of stations re-routing of buses, or delays. Figure 19 shows a vehicle OBD II Dongle telematics device with a vehicle GPS tracking.

Fig. 19 Telematics device

3.10 Warehouses

Smart warehousing is essential for the profitability of any business as it allows the company to optimize its operations and stay competitive in hard competition markets and volatile global economy. The management should adopt IoT technologies to determine the best layout and configuration of the warehouse to ensure optimum utilization of storage space to maintain a seamless workflow at its fullest efficiency and improve movement and fulfillment of goods through the warehouse. IoT smart warehouse wastes no resources and provides visibility into the flow of outgoing and incoming supply chain. Connected sensors track materials from ordering until the shipment reaches the end customer or third-party logistics (3PL) warehouses. IoT-based warehouse tracks the equipment and products more quickly and accurately, thus making the movement of products faster, and tracks the quantity and quality of goods by monitoring the temperature and location of the cargo within the warehouse in real time, which reduces food spoilage and results in increased profits and reduces management costs. IoT can help the warehouse management to calculate time, infrastructure, and budget needed to scale up the warehouse storage space using data collected by IoT devices. IoT-based warehouse collects inventory data to forecast the workload based on seasonal changes of demand and broadcast inventory information to warehouse managers to inform them of low stock, displaced products, unsuitable temperature, theft, and more. IoT robots in smart warehouses move independently and utilize sensors and cameras to help humans pick and pack products faster. IoT devices continuously run without feeling tired, which eliminates fatal human errors and reduces operation costs.

4 IoT Security and Privacy Issues

IoT devices connecting over the Internet are growing exponentially which causes a wide variety of potential concerns that relate to security and privacy. Adding more IoT devices to the Internet increases the vulnerability of connected IoT systems, which makes security needs in the heart of any decision to adopt IoT technology. IoT devices include surveillance cameras, drones, home appliances, smart home devices, monitors, sensor networks that can transmit data, smart toys, routers, and

Internet gateways. There are potential drawbacks to use IoT technology because most of these devices are developed with little attention to data protection and access control has opened gates for the hackers and attackers to invade IoT devices. Cyber-criminals are targeting IoT devices; file-less malware is the most obvious attack on IoT devices. It does not rely on physical files that can be transferred and stored on a victim machine that allows it to evade antivirus software. This means that it leaves little evidence behind it and can only be detected by sophisticated security applications. File-less attacks are spread via botnet that detects vulnerable applications. Rule-based detection can be able to detect malicious execution of commands. Machine learning techniques are now widely spread to detect file-less malware by studying the behavior of malwares [17]. In healthcare, unapproved access to IoT wearable devices can cause changes in the data collected by these devices, which may put the life of a patient at risk. In smart cities, safety penetrations IoT devices are risky and could pose risks on individuals' safety. In agriculture, safety attack on sensors can cause change in reading important information such as soil humidity, temperature, and more, which affect crop production. Hackers focused their efforts last year with the following tools.

4.1 IoT Malware

IoT malware families such as Aidra, Bashlite, and Mirai scan the ports of IoT to locate exposed ports and acquire default credentials on these devices to launch distributed denial-of-service (DDoS) attacks or gain access to IoT devices [18, 19]. IoT malware detection is either non-graph-based or graph-based detection methods. Non-graph-based methods classify a binary file as malicious or benign by extracting static features which are either high-level or low-level features. High-level features include operation code, which is a single instruction executed by the CPU and describes the behavior of an executable file. Strings are usually a sequence of characters stored in ASCII or Unicode format in an executable file. Printable strings contain valuable information such as IP address, URL, etc. to determine whether an executable file is malicious or not [20]. Low-level features include elf (executable and linkable format) file header which contains important information for malware detection and grayscale image where each executable file is converted to binary strings and combined into 8-bit vectors that represent hex value from 00 to FF [19]. Graph-based IoT malware detection methods include control flow graph (CFG) which is a directed graph that represents all possible execution paths of a program. Each block is represented by a vertex and each edge represents the control flow between basic blocks. In [21] the control flow graph (CFG) is used to demonstrate the differences and similarities between IoT malware and Android malware. Control flow graph (CFG) methods achieved 99.66% in detecting IoT malware using a dataset of 6000 malware and benign samples. Federated learning is used to detect malware affecting IoT devices. In [22] a deep learning method is proposed to detect the Internet of Battlefield Things (IoBT) malware and achieved 98.37% accuracy

rate and 98.59% precision rate. In [23] a framework for IoT malware detection is proposed that employs federated learning to train and evaluate supervised and unsupervised models without sharing critical data. This framework consists of a client side that is deployed on the RAN SLICING Edge Nodes or in the CLOUD SLICING Fog Nodes and a server side that is deployed in fog/cloud. The results showed that a lot of research is required to reach satisfying results.

4.2 Encrypted Threats

It is an encryption malware that helps attackers escape the secure socket layer (SSL) protocol and invade IoT networks with the intention of stealing data. Ransomware is an example of encryption malware that uses encryption to encrypt victim's information at ransom. Attackers encrypt a user's or organization's critical information so that they cannot access databases, applications, or files until a demanded ransom is paid. If attackers received the demanded ransom, information will be decrypted and owners can get use of it. Ransomware spreads quickly over networks and copies itself on other servers to encrypt files and databases, thus paralyzing entire organization. Ransomware threat is growing very fast generating very big revenue for hackers and paralyzing entire organizations by encrypting their critical information, thus causing a major damage [24]. IoT ransomware is capable of paralyzing the entire network of physical devices by controlling IoT devices, hitting on all IoT security aspects including authentication, integrity, and availability which cause financial losses and could be life threatening. Attacks occur on real-time IoT devices such as healthcare devices, smart vehicles, autopilots, etc. Attacks on these IoT devices are launched from multiple devices because they do not own user interfaces [25]. Botnet, malvertisement, or social engineering are the major methods for ransomware penetration [26]:

(i) Botnet: In any IoT network, botnets are incubators of all IoT malware including IoT ransomware. IoT malware penetrates the IoT network with the help of botnets, which may cause distributed DoS attacks or flooding attacks [27].
(ii) Social engineering: An attacker deceives the IoT network by acting as authorized users, to gain access to the IoT networks and steal sensitive information.
(iii) Malvertisement: Content delivery network (CDN) that appears to be benign can broadcast malware to be installed on IoT devices.

4.3 Perception Layer

It is responsible for data acquisition, so it is also called a sensor layer. This layer is vulnerable against many security attacks.

4.3.1 Node Capture

It is a serious attack against user authentication schemes through which an intruder can gain an unauthorized access of the IoT network. The attacker can perform various operations on the network such as modifying the memory content, modifying computation, or forging messages sent by the gateway to legitimate users and gain additional knowledge by interacting with the captured slave node to reveal cryptographic keys and try to break security. A captured node can make arbitrary queries on behalf of the attacker such as denial-of-service (DoS) attack against availability [28].

4.3.2 Replay Attack

It is a form of network attack where an attacker eavesdrops on a secure network communication to intercept it. The attacker can delay valid data maliciously or captures it and resends it to mislead the receiver as the messages or data appear authentic. The receiver will do what the attacker wants. The IoT replay attack reproduces a signal to control an IoT device to make spoofing and launch DoS attack.

4.3.3 Malicious Node

An intruder can add a malicious or infected node to existing network. Most malicious nodes can launch different attacks based on tampering, retransmission, and discarding methods [29]. Figure 20 shows an invisible node attack launched by malicious node C located between two legitimate nodes A and B that are indirectly connected. The malicious node C repeats the signals and messages between A and B to make them think they are directly connected. This way, malicious node C impersonates node A to node B and vice versa. Figure 21 shows a stolen identity attack launched by malicious node C which can steal authentication credentials such as cryptographic keys from node A. If malicious node C outraces legitimate node in updating the stolen credentials, then the credentials of the legitimate node will not be valid anymore. If a malicious node controls the legitimate node, it can abuse the trust relationship built with other legitimate nodes [30].

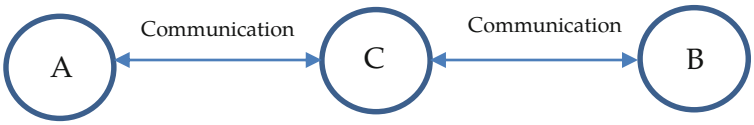

Fig. 20 Invisible node attack [30]

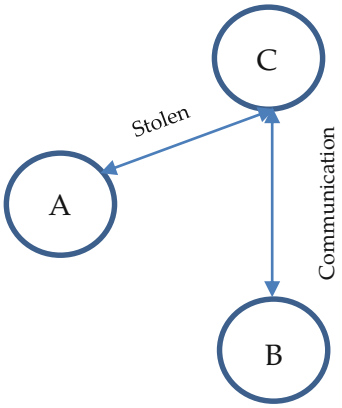

Fig. 21 Stolen identity attack [30]

4.4 Network Layer

This is a transmission layer that performs networking and routing by handling various networking devices. As it carries a large amount of information, it is a target for several types of attacks which may cause network congestion. The main types of attacks a network layer is susceptible to are authentication and integrity attacks [31]. The most common attacks on the network layer are:

4.4.1 DDoS (Distributed Denial-of-Service) Attack

It expends network resources that make services unavailable for actual users [32]. This attack attempts to prevent users from accessing the network services such as emails, portals, or other resources such as printers and storage devices. It floods the network with huge number of redundant traffic to make its resources unavailable, slowing down performance or even crashing the system [31].

4.4.2 Man-in-the-Middle Attack

In this attack, an intruder comes between the sender and receiver to intercept exchanged communication to steal personal information or impersonate both parties, which creates a real threat to confidentiality and integrity [33]. For example, an attacker can intentionally change the temperature recorded by an IoT sensor, malfunction a working device, and drive the whole process to failure [31].

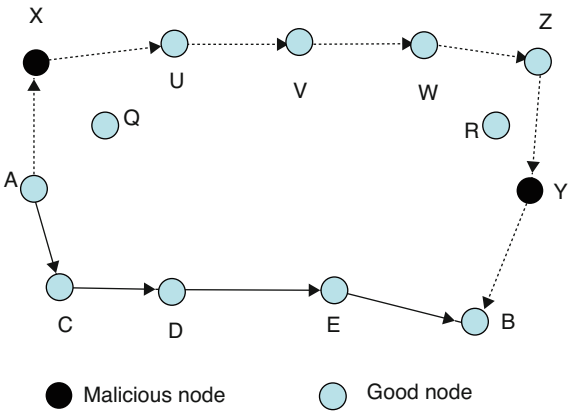

Fig. 22 Wormhole attack [34]

4.4.3 Spoofing Attack

Spoofing is easily launched when security is violated on a shared IoT network where IoT devices are sharing the same network with protected resources. When an IoT device on a shared network is hacked, the intruder can easily get access to the protected resources. Spoofing happens by impersonating an identity of a genuine IoT device using fake Internet protocol (IP), MAC addresses, or both to claim to be another genuine IoT device and gain illegal access to the IoT network. The intruder can then launch denial-of-service attacks or man-in-the-middle attacks to steal credential information and take control of genuine devices.

4.4.4 Wormhole Attack

It is one of the most challenging and severe internal attacks on IoT routing. It is very effective in attacking any protocol even with encrypted traffic [34]. Wormhole attack can insert information in wrong routes or topology information to make other nodes in the network believe they are closer to other nodes, which may be not true and can cause problems to the routing algorithm. Figure 22 shows a wormhole attack that forwards data through a tunnel from a compromised node to another malicious node at the other end of the network.

In Fig. 22 nodes *X* and *Y* are malicious nodes that formed a tunnel from *X* to *Y* to exchange packets. *X* falsely advertises that to reach *B*, a shortest path is through *X* but physically *B* is at far distance from node *X*. So, if node *A* wants to send a packet to node *B* on the other side of the network, the packet takes more time to reach the destination which is considered one of the wormhole attack symptoms [34].

4.4.5 Black Hole Attack or Drop Attack

It is a denial-of-service attack where an aggressive node displays itself as having the shortest route to the destination node using its routing protocol. The malicious node replies to the route requests before any actual node replies, thus creating a fake route. The malicious node acts as black hole and it intercepts the packets and discards them instead of relaying them, disrupting the communication between the nodes of the network without their knowledge [35]. The malicious node can launch this attack randomly or against a particular node at specific dates and times.

4.4.6 Sybil Attack

This attack is very destructive to sensor networks because a malicious node tries to gain illegal influence on the network by creating multiple fake identities that appear to be a real and unique identity to the outside. This malicious node can change the information reaching other nodes, generate false reports, and send spam messages. There are two types of Sybil attacks, namely, direct and indirect. In direct Sybil attack, honest nodes directly influenced a Sybil node, while in the indirect Sybil attacks, the nodes that directly communicate with Sybil nodes influence the honest nodes.

4.4.7 Sinkhole Attack

It is a routing attack in IoT networks. An attacker compromises a node in the network to launch attacks. This node tries to attract all the traffic from neighbor nodes by advertising fake routing update. Examples of sinkhole attacks are selective forwarding attack, acknowledging spoofing attack, dropping or altering routing information, and sending bogus information to base station [36]. In Fig. 23, node *M* launches sinkhole attack in tiny AODV. Node *A* sends RREQ to nodes *B*,*C*, and *M*. However, node *M* instead of broadcasting to node *E* just as nodes *B* and *C* do to node *D* replies back RREP to node *A*. Then node *A* will reject nodes *B* and *C* and forward packets to *M* because nodes *A* and *B* are very far to node *F* than node *M*.

4.4.8 Malicious Code Injection

It is the oldest known web application attack vector; SQL injection is one of these attacks. An attacker gains control of a working node in a network by injecting it with a malicious code. Firstly, the attacker probes the application that can accept untrusted data. By exploiting data input vulnerabilities such as data format, allowed number of characters, and amount of expected data, the attacker can launch denial-of-service attacks, resulting in loss of data integrity and loss of data, and compromise or even shut down the whole network.

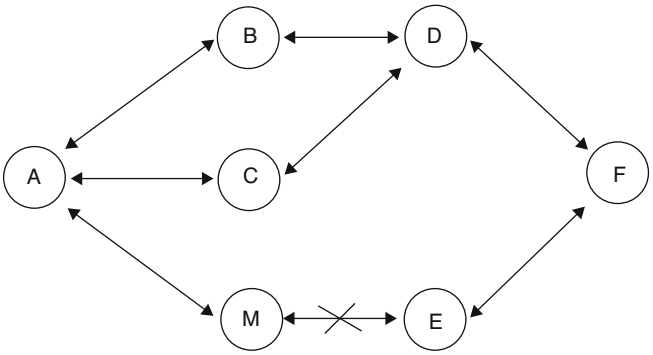

Fig. 23 Sinkhole in tiny AODV protocol (Teng and Zhang, [37]

4.5 Application Layer

4.5.1 Cross-Site Scripting

This is a dangerous injection attack where the attacker can change the content of the application [38]. In cross-site scripting (XSS) attacks, malicious scripts are injected into benign and trusted websites. The browser under attack could not know that the injected script must not be trusted and will execute it. Accordingly, the malicious script can gain access to cookies, session keys, or other sensitive information, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the victim's machine.

Cross-site scripting (XSS) attacks occur when [39]:

1. Input data enters into a web application through untrusted sources, most frequently a web request.
2. Data is within a dynamic content that is sent to a web user without being checked for malicious content.

There are three types of cross-site scripting (XSS) attacks: stored, blind, and reflected. In stored attacks the injected script is permanently stored on the target servers. The victim retrieves the malicious script when it requests the information stored on the server. Blind cross-scripting attacks occur when the attacker's malicious script is saved on the server. The attacker submits a feedback form that contains the malicious script. When the server admin opens the attacker's submitted form, the attacker's script is executed. Reflected attacks are sent to victims through different routes such emails or another website. When the victim clicks on a malicious link, browses a malicious site, or submits a specially crafted form, the injected code transfers to the vulnerable website, which reflects the attack back to the victim's browser. The victim's browser then executes the transferred malicious code.

4.5.2 Privacy and Confidentiality

It is an important issue that must be carefully handled. Unauthorized access of sensitive data is a serious attack. Endless IOT applications of smart health, smart houses, smart farming, self-drive vehicles, intelligent networks, and more require privacy [14]. Botnet attacks are another type of IOT attacks where botnets are used to launch attacks. These attacks may include malicious activities such as data theft, credential theft, unauthorized access, data theft, and distributed denial-of-service (DDoS) attacks. IoT and wearable devices are always sensing, collecting, and communicating data, which challenge the traditional social privacy and legal norms. Privacy and data breach are both significant concerns to most businesses, because it interrupts the work flow, activities, and network services [40]. Wearables generate a massive amount of data that is collected and analyzed and can be shared by several parties without its owner's knowledge. Individuals wearing wearable devices may not have control on these devices and could not approve or reject to whom this data is transferred, with whom it is shared, or how long it will be retained. This data can be sensitive such as medical, fitness, or personal health information that can be used for marketing purposes or used by insurance companies to increase their premiums or by employers for jobs-related issues [41].

5 IoT Data Analytics

Data analytics is an important component of IoT solution. It allows finding patterns, conducting forecasts, and integrating machine learning algorithms and predictive analysis and finds out insights from collected IoT data. IoT data analytics use data analysis tools to analyze huge data volumes generated by connected IoT devices to extract valuable information that can be used to improve processes, operations, and services. Without data analysis the purpose of IoT systems becomes operation automation not operation optimization. This makes data analysis processes be done by human experts which may not be available for most organizations and causes valuable data not to be used. IoT data analytics can detect data trends within collected IoT data. They can highlight expectations and deviations from normal trends or normal performance. The continuous analysis of gathered IoT data provides the management with continuous feedback on equipment performance to ensure that all equipment is running with high efficiency. Data analytic tools do not replace human experts but provide them with more insight into the ways to optimize the efficiency of equipment. Managers can put plans to cut operational costs and maintenance costs as they have the required information to predict costly breakdown of equipment and achieving strategic goals. Decision-makers can be confident that their choices are based on accurate and complete information obtained from real-time reports and alerts. Huge amount of IoT data from multiple disjoint resources that belong to different systems may have different structures that reduce data reconciliation and leads to inaccurate and incomplete data analysis, which is

considered a fundamental issue in IoT data analysis. Data not accessible by IoT data analytics tools or inaccurate collected data affect the accuracy of the generated reports.

6 AI-Powered IoT

The main role of IoT devices or sensors is to collect data. The traditional IoT processing sends data to a cloud server for processing to extract valuable information that helps managers have more insight into this data to make the right decisions. AI plays an important role in fast and accurate data analysis to improve the outcomes for users and service providers, maintain confidentiality of data and privacy, and provide security of IoT devices from cyberattacks. AI can create a predictive model which captures the information in your organization which can be used to examine data in real time [42]. The following steps help build a predictive model:

- Define the business to be analyzed, scope of analysis, and the desired output.
- Predictive models intensively depend on data. Streams of data collected or created by IoT sensors or devices that are embedded into machines are communicated to servers to be stored and ready for analysis.
- IoT data may be incomplete or contain noise which requires data preprocessing. Data preprocessing include data cleaning and complete missing data. IoT devices can aggregate and analyze data before it is transmitted to the server for ultimate analysis and action.

However, sending data collected by IoT devices to cloud server for analysis has issues with privacy, security, latency, storage, and efficiency. Data is vulnerable against man-in-the-middle attack where data can be intercepted by malicious people. So, keeping data on the IoT devices for processing improves security and privacy. Most of the data collected by some IoT devices such as surveillance cameras may be useless as nothing could happen most of the days which wastes valuable storage. Therefore, embedding intelligent systems in IoT devices allows these devices to collect data when necessary which reduces the required storage and the amount of data to be transmitted to the cloud server. Data transmission between IoT devices and the cloud server depends on the Internet. Latency occurs because of slow Internet connection where a long time is required to transmit data to the cloud server for analysis and return the output to the receiver. Edge computing is a possible solution for latency where processing of data should take place on the edge device. Edge devices have low memory, limited power, and low computation power; therefore, applications that are lightweight and more computationally efficient are required. Empowering edge devices with lightweight applications allows all data to be processed locally on these devices. With the advent of tiny machine learning (TinyML), it is possible to enable powerful artificial intelligence (AI) algorithms such as image understanding, voice recognition, hand gesture recognition, pose estimation, speech analysis, sequence analysis, and more to run efficiently on

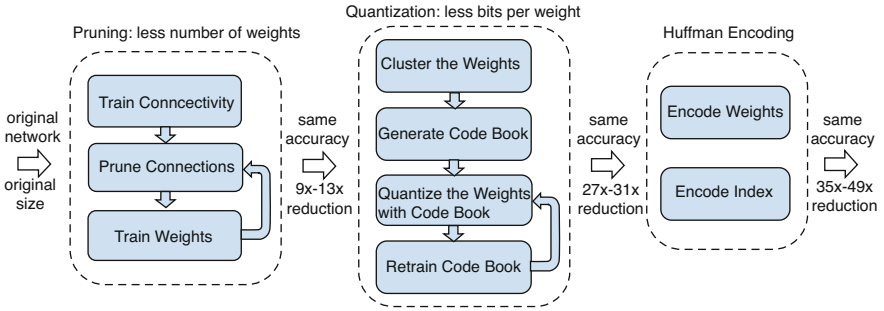

Fig. 24 The three-stage compression pipeline: pruning, quantization, and Huffman coding [43]

low-power mobile and IoT devices. TinyML is a type of machine learning that compresses deep learning networks to embed into tiny hardware such as IoT devices or mobile devices. TinyML algorithms are trained on desktop computers or in cloud servers as traditional machine learning algorithms; post-training is where TinyML starts. Deep compression is the main operation in the post-training phase. Figure 24 shows the three-stage pipeline for network deep compression: network pruning, quantization, and Huffman encoding [43]:

- *Network pruning:* reduces the number of weights by 10×
- Quantization: further improves the compression rate, between 27× and 31×
- *Huffman encoding*: reduces more the network size by storing the data in a maximum efficient way

The IoT devices that are powered with AI bring many benefits to businesses, for example, formal and informal activities to control situations and implement changes, designing and producing services specialized for customer's needs, and requirement and cognitive automation which automates low-level processes without human intervention. IoT-powered AI can discover patterns hidden in collected data which could not appear on devices or sensors, analyze it before transmitting it to other devices, predict risks and automate preventive actions, and determine redundant or time-consuming operations to eliminate or improve them to enhance the efficiency of the system. Machine learning combined with AI can be used to predict outcome and estimate parameters to improve accuracy. Fujitsu analyzes data collected by wearable devices to ensure that safety precautions are implemented by its workers [44]. Google analyzes the data collected by heat sensors in its data centers to reduce costs [45]. People can communicate with IoT devices using natural language processing which helps people to efficiently operate these devices. Robots in manufacturing are empowered with AI-powered sensors that make them more intelligent; self-driving vehicles are the best examples for hybrid IoT and AI as they can predict pedestrians' behavior and other neighboring vehicles. They can learn from each trip and become more intelligent to make appropriate actions. For example, they can predict weather conditions and road circumstances and learn to

become smarter to make appropriate actions. In retail industry, smart cameras can observe customers' behavior to predict when to reach the cashiers.

6.1 Benefits of AI-Powered IoT

Here are some of the most popular benefits of combining these two disruptive technologies to the businesses.

6.1.1 Boosting Operational Efficiency

AI in IoT crunches the constant streams of data and detects nondeceptive patterns on simple gauges. In addition, machine learning coupled with AI can predict the operation conditions and detect the parameters to be modified to ensure ideal outcomes. Hence, intelligent IoT offers an insight into which processes are redundant and time-consuming and which tasks can be fine-tuned to enhance efficiency. Google, for example, brings the power of artificial intelligence into IoT to reduce its data center cooling costs [46].

6.1.2 Better Risk Management

Pairing AI with IoT helps businesses to understand as well as predict a broad range of risks and automate for the prompt response. Thereby, it allows them to better handle financial losses, employees' safety, and cyber threats. Fujitsu, for example, ensures worker safety by engaging AI for analyzing data sourced from connected wearable devices.

6.1.3 Triggering New and Enhanced Products and Services

NLP (natural language processing) is getting better at allowing people to communicate with devices. Undeniably, IoT and AI together can directly create new products or enhance existing products and services by enabling the business to rapidly process and analyze the data. Rolls Royce, for example, plans to leverage AI technologies in the implementation of IoT-enabled airplane engine maintenance amenities. Indeed, this approach will support to spot patterns and discover operational insights [47].

6.1.4 Increase IoT Scalability

IoT devices range from mobile devices and high-end computers to low-end sensors. However, the most common IoT ecosystem includes low-end sensors, which offer floods of data. AI-powered IoT ecosystem analyzes and summarizes the data from one device before transferring it to other devices. As such, it reduces large volumes of data to a handy level and allows connecting a large number of IoT devices. This is called scalability.

6.1.5 Eliminates Costly Unplanned Downtime

In some sectors like offshore oil and gas and industrial manufacturing, equipment breakdown can result in costly unplanned downtime. The predictive maintenance with AI-enabled IoT allows you to predict the equipment failure in advance and schedule orderly maintenance procedures. Hence, you can avoid the side effects of downtime. Deloitte, for example, finds the following results with AI and IoT [48]:

- 20–50% reductions in their time invested in maintenance planning
- 10–20% increase in equipment availability and uptime
- 5–10% reduction in maintenance costs

6.1.6 Smart Thermostat

A user can check and manage the temperature from anywhere using an integrated thermostat with a smartphone based on the work schedule and temperature preferences.

Overall, IoT coupled with AI technology can lead the way to the advanced level of solutions and experience. To obtain better value from your network and transform your business, you should integrate AI with incoming data from the IoT devices.

7 Conclusion

All IoT systems architecture use IoT sensors connected to things through a network to collect data. Smart IoT devices can preprocess the data before transferring it to the data center or the cloud for analysis and storage. Every IoT system is composed of the same four components: devices, connectivity, platform, and an application. This chapter discussed the most famous IoT commercial and industrial applications with emphasis on the IoT devices used in each application. As many of IoT devices and sensors are connected and communicate with their data center or cloud using the Internet, the lack of security increases the vulnerability of these devices against cyberattacks. Also, personal information can be leaked using the IoT sensors which

violates users' privacy. Hence, IoT security and privacy issues are important issues which were discussed in this chapter. Finally, the conventional integration between AI and IoT devices was discussed where IoT devices or sensors collect data and send it to the cloud for intelligent applications to analyze this data and send the results to decision-makers. The next AI revolution is to embed intelligent applications in the IoT devices that are characterized with low resources so that data processing can be done locally. Therefore, tiny machine learning approach was discussed. Finally, the benefits of AI-powered IoT were presented.

References

1. Costa, B., Pires, P.F., Delicato, F.C., Li, W., Zomaya, A.Y.: Design and Analysis of IoT Applications: A Model-Driven Approach. In: 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Auckland, New Zealand, vol. 2016, pp. 392–399. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.81
2. Rusu, I.C.A.R.C.: Commercial and Industrial Internet of Things Applications with the Raspberry Pi. Apress (2020)
3. https://www.trialog.com/en/iot-systems-and-interoperability/ (Accessed on 03/14/2022).
4. Jayashankara, M., Udmale, S.S., Pandey, A.K., Singh, R.S.: IoT-based data analytics for the healthcare industry techniques and applications. Intell. Data-Centric Syst., 9–29 (2021)
5. Baker, S., Xiang, W., Atkinson, I.: Things for Smart Healthcare: Technologies, Challenges, and Opportunities. IEEE Access (2018)
6. Naresh, V.S., Pericherla, S.S., Murty, P.S.R., Reddi, S.: Internet of Things in healthcare: Architecture, applications, challenges, and solutions. Comput Syst Sci Eng. **6**, 411–421 (2020)
7. Anand, G., Heuss, L.: Feasibility of breath monitoring in patients undergoing elective colonoscopy under propofol sedation: A single-center pilot study. World J Gastrointest. Endosc. **6** (2016). https://doi.org/10.4253/wjge.v6.i3.82
8. Hashim, N., Norddin, N., Idris, F., Yusoff, S.N.I.M., Zahari, M.: IoT blood pressure monitoring system. Indonesian J. Elect. Eng. Comp. Sci. **19**(3), 1384–1390. ISSN: 2502–4752 (2020). https://doi.org/10.11591/ijeecs.v19.i3.pp1384-1390
9. Nelson, B.D., et al.: Wireless technologies for implantable devices. Sensors (Basel, Switzerland). **20**(16), 4604 (2020). https://doi.org/10.3390/s20164604
10. Ratnaparkhi, S., Khan, S., Arya, C., Khapre, S., Singh, P., Diwakar, M., Shankar, A.: Smart agriculture sensors in IOT: A review. Mater. Today: Proceed.. (In Press)
11. Sushanth, G., Sujatha, S.: IOT based smart agriculture system. IEEE (2018)
12. Caro, F., Sadr, R.: The Internet of Things (IoT) in retail: Bridging supply and demand. Business Horizons. **62**, 47–54 (2019)
13. Syed, A.S., Sierra-Sosa, D., Kumar, A., Elmaghraby, A.: IoT in smart cities: A survey of technologies, practices and challenges. Smart Cities. **4**, 429–475 (2021). https://doi.org/10.3390/smartcities4020024
14. Raghuvanshi, A., Singh, U.K.: Internet of Things for smart cities- security issues and challenges. Mater. Today: Proceed. https://doi.org/10.1016/j.matpr.2020.10.849
15. Natividad, J.G., Palaoag, T.D.: IoT based model for monitoring and controlling water distribution. Int. Conf. Inform. Technol. Digit. Appl., IOP Conf. Series: Mater. Sci. Eng. **482**, 012045. IOP Publishing (2019). https://doi.org/10.1088/1757-899X/482/1/012045
16. Daigavane, V.V., Gaikwad, M.A.: Water quality monitoring system based on IOT. Adv. Wireless Mobile Commun.., ISSN 0973–6972. **10**(5), 1107–1116 (2017)

17. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/ (Accessed on 07/01/20).
18. Ngo, Q.-D., Nguyen, H.-T., Le, V.-H., Nguyen, D.-H.: A survey of IoT malware and detection methods based on static features. **6**(4), 280–286 (2020)
19. Ngo, Q.-D., Nguyen, H.-T., Le, V.-H., et al.: A survey of IoT malware and detection methods based on static features. ICT Exp. **6**(4), 280–286 (2020)
20. Plu, T.N., Hoang, L.H., Touan, N.N., Tho, N.D., Binh, N.N.: CFDVex: A novel feature extraction method for detecting cross-architecture IoT malware. In: Proceedings of the Tenth International Symposium on Information and Communication Technology, pp. 248–254 (2019)
21. Alasmary, H., et al.: Graph-based comparison of IoT and android malware. In: Proceedings of International Conference on Computational Social Networks, pp. 259–272 (2018)
22. Azmoodeh, A., et al.: Robust malware detection for Internet of (Battlefield) things devices using deep eigenspace learning. IEEE Trans. Sustain. Comput., 88–95 (2018)
23. Rey, V., Sánchez, P.M.S., Celdrán, A.H., Bovet, G.: Federated learning for malware detection in IoT devices. Comp. Netw. **204**(26), 108693 (2022)
24. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html (Accessed on 05/09/2022).
25. Wani, A., Sathiya, R.: Ransomware protection in IoT using software defined networking. Int. J. Elect. Comp. Eng. **10**(3), 3166–3174
26. Bertino, E.: Botnets and internet of things security. Computer. **50**(2), 76–79 (2017)
27. Azmoodeh, A., Dehghantanha, A., Conti, M., Choo, K.K.R.: Detecting crypto-ransomware in IoT networks based on energy consumption footprint. J. Ambient Intell. Human. Comput. **9**(4), 1141–1152 (2018)
28. Butun, I., Osterberg, P., Song, H.: Security of the internet of things: Vulnerabilities, attacks and countermeasures. https://arxiv.org/pdf/1910.13312.pdf
29. Li, B., Ye, R., Gao, G., Liang, R., Liu, W., Ken Cai, E.: A detection mechanism on malicious nodes in IoT. Comp. Commun. **151**(1), 51–59 (2020)
30. Jiang, J., Han, G., Zhu, C., Dong, Y., Zhang, N.: Secure localization in wireless sensor networks: A survey. J. Commun. **6**(6), 460–470 (2011)
31. Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., Bashir, A.K.: A survey of security and privacy issues in the Internet of Things from the layered context. https://arxiv.org/pdf/1903.00846.pdf (Accessed on 05-19-2022).
32. Prabhakar, S.: Network security in digitalization: Attacks and defence. Int. J. Res. Comput. Appl. Robot. **5**, 46–52 (2017)
33. Conti, M., Dragoni, N., Lesyk, V.: A survey of man in the middle attacks. IEEE Commun. Surv. Tutor.
34. Bhosale, S.D., Sonavane, S.S.: Wormhole attack detection in internet of things. Int. J. Eng. Technol. **7**(2.33), 749–751 (2018)
35. Fazeldehkordi, E., Amiri, I.S., Akanbi, O.A.: A study of blackhole attack solutions. Syngress. (2016)
36. Kibirige, G.W., Sanga, C.: A survey on detection of sinkhole attack in wireless sensor network. https://arxiv.org/ftp/arxiv/papers/1505/1505.01941.pdf#:~:text=Sinkhole%20attack%20is%20a%20type,drops%20or%20altered%20 routing%20information.
37. Teng, L., Zhang, Y.: Secure routing algorithm against sinkhole attack for mobile wireless sensor network, in computer modeling and simulation, in proceedings of 2010. ICCMS'10. Second IEEE Int. Conf. Comp. Model. Simul. **4**, 79–82 (2010)
38. Gupta, S., Gupta, B.B.: Cross-site scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. Int. J. Syst. Assur. Eng. Manage. **8**, 512–530 (2017). https://doi.org/10.1007/s13198-015-0376-0
39. https://owasp.org/www-community/attacks/xss/ (Accesed on 06/18/2022).
40. Tawalbeh, L.'a., Muheidat, F., Tawalbeh, M., Quwaider, M.: IoT privacy and security: Challenges and solutions. Appl. Sci. **10**, 4102 (2020). https://doi.org/10.3390/app10124102
41. Thierer, A.D.: The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation. Richmond J. Law Technol. **XXI**(2) (2015)

42. Nelson, J.W. (editor), Jayne, F., Mary, A. H. (Co-editors): Using Predictive Analytics to Improve Healthcare Outcomes, Wiley (2021)
43. Han, S., Mao, H., Dally, W.J., Deep compression: Compressing deep neural networks with pruning, trained quantization and Hufman coding, 4th international conference on learning representations, *ICLR 2016*, San Juan.
44. https://www.fujitsu.com/au/imagesgig5/IoT_solutions_UBIQUITOUSWARE_Digital_ Solutions.pdf (Accessed on 05/06/2022).
45. https://static.googleusercontent.com/media/www.google.com/en//corporate/datacenter/dc-best-practices-google.pdf (Accessed on 05/06/2022).
46. https://www.clariontech.com/blog/ai-and-iot-blended-what-it-is-and-why-it-matters (Accessed on 06/18/2022).
47. https://www.rolls-royce.com/country-sites/sea/discover/2021/tapping-ai-technologies-to-create-solutions-of-tomorrow.aspx (Accessed on 05/06/2022).
48. https://www.clariontech.com/blog/ai-and-iot-blended-what-it-is-and-why-it-matters (Accesed on 06/18/2022).