5 IoT Applications and Case Study

Syllabus

Broad categories of IoT applications : Consumer IoT, Commercial IoT, Industrial IoT, Infrastructure IoT, Military Things (IoMT)
IoT Case studies : Home automation with IoT, River water pollution monitoring, Smart city street light control and monitoring, Health care monitoring, Voice Apps on IoT device.

Contents

5.1 Broad Categories of IoT Applications

- With the advent of the Internet of Things era, homes, cities and almost everything is becoming smart. Those smart objects can sense the physical world by obtaining data from sensors, affecting the sensed world by triggering actions using actuators, engage users by interacting with them whenever necessary, and process gathered data to provide useful information to us.
- An increasing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things.
- Examples of such objects include thermostats and Heating, Ventilation, and Air Conditioning (HVAC) monitoring and control systems that enable smart homes. There are also other domains and environments in which the IoT can play a remarkable role and improve the quality of our lives.
- These applications include : Transportation, health care, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult.
- Currently, the IoT vision is mainly focused on the technological and infrastructure aspect, as well as on the management and analysis of the huge amount of generated data.
- Consumer devices are always a public concern, but there are currently five types of IoT applications :
  a) Consumer IoT : Such as light fixtures, home appliances, and voice assistance for the elderly.
  b) Commercial IoT : IoT applications in the healthcare and transport industries, such as smart pacemakers, monitoring systems, and vehicle to vehicle communication (V2V).
  c) The Industrial Internet of Things : IIoT includes digital control systems, statistical evaluation, smart agriculture, and big industrial data.
  d) Infrastructure IoT enables the connectivity of smart cities through infrastructure sensors, management systems, and user-friendly user apps.
  e) Military Things (IoMT) applying IoT technologies in the military field, such as robots for surveillance and human-wearable biometrics for combat.

5.1.1 Consumer IoT

- Consumer IoT refers to the billions of physical personal devices, such as smartphones, wearables, fashion items and the growing number of smart home appliances, that are now. Connected to the internet, collecting and sharing data.

- Consumers want IoT products that fit seamlessly into their daily lives and simplify routine tasks. Finding keys, locking the front door, turning lights on and off, these tasks can be controlled with wireless technologies.
- Fig. 5.1.1 shows consumer IoT.

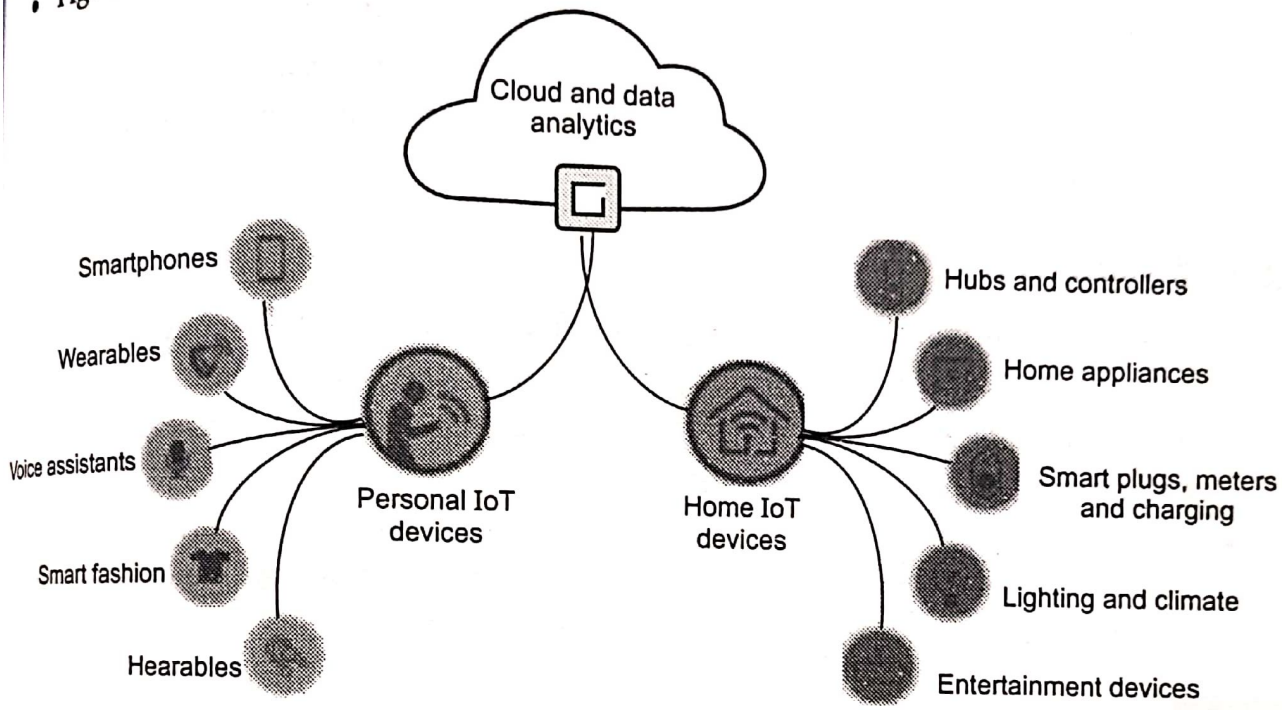


Fig. 5.1.1 Consumer IoT

- Consumer smart assistants, such as Amazon Alexa, Google Home and Apple Homepod, are the hubs for consumer IoT. They build on stable technologies : Bluetooth (BLE,) Wi-Fi and derivatives of ARM mobile processors. On the software side, they all rely on Natural Language Processing (NLP) and acoustics that are fairly mature.
- The real-time data collected from connected devices and smart connected consumer products can generate insights and provide personalized information and services to the consumers.
- Smart homes, connected vehicles, wellness and fitness through wearables, smart retail and smart farming are a few examples of how businesses can achieve their short - term and long - term goals.
- Business-to-consumer value : Using product data to inform better customer experience, personalization, reliability, preemptive support, convenience, security, product/service improvement, etc.
- Business-to-business value : Using product data to inform operational efficiencies, improve sales conversion, marketing decisions, security, inventory optimization, etc.

- Business-to-ecosystem value : Using product data to inform partner strategies, integrations, APIs, content needs, supply chain efficiencies, etc.
- Consumer IoT has long held a reputation for poor security standards. Homes today are filled with connected devices. It's not just smart speakers, it's app - enabled espresso machines and wifi - connected security cameras.
- The majority of IoT devices purchased for the home are relatively cheap and little effort is made to protect them at a hardware or software level at this end of the spectrum by manufacturers.

5.1.2 Commercial IoT

- Commercial IoT lies between consumer IoT and industrial IoT applications.
- Commercial IoT refers to devices and systems for business and enterprise use. These can vary broadly by sector. IoT is increasingly leveraged in healthcare, event venues, office buildings, and more.
- Specifically, when we talk about commercial IoT some of the key use cases that we see are intelligent asset tracking, smart office and buildings, connected lighting, sensing and monitoring of all types and location services.

5.1.3 Industrial IoT

- Industrial IoT (IIoT) infrastructure should be protected by a comprehensive security solution (device-to-cloud) that does not disrupt operations, service reliability or profitability.
- Industrial IoT refers to devices and systems used in manufacturing or industrial purposes. Examples include supply chain asset tracking and fleet tracking.
- Fig. 5.1.2 shows industrial IoT system architecture. (Refer Fig. 5.1.2 on next page)
- The common requirements of the IoT are technical requirements independent of any specific application domain.
- IoT non-functional requirements refer to the requirements related to the implementation and operation of the IoT itself , i.e. Interoperability, scalability, reliability, high availability, adaptability, manageability.
- IoT functional requirements refer to the requirements related to the IoT actors, these requirements have been categorized as,
  1. Application support requirements
  2. Service requirements
  3. Communication requirements
  4. Device requirements

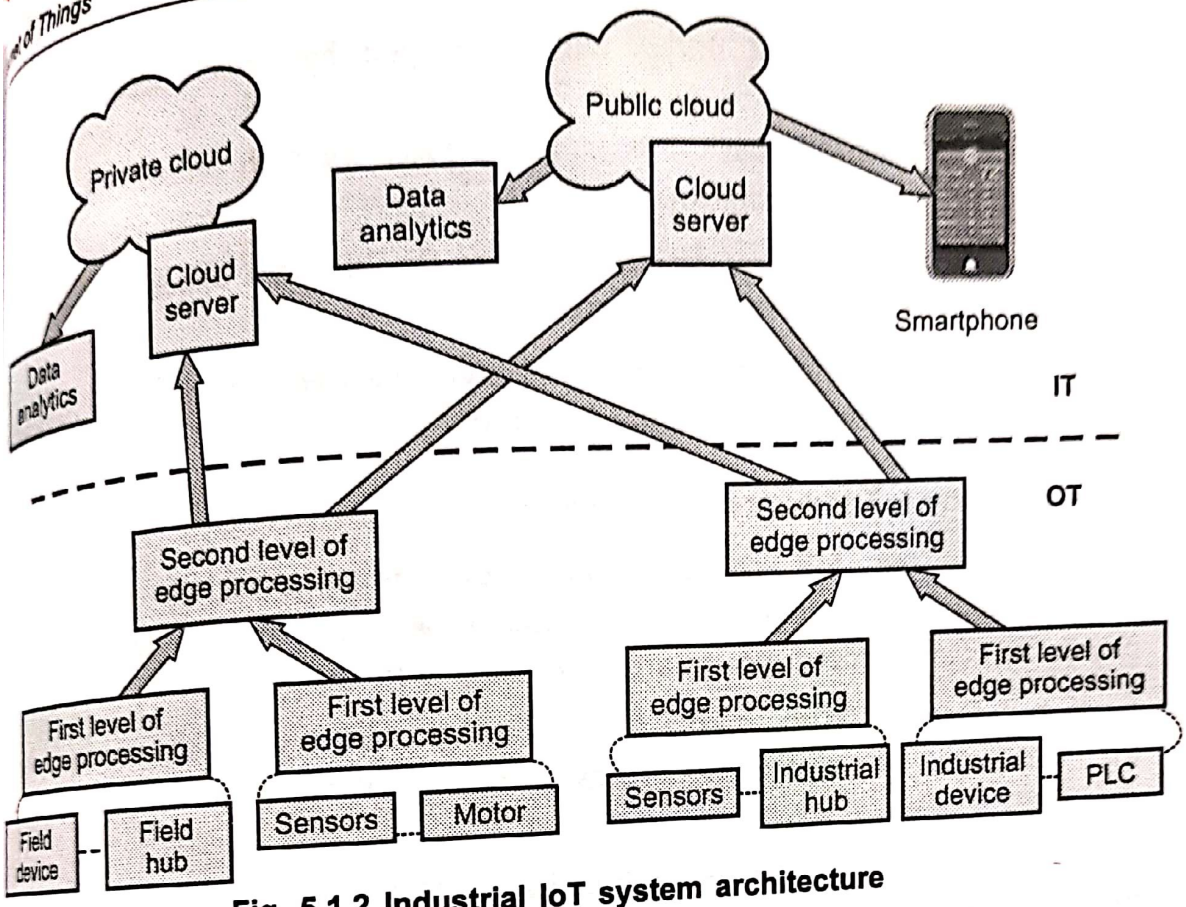


Fig. 5.1.2 Industrial IoT system architecture

5. Data management requirements
6. Security and privacy protection requirements.

- The IoT application capabilities for industrial application should meet requirements such as :

1. Reliability : Reliable IoT devices and systems should allow a continuous operation of industrial processes and perform on-site activities
2. Robustness : The IoT application and devices should be robust and adapted to the task and hard working conditions
3. Simple to use
4. Low maintains cost
5. Support optimal and adaptive set of features
6. It must have reach sensing and data capabilities
7. Industry grade support and services. The IoT applications should be supported over years in operation by a set of rich tools and continuously updated services
8. Support standardization
9. Security and safety.

- The industrial internet of things will be shaped by the appearance of three features :
  1. The enhancement of basic mechanical devices through sensors and other data producing devices ("smartness");
  2. The possibilities of ever faster and more flexible data allocation, transfer and processing (computing capacities);
  3. The ever increasing digital interconnectivity between the engaged devices and computational capacities (digital integration).

Challenges faced by IoT industry applications

1. Security. As the IoT connects more devices together, it provides more decentralized entry points for malware. Less expensive devices that are in physically compromised locales are more subject to tampering.
2. Trust and Privacy. With remote sensors and monitoring a core use case for the IoT, there will be heightened sensitivity to controlling access and ownership of data.
3. Complexity, confusion and integration issues. With multiple platforms, numerous protocols and large numbers of APIs, IoT systems integration and testing will be a challenge to say the least. The confusion around evolving standards is almost sure to slow adoption.
4. Evolving architectures competing standards. With so many players involved with the IoT, there are bound to be ongoing turf wars as legacy companies seek to protect their proprietary systems advantages and open systems proponents try to set new standards. There may be multiple standards that evolve based on different requirements determined by device class, power requirements, capabilities and uses. This presents opportunities for platform vendors and open source advocates to contribute and influence future standards.
5. Concrete use cases and compelling value propositions. Lack of clear use cases or strong ROI examples will slow down adoption of the IoT. Although technical specifications, theoretical uses and future concepts may suffice for some early adopters, mainstream adoption of IoT will require well-grounded, customer-oriented communications and messaging around "what's in it for me."
6. There are several wireless standards which can be used to connect devices to a network, most are still developing. That means delays as products play catch - up with new networking standards.

5.1.4 Infrastructure IoT

- Five things are making up an IoT infrastructure are IoT platforms, access technologies, data storage and processing, data analytics, and security. An essential part of any internet - connected device, these five pillars are what enable growth for future IoT solutions.

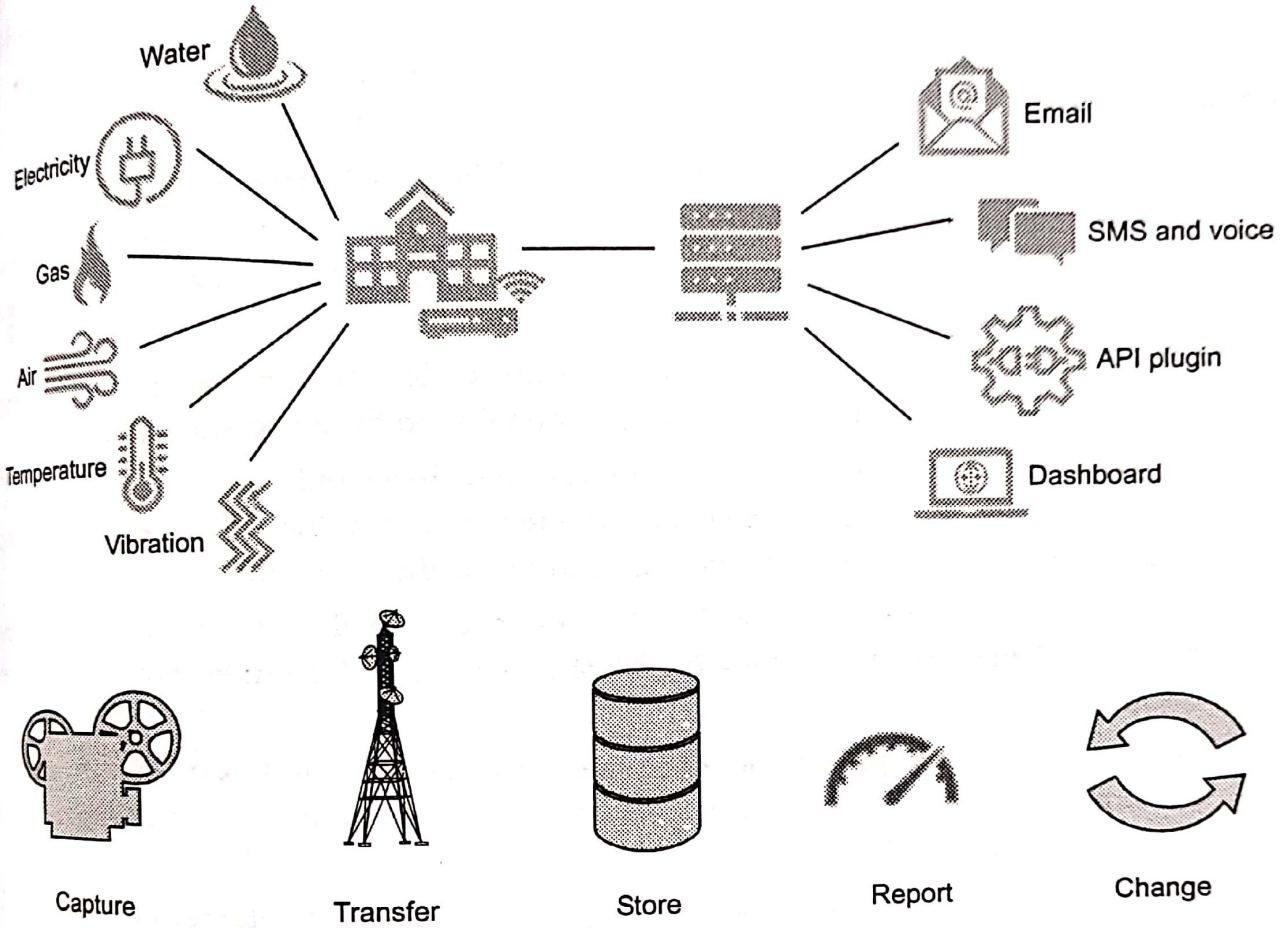


Fig. 5.1.3

- Smart infrastructure also includes implementing charging stations in parking systems, city fleets, shopping malls and buildings, airports, and bus stations across the city. Electronic Vehicle (EV) charging platforms can be integrated with IoT to streamline the operations of EV charging and addresses the impact of the power grid.
- A simple IoT infrastructure can be broken down into five key areas, capture, transfer, store, report and change.
- Capture covers the type of data source and the way the information is captured. This could be temperature or power consumption using digital, analogue or Modbus inputs. This data can then be transferred directly to the cloud using LoRaWAN for example or it can be transmitted to a gateway first using RF 868 mHz and then from the gateway to the cloud using GPRS 2G/3G.

- The data could be stored on the IoT supplier's cloud or sent via an API to the user's own cloud. From the cloud the data can be Reported and ingested in several ways. This could be in the form of a dashboard, an email alert or via an API into existing reporting tools.
- Once the information has been ingested it can be used to influence some form of change may that be a physical input or an automated response back via the IoT infrastructure or another system.

5.1.5 Military Things (IoMT)

- The IoMT is the application of Internet of Things (IoT) technologies and concepts to the military domain. Military IoT adoption is still in its infancy, however defence companies and the armed forces are eager to prepare, understand and leverage the IoT.
- There are clear military benefits from the use of IoT devices for the armed forces, ranging from vehicle maintenance to personnel monitoring to stock control.
- In today's scenarios military commanders may have only several minutes to be presented with an assessment of the situation in a way that is quickly assimilated, to assess potential courses of action and to make their decision.
- It needs to draw upon all possible sources to ensure that the most complete and relevant picture can be created of the situation, and the implications of different decisions understood.
- However, the integration of heterogeneous sensors and systems diverse in technology, environmental constraints and level of fidelity is a challenging issue not only for the military organizations.
- To provide a response to these challenges, the concept of Internet of Things (IoT) is extensively developed world-wide with focus on civilian applications. IoT is considered as an integral part of Future Internet and could be defined as a **dynamic global network infrastructure** with self-configuring capabilities based on standard and interoperable communications protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.
- The concept of IoT developed for civilian market does not fit the military requirements. Highly dynamic and disruptive environment, fragile nature of wireless communications, especially at lower tactical levels, specific requirements for speed and fidelity with which information must be exchanged and analysed requires robust and effective mechanisms, as well as specific applications that present IoT solutions do not provide.

- The Internet of military things refers to a network of sensors, wearables, and other devices that use cloud and edge computing to give advantage to a fighting force.
- Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices that increases the capacity and speed of data transfer and provides several add - on facilities.
- IoMT is a type of Internet of Things designed for combat operations and warfare based upon smart technology and artificial intelligence. It comprises a complex network of interconnected entities in the military domain that continually communicate with each other to accomplish a broad range of activities in a more efficient and informed manner.

5.2 Home Automation with IoT

- Home automation is the automatic control of electronic devices in your home. These devices are connected to the Internet, which allows them to be controlled remotely.
- Interconnected devices enable to intelligently monitor and control smart homes in a future Internet of Things.
- Energy saving applications, for example, control indoor climate and electricity usage by employing context information to switch off appliances (e.g., lights, computers), reduce room temperature, close windows, or stop warm water circulation.
- Home automation works on three levels :
  1. **Monitoring** : Monitoring means that users can check in on their devices remotely through an app. For example, someone could view their live feed from a smart security camera.
  2. **Control** : Control means that the user can control these devices remotely, like planning a security camera to see more of a living space.
  3. **Automation** : Finally, automation means setting up devices to trigger one another, like having a smart siren go off whenever an armed security camera detects motion.

5.2.1 Smart Lighting

- Smart control the lights with automation signal system to save energy. Smart, connected lighting is the next - generation energy - efficient LED products with additional sensors to sense things such as occupancy and temperature.

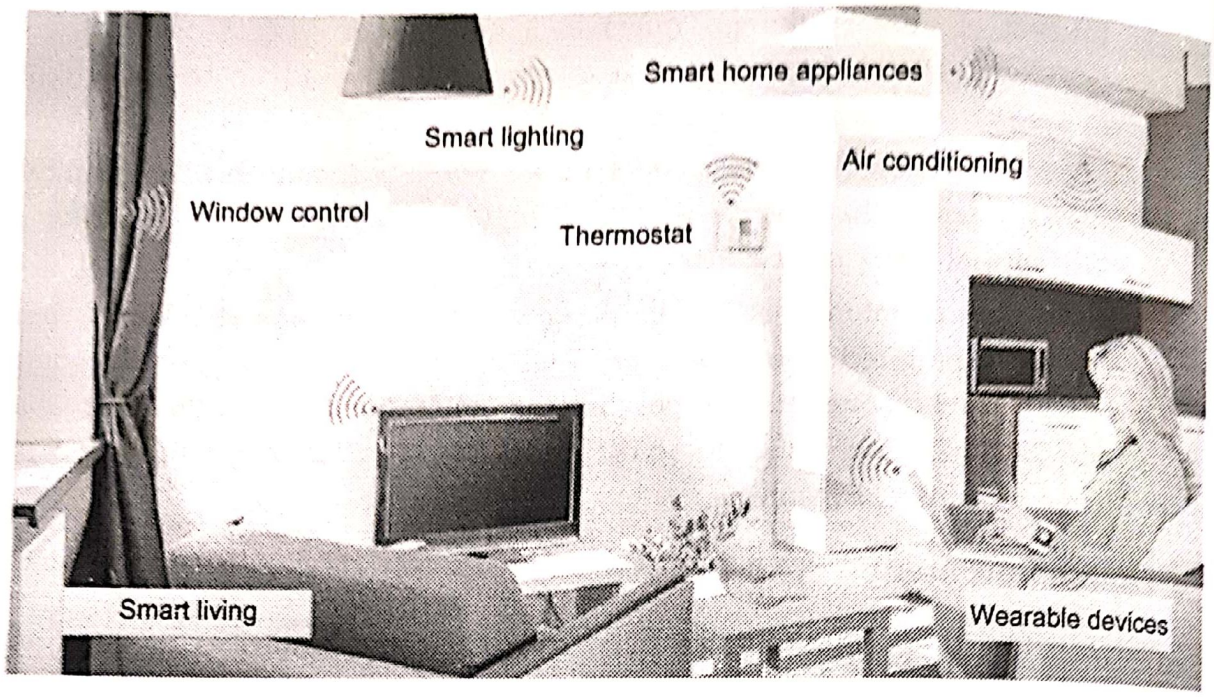


Fig. 5.2.1 Smart home

- In automatic light control system, Light Dependent Resistor (LDR) sensor is used to detect bright /medium /dim /dark conditions.
- It is simple enough to envision the addition of sensors and communications to create that initial concept of smarter, more adaptive lighting. If people are present, turn the lights on; if not, turn them off. Or use your smart phone to connect to the lighting system and tune it to the desired brightness level or to a particular color.
- Smart lighting is considered the one of the main solutions for energy reduction by means of controlling lighting level according to desired need with minimum energy consumption.
- Smart - lighting systems utilize motion and light sensors for performing the control algorithms.
- The system uses motion and light sensors for detecting the surrounding environment. There are lamps controlled with the specific lighting level in order to supply the adequate amount of lighting required without affecting the user visibility.
- Certainly the required lighting level is strongly dependent on the weather conditions. In clear weather at night might require more luminance than cloudy one, due to the reflection from the clouds.
- While during mist and foggy weathers require the highest possible lighting level, as the visibility reaches its lowest. On snowy weather it might require an intermediate level between clear and foggy.

- During night it requires high lighting levels, while at day it needs just fade level to provide guidance or turn off if the weather is clear. The lighting concentration in the yard is affected by the above conditions.

5.2.2 Smart Appliances

- The role and scope of smart appliances in the home (Washer, dryer, refrigerator, dishwasher, fridge, freezer, air conditioner, vacuum cleaner and so on) is on the increase with the market being estimated to have a year on year compound growth of slightly over 15 %.
- Connecting everyday objects to the internet is an essential element of the IoT. Some appliance suppliers use a low power wireless network to communicate over such as bluetooth, whilst others utilise the existing higher powered Wi-Fi network used for a tablet or computer wireless connectivity. Once a network is in place objects can populate the home environment and communicate with the user and each other.
- The ability of an object to respond to remote commands and change its behaviour makes it an active device, such as the new Hive heating thermostat or a Sky+ box.
- Where the remote object has no ability to respond to remote control requests then it is considered passive as with some fixed cameras, microphones or temperature sensors.
- IR Sensor : It will be activated in the automated mode to detect person entering or coming out of the room and set a counter based on that. If the counter show there is a person inside it will light up the room automatically and turn on the AC depending upon the temperature reading.
- Sensors provide data about motion, occupancy, glass breakage, door and window openings, water leaks, light intensity, temperature, energy consumption, camera, and even appliance plug insertion or removal.
- Controllers turn power on and off or adjust settings on appliances, furnaces, air conditioners, space heaters, fans, pool pumps, water heaters, lighting, home theatres, music, motorized blinds, door locks, and plug loads.
- To be deemed intelligent, an appliance's sensors and controllers should use internet protocol communication.
- Smart refrigerators can keep track of the items stored and send updates to the users when an item is low on stock.
- Smart TV allow user to search video and movies from the Internet on a local storage drive, search TV schedule, fetch news and other things from the Internet.
- OpenRemote is the professional open source middle-ware for an Internet of Things. Integrate any device or protocol, and design your own user interface and

automation. Use our online designer, sync to the controller, and control with this app.

- OpenRemote is a state of the art open source software platform for building control and automation.
- OpenRemote allows for designing a fully customizable building and home control solution without the need to actually write code.

5.2.3 Intrusion Detection

- Intrusion Detection System (IDS) includes both hardware and software mechanisms and IDS is responsible for identifying malicious activities by monitoring network environment and system.
- The purpose of home intrusion detection system is to detect intrusions using sensors and raise alerts, if necessary.
- With the help of Light dependent resistor and PIR motion sensor, it detect the motions in the room. If a motion is detected, system capture the image with the help of a webCam and store locally. Now the alerts are sent to the user with the captured image.
- Fig. 5.2.2 shows block diagram of intrusion detection.

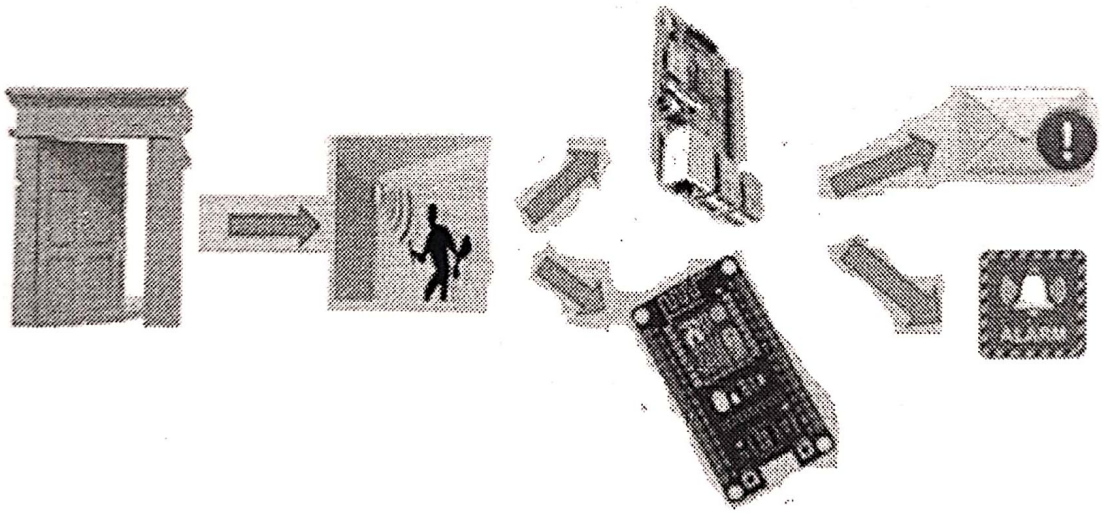


Fig. 5.2.2 Block diagram of intrusion detection

- To detect any form of intrusion in restricted areas and report it immediately, following concept is used.
  1. A PIR sensor is required to detect the presence of any human being in the room.
  2. An RFID is required to validate the presence of the person in the room by tallying his identity with those in the database.

3. A camera is required to click the picture of the room and send it via email as an alarm.
4. An internet connection is required to register all these movements on a website so that it can be accessed from any place and any device.

- The different input / output devices are controlled using TCP/IP over the IEEE 802.11 standard protocol. Data being gathered from sensors, such as PIR sensors, temperature sensors, IR transmitter and receiver is being processed on micro - controller as a server.
- Passive Infrared Sensor (PIR) Sensor : PIR sensor is an electronic sensing device that senses infrared (IR) light emitted from entities in its field of view and used to detect motion in its range. It is activated only in the security mode to detect any unwanted motion at the entrance. If any unwanted movement is detected then it will signal the microcontroller to take necessary steps.
- Alarm : It will only be activated in the security mode when some intruder is detected by the PIR motion sensor.
- Cloud controlled intrusion detection is possible by using location aware services. Here geo - location of each node is independently detected and stored in the cloud.
- Some intrusion detection system uses UPnP technology. It is based on image processing to recognize the intrusion.

5.2.4 Smoke for Gas Detection

- Smoke or gas detector sensor which detects the smoke and turns on the buzzer alarm and all these are update on the web page.
- MQ2 is a semiconductor type sensor, which can appropriately sense the presence of smoke, LPG, methane, butane, propane and other hydrocarbon.
- When it comes in contact with the gas to be monitored, the electrical resistance of the sensor decreases; enabling the microcontroller to respond to the situation.
- When it detects the concentration of combustible gas in the air it outputs its reading as an analog voltage. The sensor can measure concentrations of flammable gas of 300 to 10,000 ppm. The sensor can operate at temperatures from – 20 to 50 °C and consumes less than 150 mA at 5 V.
- The MQ-2 smoke sensor reports smoke by the voltage level as output. The more smoke is there, the greater the voltage output. The MQ-2 also has a built-in potentiometer to adjust the sensitivity to smoke.
- By adjusting the potentiometer, one can change how sensitive it is to smoke, so there is a form of calibrating it to adjust how much voltage it will give in relation to the smoke it is exposed to.

5.3 River Water Pollution Monitoring

- In conventional systems, the monitoring process involves the manual collection of sample water from various regions, followed by laboratory testing and analysis. This process is ineffective, as this process is arduous and time-consuming and it does not provide real - time results.
- The quality of water should be monitored continuously, to ensure the safe supply of water from any water bodies and water resources. Hence, the design and development of a low - cost system for real-time monitoring of water quality using the Internet of Things (IoT) is essential.
- Monitoring water quality in water bodies using Internet of Things helps in combating environmental issues and improving the health and living standards of all living things.
- The proposed system monitors the quality of water relentlessly with the help of IoT devices, such as, NodeMCU. The in-built Wi-Fi module is attached in NodeMCU which enables internet connectivity transfers the measured data from sensors to the Cloud.
- Fig. 5.3.1 shows water monitoring system.

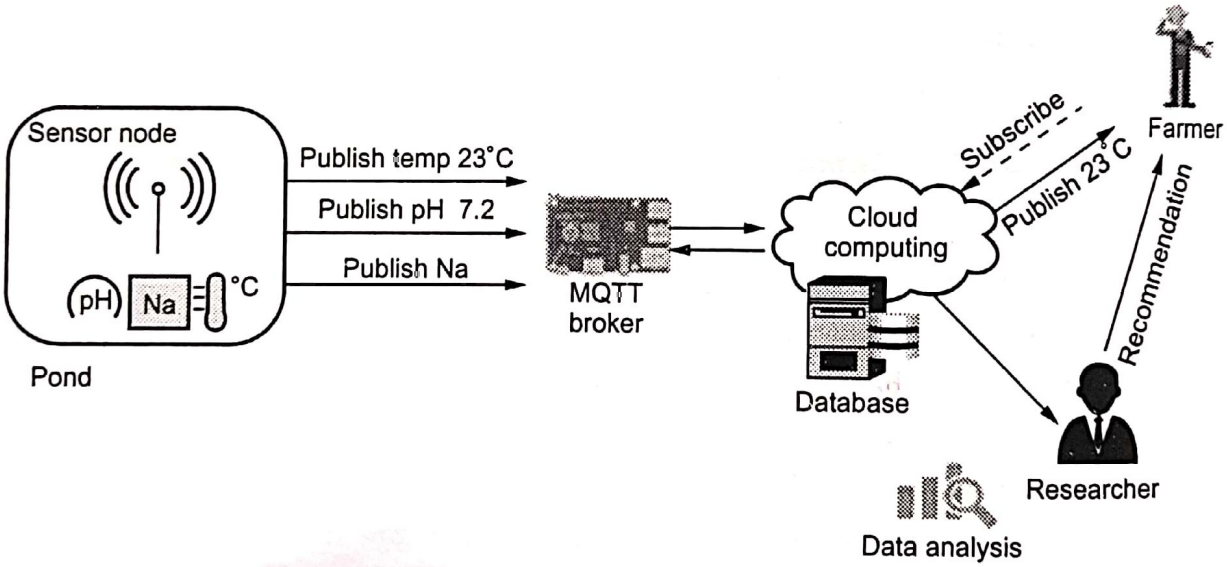


Fig. 5.3.1 Water monitoring system

- The system mainly consists of sensor node as publishers, and Raspberry pi MQTT broker, and mobile client devices as subscribers. The sensor nodes are built with small embedded devices, LoRa wireless interface, and water quality sensors, i.e. water temperature sensor, pH sensor, and salinity sensor.
- **Water quality sensor :** The pH meter is used for the quality check if water is safe for use.

- **Temperature sensor :** A device which gives temperature measurement as an electrical signal is called as temperature sensor. This electrical signal will be in the form of electrical voltage and is proportional to the temperature measurement.
- **Water level sensor :** This sensor will help us decide if we have enough quantity of water to be supplied. An ultrasonic wave is triggered from the sensor and distance to target is determined by calculating the time required after the echo is returned. The sensor emits a high-frequency pulse, generally in the 20 kHz to 200 kHz range, and then listens for the echo.
- Sensor node technical specification is listed below :

Microcontroller	Arduino MEGA 2560
Wireless Interface	LoRa Shield with 915 MHz Antenna
Sensors	Water Temperature, Salinity, pH
Battery	12 V 18AH Rechargeable Sealed Lead Acid
Solar Cell	20 WP 12 V
Packet Size	17 bytes
Transmission Interval	60 seconds

5.4 Smart City Street Light Control and Monitoring

- The number of urban residents is growing by nearly 60 million every year. In addition, more than 60 percent of the world's population will be living in cities by 2050.
- As a result, people occupying just 2 percent of the world's land will consume about three-quarters of its resources. Moreover, more than 100 cities of 1 million people will be built in the next 10 years.
- Over the past decade, the city of Amsterdam, the Netherlands, has developed a vision for collaborating, envisioning, developing, and testing numerous connected solutions that could pave the way to a smarter, greener urban environment.
- Fig. 5.4.1 shows concept of smart city. (Refer Fig. 5.4.1 on next page.)
- Smart city includes :
  1. Smarter management of city infrastructure using big data analytics
  2. Collaboration across multiple and disparate agencies using cloud technologies
  3. Real - time data collection, enabling quick response using mobile technologies
  4. Enhanced security : Improved public safety and law enforcement, and more efficient emergency response
  5. Better city planning improved schematics, project management and delivery

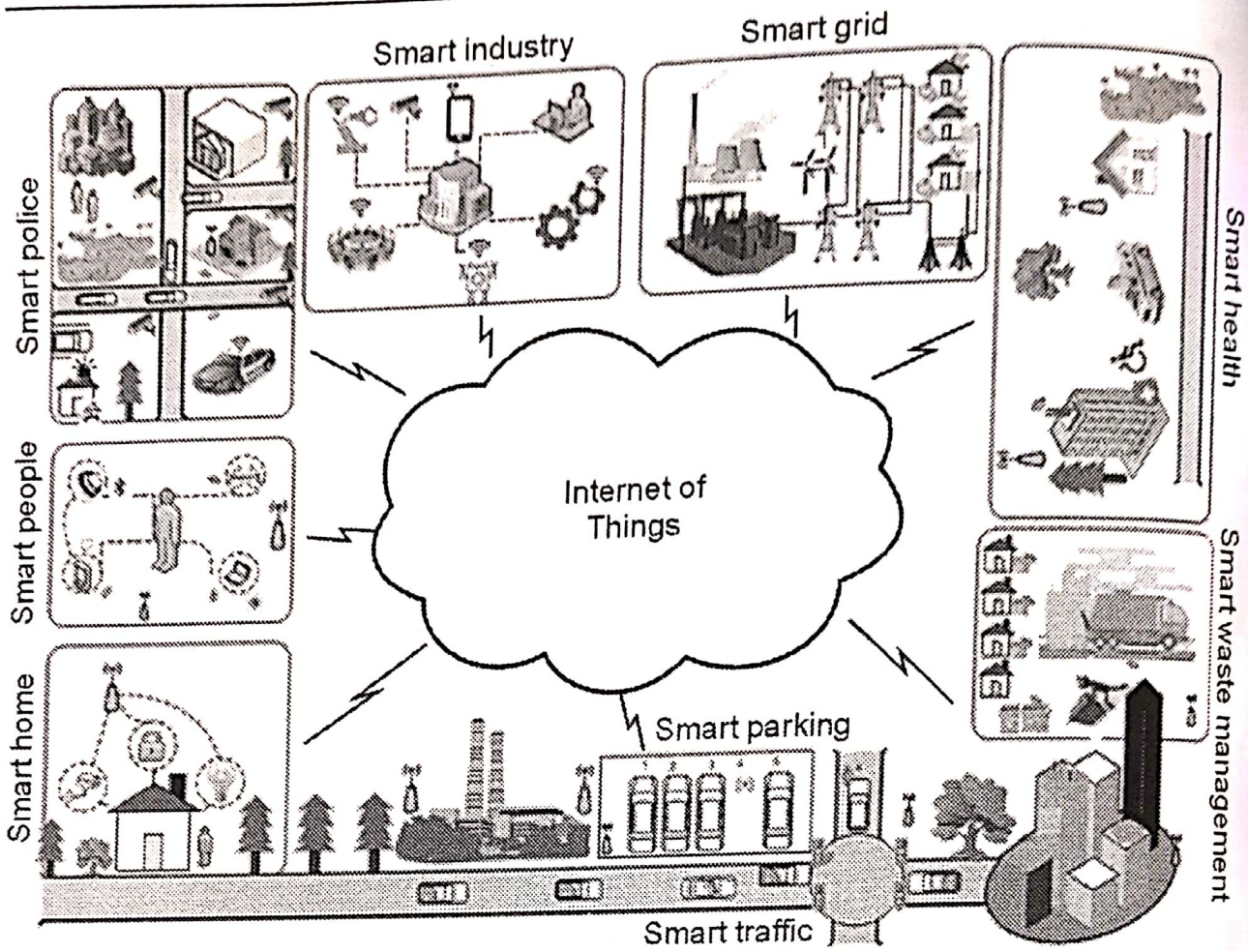


Fig. 5.4.1 Smart city

6. Networked utilities smart metering and grid management
7. Building developments more automation, and better management and security.

- With smart city applications producing continuous large data from heterogeneous sources, existing relational database technologies are inadequate to handle such huge amounts of data given the limited processing speed and the significant storage expansion cost.
- To address this problem, big data processing technologies, which are based on distributed data management and parallel processing, have provided enabling platforms for data repositories, distributed processing, and interactive data visualization.

5.4.1 Smart Parking

- Traffic congestion is major problem in big cities. Searching for a parking space is a routine (and often frustrating) activity for many people in cities around the world.

- After finding parking space to the driver, he parks the vehicle, it maybe spend small amount of time to looking for a city council parking attendant to pay the parking fees.
- The smart parking system is designed by making use of some IOT supportable hardware's such as raspberry pi, auridino boards etc.
- Smart parking systems typically obtains information about available parking spaces in a particular geographic area and process is real - time to place vehicles at available positions.
- It involves using low-cost sensors, real-time data collection, and mobile-phone-enabled automated payment systems that allow people to reserve parking in advance or very accurately predict where they will likely find a spot.
- When deployed as a system, smart parking thus reduces car emissions in urban centers by reducing the need for people to needlessly circle city blocks searching for parking.
- It also permits cities to carefully manage their parking supply smart parking helps one of the biggest problems on driving in urban areas; finding empty parking spaces and controlling illegal parking.

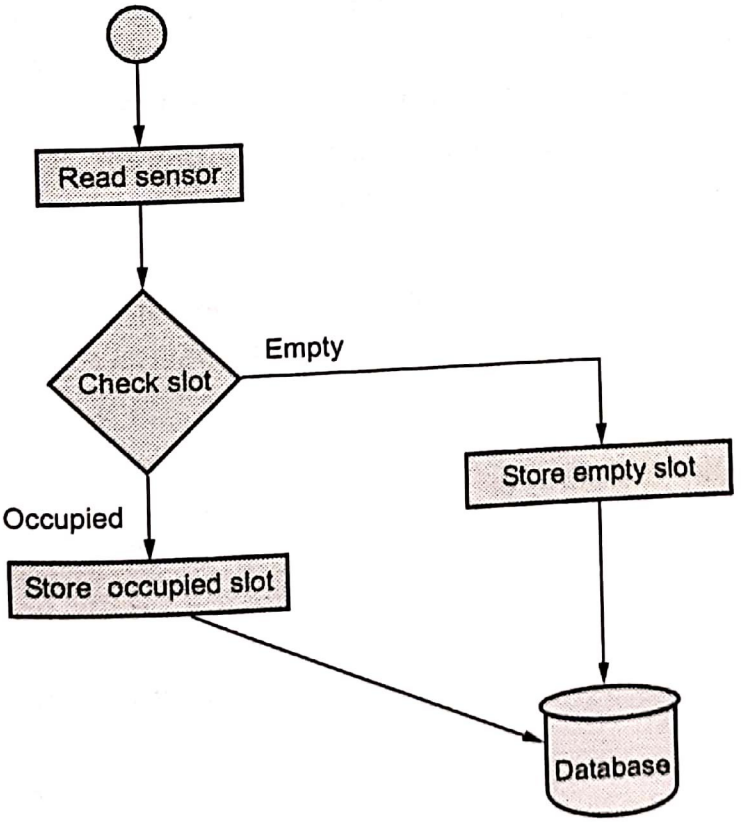


Fig. 5.4.2 Process specification for smart parking IoT system

- Smart parking application can be accessed by drivers from smart phones, tables. Sensor is used for each parking slot, to detect whether the slot is empty or occupied.
- Local controller collect the information and send to server using Internet. Fig. 5.4.2 shows process specification for smart parking IoT system.
- Each parking slot contains the sensor and it reads at regular intervals. Sensor sends the status information to local processing centre.
- Fig. 5.4.3 includes four layers : a sensing, networking, middleware and application layer. (See Fig. 5.4.3 on next page).
- Sensing layer defines a platform where sensor devices are embedded into the parking lot to detect car presence/absence, and RFID devices located at the parking gates and strategic points of the parking are used to identify cars based on a unique mapping between RFID tags and car.
- Networking Layer : TCP/IP over Ethernet for connecting the gateway to the parking server and database and Internet access for remote access to the smart parking system from outside.
- Middleware layer hosts different databases and associated servers and manages all of the software intelligence provided by the smart parking system to provide smart services to users by enabling communication between the application layer where services are requested and the lower layers where smart devices are embedded into the parking lot to provide smart services.
- The application layer is the layer where the different services are defined and provided to different users. Client devices have been connected via the TCP/IP protocol to a parking database.
- Parking availability status by integrating into the car detection system sources of light on parking spots, which are controlled by actuators to inform of the status of a parking spot : e.g., red for occupied, green for empty, yellow for reserved and blue for out of service.
- Remote availability checking using the Internet and/or the GSM network to check in real time the availability of the smart parking system.
- The data of smart parking lots are able to provide profits for both customers and merchant's daily lives in the smart cities. This service works based on road sensors and intelligent displays which lead drivers to the best path for parking in the city.

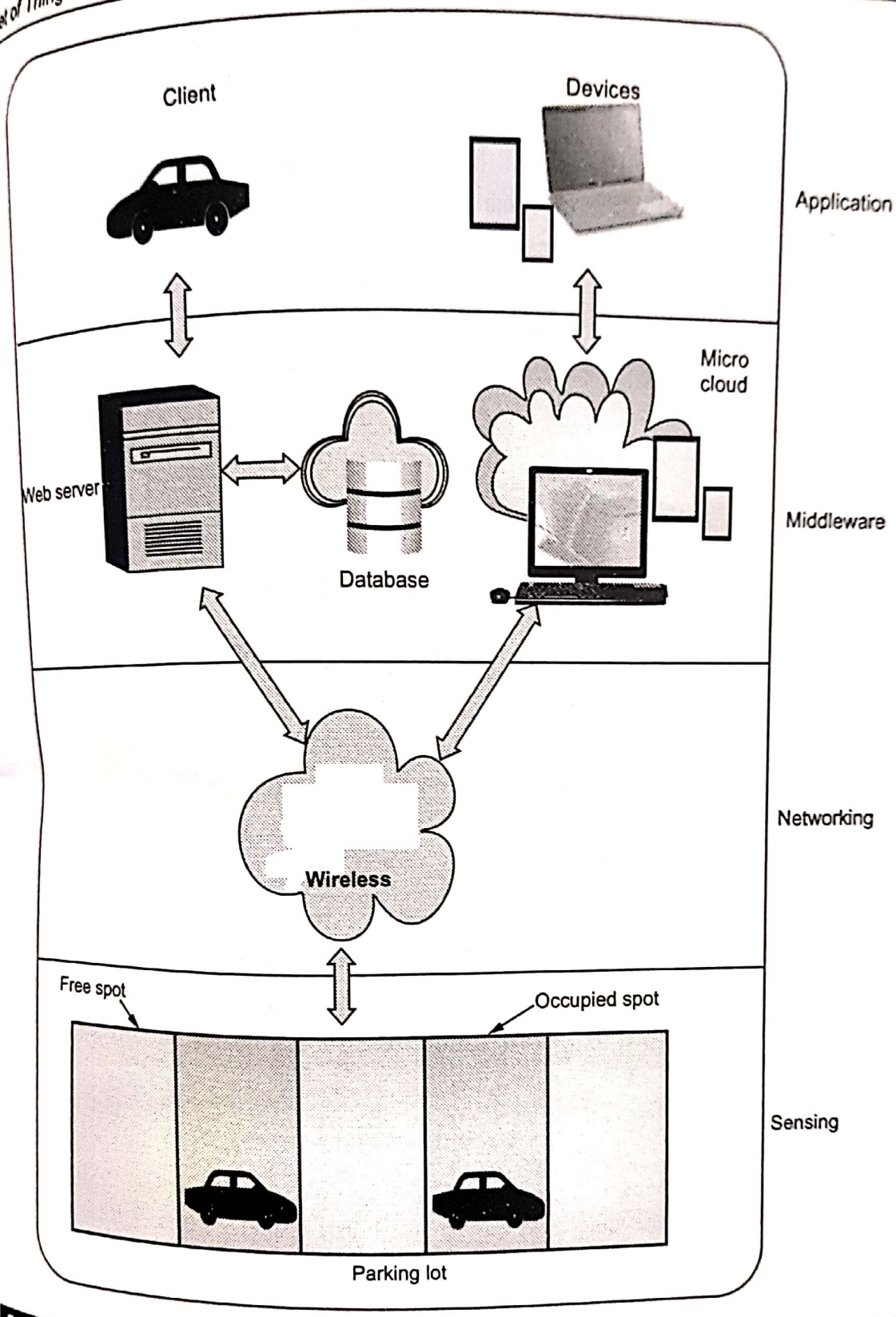


Fig. 5.4.3

5.4.2 Smart Lighting

- The street lighting is one of the largest energy expenses for a city. The street light section comprises of all the light lamps in an area with current sensors and RF

module. 'N' street lights of this section communicates with local controller unit wirelessly through RF module (Zigbee). 'N' local controller unit communicates with main server through IoT due to its global coverage area.

- Smart light infrastructure is the backbone of the IoT in smart cities. Smart and wireless street light luminaries can act as service gateways for other street level IoT devices.
- Smart street lights are intelligent lights that gather dynamic data i.e. data that keep changing dynamically by time, through some sensors and generate required information for the request claimed by a citizen on road.
- Smart street light saves energy by sensing the surrounding through their sensors expecting some other sensor in some other device.

5.4.3 Smart Roads

- Sensor is installed on road to provides road traffic condition, travel time estimation, congestion and accident.

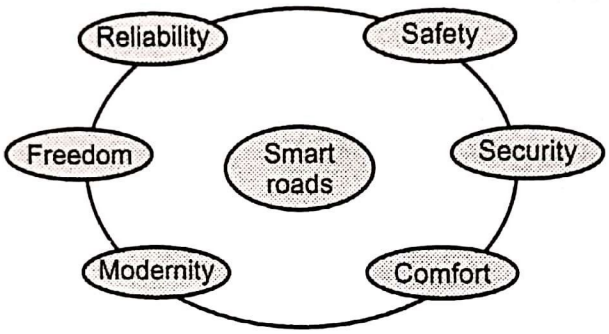


Fig. 5.4.4 Smart roads characteristics

- Sensor collect this information and stored on the central database using cloud. This information helps for solving traffic congestion, making safe driving, keeping road condition upto date.
- User can access the information from the cloud. User also get real time information.
- Real time traffic maps can be obtained to enable smooth flow. Traffic can be reduced with systems that detect alternate routes. User get timely information so they can locate a traffic free road, saving time and fuel. This information can reduce traffic jams and pollution improves the quality of life.

5.5 Health Care Monitoring

- The World Health Organization (WHO) defines E - health as : E - health is the transfer of health resources and health care by electronic means. It encompasses

three main areas : The delivery of health information, for health professionals and health consumers, through the internet and telecommunications.

- E - health provides a new method for using health resources - such as information, money, and medicines and in time should help to improve efficient use of these resources.
- E - health brings special characteristics. The monitoring device's environment is a patient; a living and breathing human being. This changes some of the dynamics of the situation. Human interaction with the device means batteries could be changed, problems could be called in to technical support and possibly be resolved over the phone rather than some type of service call. In most cases, the devices on the patient are mobile not static with regard to location.
- Fig. 5.5.1 shows high level E - health ecosystem architecture.

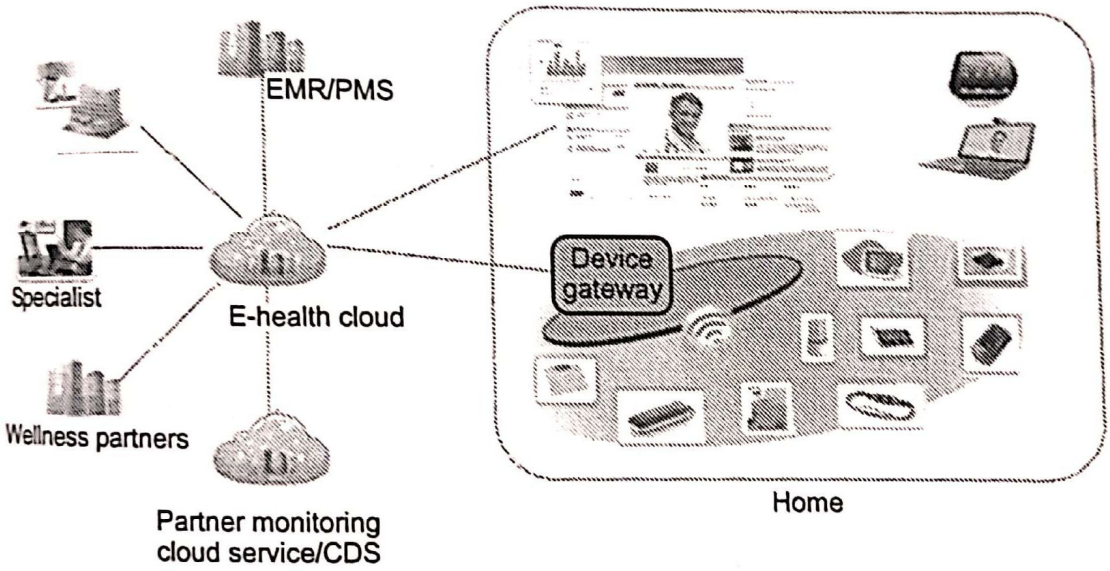
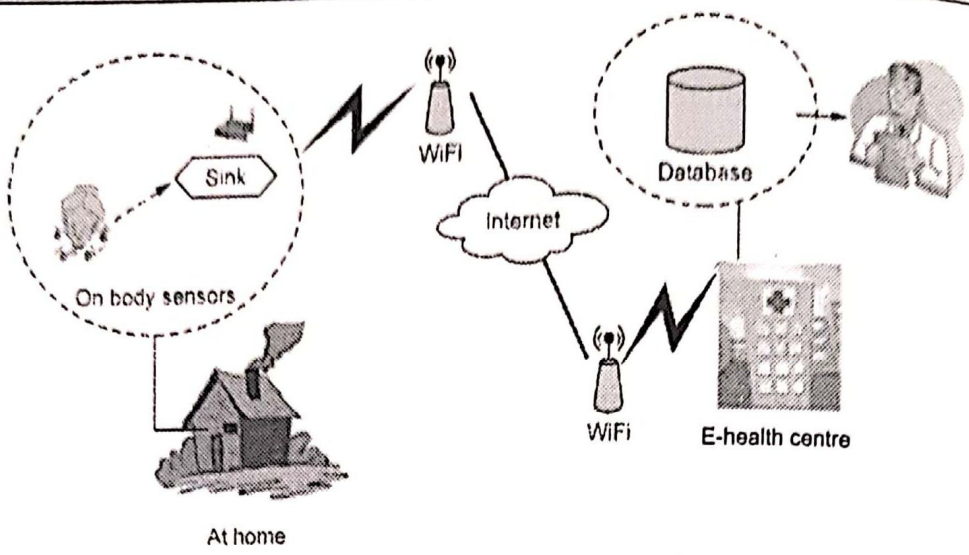


Fig. 5.5.1 High level E - health ecosystem architecture

- The data flow architecture focuses on the source of the data, the destination the data and path the data. The source of the data is typically the sensor.
- The data can be either locally cached or is sent to the upstream systems without storing in the sensor. The path taken by the data includes a gateway, which can also cache some of the data and do distributed processing.
- Intermediate hubs can also store and process the data to filter out or make certain decisions. A distributed rules engine is used to make distributed decisions at the closest point of care. This enables data traffic to be filtered and processed efficiently without having every data being processed by the cloud service



- The development of wireless networks has led to the emergency of a new type of E - healthcare system, providing expert-based medical treatment remotely on time.
- With the E - healthcare system, wearable sensors and portable wireless devices can automatically monitor individuals' health status and forward them to the hospitals, doctors and related people.
- The system offers great conveniences to both patients and health care providers. For the patients, the foremost advantage is to reduce the waiting time of diagnosis and medical treatment, since they can deliver the emergent accident information to their doctors even if they are far away from the hospital or they don't notice their health condition.
- In addition, E - health system causes little interruption to patient's daily activities. For the health care providers, after receiving the abnormal signals from the patients, appropriate treatment can be made, which saves medical resources.
- Furthermore, without direct contact with medical facilities, medical personnel or other patients, the patients are unlikely to be infected with other diseases.
- However, to ensure the security and privacy of patient's medical records encounters a lot of challenges :
  1. How to achieve the confidentiality and integrity of patients' information,
  2. The security of wireless body area network,
  3. The privacy and unlink ability of patients' health status,
  4. The undeniability and unlinkability of doctors' treatment,
  5. The location privacy of patients, the fine - grained access control of patient's medical record, the mutual authentication between patients and hospitals, etc.
- It would be useful to create an up-to-date bibliography on secure E - healthcare systems.

6 Voice Apps on IoT Device

There will be three types of voice communication in IoT environments :

1. Bi - directional voice communication
2. Mono - directional voice communication
3. Voice recognition.

- Reasons that voice is suited to a range of IoT applications :
  1. Speech is the natural mode of communication for humans. It is both intuitive and easier to convey commands verbally.
  2. Voice recognition is particularly appealing when the human's hands or eyes are otherwise occupied.
  3. Voice telephony is an efficient means of bi - directional voice communication with machines that can listen, and respond without the need for complex commands.
  4. Cost saving factors : Voice integration could potentially challenge the need for a touch screen on many devices, as it reduces the cost for devices that will be dormant for the majority of the time.
- The IoT market is broad and encompasses a range of consumer, commercial and industrial applications where voice can play a role. There are significant differences between the drivers for implementing voice into consumer products and from those that drive the same technology in the consumer market.

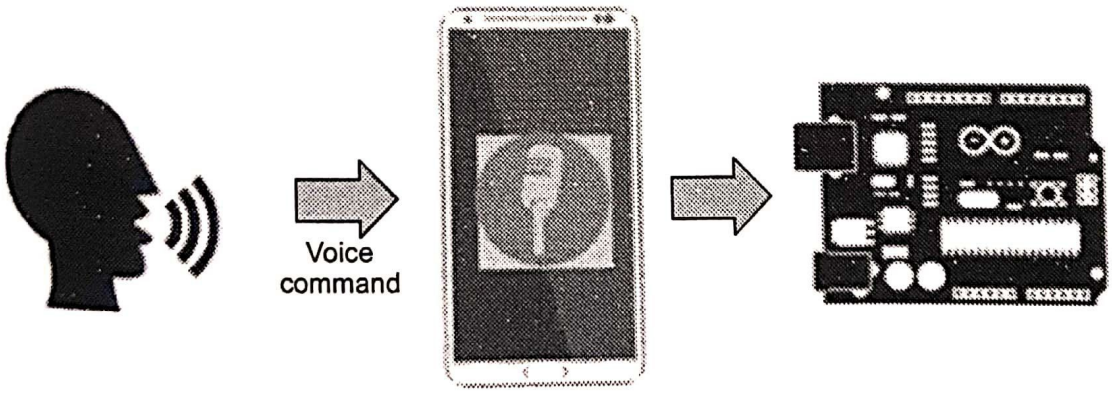


Fig. 5.6.1

- Voice is a feature that does not need to make any consideration for infrastructure, other than the need for an Internet connection.
- Consumer applications for voice include virtual assistants on smartphones as well as devices that do not include integrated telephony functions, such as wearable devices with minimal screen real - estate.

- Devices in this category include smartwatches and fitness wearables that can offer hands - free voice activation of a multitude of functions, through to smart televisions and games consoles.

Alexa Voice Service (AVS) Integration for AWS IoT

- Alexa Voice Service (AVS) Integration for AWS IoT is a new feature that cost - effectively brings Alexa Voice to any connected device without incurring messaging costs.
- AVS for AWS IoT has three components :
  1. A set of reserved MQTT topics to transfer audio messages between Alexa enabled devices and AVS.
  2. A virtual Alexa enabled device in the cloud that shifts tasks related to media retrieval, audio decoding, audio mixing, and state management from the physical device to the virtual device.
  3. A set of APIs that support receiving and sending messages over the reserved topics, interfacing with the device microphone and speaker, and managing device state.

❑❑❑

SOLVED MODEL QUESTION PAPER

(As per New Syllabus)

Internet of Things

Semester - VII(Electrical / IT) Open Elective - III

Semester - VII(ECE) Professional Elective - V

Time : 2 Hours] [Total Marks : 56

Instructions : 1) Attempt any FOUR questions out of EIGTH questions.

2) Make suitable assumptions wherever necessary.

3) Figures to the right indicate full marks.

Q.1 a) *Define IoT. List the characteristics of IoT.* **[Refer sections 1.1.1 and 1.1.2]** **[3]**

b) *Explain IoT communication model.* **[Refer section 1.5.2]** **[4]**

c) *Describe briefly various IoT levels.* **[Refer section 1.7]** **[7]**

Q.2 a) *What is sensor and actuators ?* **[Refer section 2.1]** **[3]**

b) *Explain IoT system building blocks.* **[Refer section 2.3]** **[4]**

c *Explain interfacing of LED and switch with Raspberry Pi.* **[Refer section 2.7.2]** **[7]**

Q.3 a) *List and explain components of BLE.* **[Refer section 3.6.2]** **[3]**

b) *What is difference between CoAP and MQTT ?* **[Refer section 3.7.3]** **[4]**

c) *Explain the following:*
i) DDS *ii) IPv4* **[Refer sections 3.7.8 and 3.4]** **[7]**

Q.4 a) *What are the challenges of IoT security?* **[Refer section 4.6]** **[3]**

b) *Describe IoT security needs and issue.* **[Refer section 4.1]** **[4]**

c) *Explain key management and update management.* **[Refer sections 4.4 and 4.5]** **[7]**

Q.5 a) *What is consumer IoT ?* **[Refer section 5.1]** **[3]**

b) *How IoT is used in intrusion detection system?* **[Refer section 5.2.3]** **[4]**

c) *Discuss IoT application as health care monitoring.* **[Refer section 5.5]** **[7]**

Q.6 **a)** *Explain BLE topology.* **[Refer section 3.6.3]** [3]

b) *Discuss Raspberry Pi interface.* **[Refer section 2.6]** [4]

c) *Explain MAC layer of IEEE 802.15.4.* **[Refer section 3.2.2]** [7]

Q.7 **a)** *What do you mean risk assessment ?* **[Refer section 4.2.1]** [3]

b) *Explain web socket.* **[Refer section 3.7.6]** [4]

c) *What is web of things ? Explain architecture standardization for WoT.* **[Refer section 1.10]** [7]

Q.8 **a)** *What is military things?* **[Refer section 5.1.5]** [3]

b) *Explain HTTP request methods and actions.* **[Refer section 3.7.4.1]** [4]

c) *What is M2M ? Explain architecture and components of M2M.* **[Refer section 1.2]** [7]

❑❑❑