FALL SEMESTER 2021-2022

CSE3009-Internet of Things

Digital Assignment -1

Submitted by: Alokam Nikhitha(19BCE2555)

Submitted to: Dheeba J

1.Describe the real time example in terms of sensors used (its description), networking (connecting technology), and application layer protocols and whether it uses cloud and big data analytics

❖ Health care Monitoring System for Elder people:

The healthcare Internet of things (IoT) based on medical digital devices makes the home health monitoring for the elderly possible. By establishing an IoT-based home care monitoring system, the elderly can know about their health condition and get services provided by the health care center without walking out of home. It would also make the government and the society able to cushion the blow of the aging population.

Network layer In IoT architecture, the network layer is also called as transmission layer. It works by sending the data received from the perception layer to the processing unit securely. IPV6 addressing for LowPAN devices are used in Network layer.

Application layer assures the authenticity, security, privacy and robustness of data which is sent over the communication system. In this case we use CoAP, MQTT

This Monitoring System uses Cloud computing:

Using cloud computing and IoT in this process can significantly improve the monitoring of patients. Therefore, it is important to provide a useful method in the medical industry and computer science to monitor the status of patients using connected sensors. Thus, due to its optimal efficiency, speed, and accuracy of data processing and classification, the use of cloud computing to process the data collected from remote patient sensors and IoT platform has been suggested.

❖ Smart transportation System

Smart Transportation Systems apply a variety of technologies to monitor, evaluate, and manage transportation systems to enhance efficiency and safety. The rapid growth in the population of the urban area has forced the authorities to effectively use the existing infrastructure, in which smart transportation has to play a key role. An overview of a few services offered by a smart transportation system to enhance the safety at roads, provide on-time availability of information to drivers and passengers, reduce traffic congestion, reduce accidents, and so on are discussed here

Network Layer: Applications requiring longer ranges such as smart transportation use protocols, which are in the local area network (LAN) class, such as IEEE 802.11 (WiFi). Intra-vehicular considers the communication inside the vehicle and includes protocols such as Bluetooth, Radio Frequency Identification, Near Field Communication, IEEE 1609 WAVE, WiFi HaLow and ultra-wideband.

Environmental includes all protocols for communication networks used outside of the vehicle which include IEEE 802.15.4, 802.11p, 2G/3G/4G/ LTE, WiMAX and Low-Power Wide Area Network.

Application layer – MQTT, CoAP, XMPP, DDS are used in this layer.

Smart Transportation uses Bigdata Analytics

Vehicles are connected to the Internet and generate large amounts of data. Data analytics can help transport management authorities. Find out the history of road mishaps (e.g., under what circumstances did the accident occur and at what speed were the drivers driving during the mishap) so minimize the number of road accidents and determine the time when the traffic load reaches its peak and also prepare an optimal route plan that can help minimize traffic congestion.

❖ Smart water filtration system

Information collected by sensors Device Status, Water Flow Rate, Water pH, Water Filter Cartridges information Sensors will collect measurements from equipment and record ambient conditions. A data logging or networking device will intercept the stream of data from of the sensors and aggregate them in a central location. A dashboard or other interface will interpret the data and help you prioritize what to act on first.

Network layer In IoT architecture, TCP protocol .It requires more power consumption which makes them not much feasible for WDN. The short range protocols include Zigbee

Application layer may include AMQP,MQTT protocol

- It requires more power
- consumption which makes them not much feasible for WDN.
- The short range protocols include Zigbee, 6lowpan,consumption which makes them not much feasible for WDN.

Smart water filtration system uses big data,

Hand in hand with dynamics is the need to think about different timescales: (daily) variations, weekly trends (especially weekend versus weekday differences), and seasonal shifts. For each of these, the data analytics needs are quite different and need to be carefully considered. For daily variations it can be useful to compare one day to the next by overlaying the dynamic data.
Handling bad measurements/outliers will be handled by big data solutions.

2. In terms of security what are the different security threats to IoT devices. List and explain that. (2)

The security challenge is the most important undertaking in IoT. The application information of IoT will be industrial, enterprise, client or personal. This application information ought to be secured and have to stay personal towards robbery and tampering. For example, the IoT applications might also additionally store the outcomes of a patients health or purchasing shop. The IoT enhance the conversation among gadgets however still, there are troubles associated to the scalability, availability and reaction time. Security is a challenge in which the data is securely transmitted over the internet. While transporting the data throughout global border, safety degree act can be carried out via way of means of authorities law such as Health Insurance Portability and Accountability (HIPA) act. Among exceptional safety demanding situations, the maximum essential demanding situations applicable to IoT are discussed.

- **Data Privacy:** Some producers of smart TVs accumulate information about their clients to research their viewing behavior so the information gathered via way of means of the smart TVs might also additionally have a undertaking for data privateness for the duration of transmission.
- **Data Security:** Data security is likewise a awesome challenge. While transmitting data seamlessly, it's miles essential to cover from observing gadgets at the internet.
- **Insurance Concerns**: The insurance companies installing IoT devices on automobiles accumulate data about health and using status to be able to take decisions about insurance.
- **Lack of Common Standards**: Since there are a lot of requirements for IoT gadgets and IoT production industries. Therefore, it's miles a large undertaking to differentiate among approved and non-approved gadgets linked to the internet.
- **Technical Concerns**: Due to the improved utilization of IoT devices, the visitors generated via way of means of those gadgets is likewise increasing. Hence there may be a want to growth community capacity, therefore, it's also a undertaking to store the big quantity of data for analysis and further storage.
- **Lack of visibility and device control** : Many IoT devices continue to be unmonitored, untracked, and improperly managed. As gadgets join and disconnect from the IoT community, looking to reveal them can turn out to be very difficult. Lack of visibility into tool repute can save you companies from detecting or maybe responding to capacity threats.
- **Botnets** :Botnets are a chain of internet-linked devices which can be created to thieve data, compromise networks, or ship spam. Botnets comprise malware that permits the attacker to get admission to the IoT tool and its connection to infiltrate an organization's community, turning into one of the pinnacle threats for businesses.
- **Weak passcodes:** Although elaborate passcodes can show to be steady for maximum IoT gadgets, one susceptible passcode is all it takes to open the gateway on your organization's community. Inconsistent control of passcodes in the course of the place of work permits hackers to compromise your whole enterprise community.
- **Security Attacks & System Vulnerabilities:** There have been a number of work achieved with inside the situation of IoT security up till now. The associated work may be divided into system security, application security, and network security

a) **System Security:** System security especially focuses on universal IoT system to pick out exceptional security demanding situations, to design different security frameworks and to offer proper security recommendations to be able to preserve the safety of a community.
b) **Application security:** Application Security works for IoT application to deal with safety troubles in keeping with situation requirements.
c) **Network security:** Network security offers with securing the IoT communication network for conversation of distinct IoT devices.

3. Solutions to overcome this security issues (2)

- **Secure the IoT Network** : Protect and secure the community connecting IoT gadgets to the back-give up structures at the net through enforcing conventional endpoint protection capabilities which include antivirus, anti-malware, firewalls, and intrusion prevention and detection structures.

- **Authenticate the IoT Devices :** Allow the customers to authenticate the IoT gadgets through introducing a couple of person control capabilities for a unmarried IoT tool and enforcing strong authentication mechanisms which include two-component authentication, virtual certificates, and biometrics.
- **Use IoT Data Encryption :** To guard the privateness of customers and save you IoT facts breaches, encrypt the facts at relaxation and in-transit among IoT gadgets and back-give up structures through the use of popular cryptographic algorithms and fully-encrypted key lifecycle control tactics to enhance the general protection of person facts and privateness.
- **Use IoT PKI Security Methods :** To make certain a stable connection among an IoT tool & app, use IoT public key infrastructure protection strategies which include X.509 virtual certificate, cryptographic key, and life-cycle talents consisting of public/non-public key generation, distribution, control, and revocation.
- **Use IoT Security Analytics :** Use IoT Security Analytics Solutions which can be succesful to stumble on IoT-particular assaults and intrusions, which can't be recognized through conventional community protection answers like firewalls.
- **Use IoT API Security** : Methods Use IoT API Security strategies now no longer handiest to guard the integrity of the facts motion among IoT gadgets, back-give up structures, and programs the use of documented REST-primarily based totally APIs, however additionally to make certain that handiest legal gadgets, developers, and apps are speaking with APIs or detecting capacity threats and assaults towards specific APIs.
- **Test the IoT Hardware** Place a strong testing framework in location to make sure the safety of IoT hardware. This consists of stringent testing of the IoT tool's range, capacity, and latency.
- **Develop Secured IoT Apps** Given the immaturity of the present day IoT technology, the builders of the IoT applications need to emphasize on the safety issue in their IoT applications via way of means of strictly imposing all of the above-referred to IoT protection technologies
- **Avoid Launching IoT Devices in a** Rush To live beforehand in the competition, the producers of the IoT devices are frequently in a hurry to release their merchandise in the marketplace at the bottom prices. And, at the same time as doing that, they don't pay sufficient interest to offer protection updates and patches. This poses a extreme risk to the safety in their IoT gadgets in the lengthy run.
- **Beware of Latest IoT Security Threats & Breaches**: To make sure the security of the IoT devices and applications, the device makers and app builders need to watch out for the latest IoT security threats and breaches. Since the IoT continues to be an rising technology, its protection breaches are sure to happen.