MANTECH Publications

Journal of Internet of Things and Information Technology
Volume 5, Issue 3, September-December, 2022

Embedded Systems and the Issues of Connected Devices

Dr. B.P. Chouhan[1], Nandini Singh[2], Jyoti Nagare[3]
Professor[1], Students[2, 3]
Department of Computer Science Engineering
Yogananda College of Engineering and Technology (YCET)
Corresponding Author's Email: - *nandani47singh5@gmail.com[2]*

Abstract
As the number of linked IoT devices is likely to skyrocket in the next few years, it is critical that the connected devices in an embedded system interact conveniently and securely. On the other hand, the communication network for these devices must live up to the promises of being secure, complex, free of congestion, and compliant with emerging standards.

Keywords: *- Iot, Embedded System, Bandwidth, Concerns and Considerations*

INTRODUCTION

This article talks about the most important things to think about when deciding which networking technologies to use in your IoT application. These include operating range, available bandwidth, optimal power usage, essential intermittent connectivity, device collective interoperability, and IoT security and privacy considerations.

As an essential component of the future Internet-of-Things (IoT), real vision and consideration of IoT networking cannot be achieved without IoT security. This article provides you with a cognitive grasp and awareness of hidden obstacles and concerns in embedded systems to enable safe communication and smooth operations as sensors, data storage, Internet bandwidth, and analytics get quicker, cheaper, better, and more integrated.

Users will be able to rely on IoT networking considerations to make better selections of linked devices and technology. IoT device networking will have a huge influence on many areas of how we use IoT in our daily lives. [4,5]

The IoT is Emerging and Evolving

The first fact about the Internet of Things is that it evolved from a platform for specialised hobbyists to a worldwide ecosystem of devices and information systems. Since its inception, IoT has evolved into a significant communication infrastructure aimed at providing anywhere, anytime connection to a large number of linked devices in Embedded Systems. As the globe moves toward being a linked global society, technology continues to advance at a rapid pace.

Device Power Consumption Matters

Because power and memory are key limits for every linked component in an embedded system, transporting data and records over long distances requires more energy than transmitting data and records over short distances. You should think about products or equipment that use a battery to save power in order to extend the life of the battery and save operating costs. It is vital for many Internet of Things (IoT) applications to power devices using a battery. When your gadget is not in use, you can put it to sleep. Another important component for energy or power conservation for linked devices in an embedded system is the use of low-power radio technology protocols.

Security is a primary concern with connected devices in embedded systems.

Because all devices in Embedded IoT ecosystems are directly connected to the internet, each device is responsible for its own security, making security a local fundamental concern for every connected thing or device. Monitoring and avoiding security concerns and events should be a top priority for an IoT ecosystem. To avoid tampering, the IoT ecosystem must choose networking technologies that implement end-to-end security, including device authentication (referred to as smart configuration), data encryption (data protected by converting the data to encrypted data), and open port protection.

End-to-end Security Design for Connected Devices in an Embedded System

Connecting your devices to the cloud safely with end-to-end security architecture that protects data wherever it goes throughout its lifecycle. The critical and sensitive data is encrypted using the Advances Encryption Standard (AES).

The IoT ecosystem connects the device to the cloud via various network interfaces. As a result, data flowing along the chain's network element should be secured using network encryption. Wireless Protected

Access-2 (WPA-2) is primarily used to secure wireless networks. The SSL or TLS protocols maintain the privacy of data going across the network while also ensuring the data's integrity.

Collective Interoperability of Devices is Vital

Interoperability is the capacity of devices and system components to interact with one another, independent of manufacturer or technical specifications. This is why interoperability is critical for the proper development of IoT networking.

The quantity and variety of IoT devices will present another issue to deal with, which is device interoperability. How will endpoints, microcontrollers, and software from various software vendors interact with one another? What message patterns and management mechanisms will they employ when they collaborate? There is currently no reasonable response to the question. Similarly, as with each new generation, several suppliers are advertising not only their end devices and software but their whole ecosystem. Fortunately, there are frequently open source alternatives to commercial IoT solutions and arrangements that are completely independent of operating systems.

Interoperability is the ability of structures or structural additives to interact with one another, independent of manufacturer or technical specifications. This is why interoperability is critical for the proper development of an IoT middleware framework to support message protocols and structures. [2]

Device Level Interoperability

The IoT sector will benefit from some standardisation in the future, but until then, you'll need a mobility management infrastructure.

Need of Uninterrupted Services with Intermittent Connectivity

When your linked device or item loses connection to the cloud at random intervals, this is referred to as "intermittent connectivity. Cloud services will struggle to provide continuous services to devices and systems with intermittent network access to the cloud, such as linked automobiles and drones. In the IoT, device connectivity occurs at random due to the physical location of the edge or connected device, such as a mobile phone, or because the connected device is battery powered or connects at predetermined periods to save power or bandwidth. However, an unstable network may cause devices to lose connectivity or suffer from a high rate of delay. [1]

Because of connection issues, there are several challenging circumstances that occur with the advent of the Internet of Things in terms of aggregating data into a central data repository. In such a case, we would rely on an IoT ecosystem with connectivity-aware or connectivity-based protocols to assure uninterrupted service and more stable connectivity.

Upstream Bandwidth at a Premium

In IoT, data must go via a substantial quantity of upstream traffic from device to cloud. Upstream refers to the direction in which data can be sent from the client to the server in IoT networking (upstream traffic). This is significantly different from the downstream bandwidth at which the data may be received. A typical broadband internet connection has greater downstream capacity than upstream bandwidth; often, upstream bandwidth is expensive.

IoT devices, in particular, generate large amounts of data at network edges, and the number of devices deployed in an IoT network can quickly overload upstream capacity.

The overheads in networking and messaging protocol packets are significant, as the real data being transferred is padded with empty data. As a result, the data size should be considered in relation to the pocket size of the networking protocol. Reduced data volume (less frequent sampling) and data aggregation should be implemented to meet peak bandwidth requirements.

A well-fitting range is always anticipated. The range is the next factor to examine. The IP (Internet Protocol) stack is typically used to connect IoT devices or items to the Internet. As a result, your network should be configured to receive data from IoT devices and transfer it to the appropriate location. The range of an IoT network may be defined as the distances that data travels in a typical IoT network.

The Internet of Things divides linked devices into two categories: short-range and wide-area range. The short range category includes devices connected by short range wireless technology that operates in the centimetre and metre range, such as RFID, NFC, Bluetooth, Wi-Fi, and ZigBee.

While the wide area ring section covers extensive distances measured in kilometres, it also includes devices that use cellular connections (CDMA) as well as unlicensed low power radio technologies such as LoRa, Sigfox, and 6LoWPAN. As a result, selecting a network protocol that is compatible with a wide range of applications is critical.

If the transmission of a large amount of data across a specified range causes a difficulty, edge computing can alleviate the problem by processing the data close to the source (device or local server) rather than gathering and centralised at a data centre. Edge computing enables analysed data from each device or source to leave the edge network. Because most IoT devices are powered by tiny batteries, it is vital to strike a balance between performance and power consumption. [3]

CONCLUSION

The linked world of embedded systems provides a plethora of new avenues for expert businesses seeking to conquer the globe through technology and data. Those that intend to profit from this wave while avoiding unnecessary hurdles and ensuring data security require a security arrangement that provides regular monitoring of security concerns, possible threats, and network weaknesses. As a result, the IoT architecture and ecosystem should be developed with this in mind, by looking after and coordinating the fundamental IoT areas both on a device and vertical level to provide for security and provisioning (device identification) throughout the product life cycle.

REFERENCES

1. https://www.sikich.com/insight/iot-security-considerations-internet-of-things-security/
2. William Stallings. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. 1st Edition, Kindle Edition.
3. https://en.wikipedia.org/wiki/Internet_ of_things
4. https://tools.cisco.com/security/center/ resources/secure_iot_proposed_frame work
5. https://www.embedded-computing.com/embedded-computing-design/10-internet-of-things-design-considerations