Ministry of Electronics & Information Technology Government of India

सत्यमेव जयते

DSCI PROMOTING DATA PROTECTION A NASSCOM® Initiative

National Centre of Excellence Cybersecurity Technology And Entrepreneurship

CYBERSECURITY CENTRE of EXCELLENCE A joint initiative of DSCI & Government of Telangana

IoT SECURITY GUIDE

AUGUST 2022

Table of Contents

CONTENTS

Table of Contents

CONTENTS

Table of Contents

CONTENTS

EXECUTIVE SUMMARY

The Internet of Things (IoT), which will soon expand to the Internet of Everything, is a historical shift in the way we interact with our surroundings, our workplaces, and society. Our ability to converge the digital and physical worlds through IoT holds tremendous potential for the digital economy.

With the advent of 5G technologies, IoT technologies are set to take a giant leap forward. 5G can support a large number of static and mobile IoT devices, which have unique bandwidth, speed, and quality of service requirements. With these capabilities, we will see an explosion in IoT usage and innovation. In fact, as per an IDC report, IoT is expected to consist of more than 55 billion connected devices generating 80 Zettabytes of data by 2025. However, in addition to new opportunities, the IoT era also introduces new attack surfaces, which are already being exploited by cybercriminals.

While IoT promises to bring efficient business results across several industry verticals, organisations just focusing on connectivity to win the digital transformation race and putting security in the backseat would place the entire ecosystem at risk of fraud and attack.

In this context, we aim to present a wide spectrum of technological perspectives on IoT Security through our **IoT Security Guidebook**. This guidebook is a comprehensive document that covers IoT communication protocols as well as advice for building architectures for designing and developing IoT applications. Furthermore, the document highlights existing security architectures used across various industries. Threat modelling for IoT will assist developers in risk prioritization and lay the groundwork for establishing a product protection plan.

The purpose of the IoT Security Guidebook is to help the budding Internet of Things industry develop a unified knowledge of security challenges. The IoT Security Guidebook advocates for a methodology for designing secure IoT Services that ensures security best practices are followed throughout the service's life cycle. The documents offer recommendations on strategies to deal with common security threats and flaws in IoT services. It is intended to give a set of design recommendations for developing a secure product for IoT service providers. This document will operate as an overarching model for evaluating which features of advanced technologies or services are significant to the developer. Once these elements, or components, have been identified, the developer can assess the risks associated with each one and decide how to mitigate them.

Its scope is identified as design and deployment-specific recommendations for IoT services. It should be noted that national rules and regulations for a given territory may take precedence over the guidelines outlined in this document in some circumstances.

Key Takeaways

IoT is the network of inter-connected devices that can process data and communicate with each other, without the need for human intervention. IoT-based technology will deliver an advanced level of services in the coming years, effectively changing how people live their lives. Mobile computing, Pervasive Computing, Wireless Sensor Networks, and Cyber-Physical Systems are just a few of the categories where IoT is well-established. A few of the opportunities include new business models, diversification of revenue systems, real-time information and global visibility. The elements that shape the IoT ecosystems are Intelligent decision-making, communications, embedded systems, sensors and actuators. Advancements in Wearables, Smart Homes, Smart Cities, Smart Grids, Industrial, connected cars, Smart Retail, Smart Supply Chain, Smart Farming and Connected Health are a very few of the categorical examples of IoT use cases. This document outlines some of the prominent standard IoT network communication protocols such as Wi-Fi (Wireless Fidelity), Bluetooth, Zigbee, and 6LoWPAN (IPv6 over Low-power wireless personal area networks) and LoRaWAN (Long Range Wide-area network).

A significant proportion of IoT solutions designed for a specific application are dispersed and heterogeneous, making standardisation difficult. Security is one of the most important considerations for IoT, and it must be recognised alongside the overarching need for safety, as the entire world is closely intertwined with both concerns. The IoT Application Architecture gives detailed outline models and strategies for both design and development of an application. It also offers the readers a blueprint and recommendations to develop an application in a well-structured manner. The lack of technical standardisation in the IoT ecosystem exposes hardware, software, and relevant data to attacks and threats. It is therefore essential to dedicate more time to formulating industry guidelines and architectural standards required to efficiently implement IoT. Regulation of IoT products will be beneficial to improving the scalability, interoperability, security, and reliability of these products, especially given the complicated nature and uncertainty of the IoT ecosystem.

The document also underlines the Security concerns of IoT, since almost all IoT devices can threaten personal Confidentiality and public safety through cyberattacks. A few standard problems while tackling the security concerns include limited device resources, fragmentation of Standards and regulations, Security Integration and Data Privacy. The broad range of security concerns needed in IoT to enable design security, data protection, risk analysis and other concerns are outlined. The best practices to tackle these are by establishing secure IoT lifecycle guidelines on software and hardware development, Implementing role separation in Application Architecture and Supporting the establishment of IoT security strategies and Regulations.

The document also highlights the solutions among different Industries such as Huawei's IoT solution security architecture (the 3T + 1M framework), LTTS IoT Security Framework and Zero trust Architecture. The document presents the key components of LTTS IoT Security Framework and oneM2M standards and the benefits of using oneM2M.

The document presents several IoT Application architectures in focus such as,

- The Healthcare industry uses a bounded network with high integrity zone, a boundaryless network and a hybrid with different network technologies.
- Smart Home Ecosystem that uses Hub Architecture also addresses the security concerns of hub including device and software security.
- Industrial control systems are a broad category that includes DCS, SCADA as well as other PLCs used in Industries and essential infrastructures.

The document also highlights the solutions among different Industries such as Huawei's IoT solution security architecture (the 3T + 1M framework), LTTS IoT Security Framework and Zero trust Architecture. The document presents the key components of LTTS IoT Security Framework and oneM2M standards and the benefits of using oneM2M.

- Distributed Denial of Service (DDoS), provides types of attacks at different levels such as device level, network level and Application level.
- Hardware Security provides types of attacks on hardware such as side-channel Attacks, Rowhammer attacks, Hardware Trojan attacks, Physical attacks, Reverse engineering, Hardware IP Piracy, Mod-chip attacks and Security Architecture Attacks.

Hardware security issues arise when the vulnerabilities at different levels are not patched due to the lack of robust security for software and system. The document comprehensively outlines the Embedded system Hardware and Security, and the properties of securing an embedded system. A very minor vulnerability is required to create an exploit, to attack an embedded system. To achieve security, a list of properties of highly secured embedded systems is specified in the document.

The document gives a comprehensive understanding of the Data-at-rest Protection, which secures the data from unauthorized access.

The document states about the data layers that include,

- The hardware layer, the whole medium used for storage is encrypted by using FDE. It encrypts all the information including the hidden files.
- Block Manager Layer, the encryption is carried out at a higher level, the device-management layer, typically a block-oriented driver.
- The file system layer provides well-gross control over the selection of information that requires storage privacy.
- The application layer can add their data protection by using underlying file-system encryption features.

Information concerning secure boot and methods, Hardware resource partitioning, Software containerization and Isolation, Attack surface Reduction, least Privilege and Mandatory Access Control, Implicit Distrust and Secure Communication, Data Input Validation, Secure software development, build options and OS configurations, Integrity Monitoring and Auditing have been addressed.

A few of the Attacks involving Privacy violation and Data leakage Attacks in each of the layers is specified. Weak authentication Attacks, firmware Hijacking, Device scan Attacks, MITM attacks, Identity spoofing attacks, Malware injection attacks, SQL injection attacks, and Cross-site Scripting are just a few of the attacks associated with embedded system security and appropriate measures to prevent the attacks are presented.

The document exemplifies SCADA (Supervisory control and data acquisition) as they are a set of computing devices both software and hardware that work together to control a system. The main components of SCADA involve Supervisory computers, Remote terminal units, PLCs and Human-machine interfaces (HMI). Since SCADA networks are widely used in today's businesses to monitor and study real-time data, control industrial operations and connect with devices. As these systems are critical for industrial organizations, the need for SCADA security is essential.

Cyberthreats to SCADA and IoT Systems need to be comprehended, as these systems are usually used to manage Industrial Control Systems. Suggestions proposed by the President's critical infrastructure protection board in the United States to increase SCADA cyber security in protecting Industrial control systems have been stated. While securing the SCADA systems, the challenges to secure SCADA systems in IoT-Cloud Environments have been acknowledged. Advanced Persistent threats, Data Integrity, MITM, Replay Attacks and Dos Attacks are just a few of the threats to SCADA systems in the IoT-cloud context. The Best practices for securing IoT-Cloud-based SCADA systems are Network Segregation, Monitoring and Analysis, Log Analysis, File integrity monitoring, network traffic analysis, Memory dump analysis, Actively evaluating of security vulnerabilities, and Constant updating and fixing.

The threat model for IoT involves a Risk evaluation methodology which measures the relative importance of risk and helps organizations work on it. There are several forms of threat modelling and also how to carry out threat modelling by determining the trust boundaries, who the stakeholders are, the vital assets that must be safeguarded, attack surfaces, possible future risks and threats that have been detected are subjected to a risk assessment. Data-centric Threat modelling explains the combination of attack and protection side details for data of interest in a structured model that aids in vulnerability analysis, decision making, and change management in steps.

The document illustrates the importance of IoT Threat modelling with an Architectural IoT Threat Modelling Example which describes basic threats architecturally-based IoT hazard modelling. Threat modelling for Device-Level security describes different threat modelling methods, and their features and also gives an in-depth knowledge of each model with its frameworks. There are different types of threat models which target different IoT Networks which have different threats and risks which can cause different rates of damage. The document guides on identifying threats and providing security with risk mitigation by conducting assessments. There are millions of devices connected to the internet across the globe and there are several vulnerabilities they carry which could compromise users' data.

There is a lot of research and development ensuing in IoT Security in several areas. The key areas, their importance, technologies and challenges are described in this document. There are two different security standards covered in this document which are IIoT and IoXT. IIoT is used in manufacturing, supply chain monitoring, and management. IoXT has some rules and this document explains each of them in detail. There are IoT security standard protocols each protocol covers a different area but shares a common base of making IoT better on a daily basis. This document explains the importance of these protocols and how they support organizations by explaining their working models and functionalities.

The advent of 5G will connect all the citizens virtually through machines, objects, and devices. This document explains different technologies used in 5G, deployment and how they changed the phase of connectivity in IoT along with the security recommendations for 5G which explains vulnerabilities and attacks that can cause data thefts and also how can one avoid these by following different strategies, and security solutions to make a better 5G environment.

1.1 Evolution of IoT

The Internet of Things (IoT) is a conceptual paradigm that has emerged over the last few years. Kevin Ashton introduced the concept of IoT back in 1991. It describes a wide ecosystem where interconnected devices and services collect, exchange, and process data to adapt dynamically to a context.

Internet of Things (IoT): a wired or wireless network of uniquely identifiable connected devices that can process data and communicate with each other with or without human involvement.

IoT encompasses several fields of study, including Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and Cyber-Physical Systems (CPS). IoT represents a growing and changing field with many definitions.

The Internet of Things is tightly bound to cyber-physical systems and, in this respect, is an enabler of Smart Infrastructures by enhancing their quality-of-service provisioning. The IoT is the natural evolution of computing, and it brings its own challenges – an immature ecosystem plagued by fragmentation of standards and security concerns in a currently non-homogeneous IoT market because each industry and application are different. Another IoT challenge worth highlighting is its ability to scale globally. According to the IoT Analytics "State of IoT - Summer 2021" report, the global number of connected IoT devices is expected to grow 9% to 12.3 billion active endpoints and by 2025 the total number of IoT connections is predicted to reach 27 billion. Currently, there are different solutions available in the market through various manufacturers such as Google, Microsoft, Amazon, Apple, and Samsung, among others, many of which use their proprietary cloud service, protocols, and operating system.

The threats and risks related to the Internet of Things devices, systems and services are manifold and evolve rapidly. With a great impact on citizens' safety, security and privacy, the threat landscape concerning the Internet of Things is extremely wide. Hence, it is important to understand what needs to be secured and to develop specific security measures to protect the Internet of Things from cyber threats. Involving billions of intelligent systems and millions of applications, IoT will drive new consumer and business behaviours, which will demand increasingly intelligent solutions.

As per Fortune Business Insights, the projected growth of the global IoT market by 2028 is $1,854.76 billion creating several opportunities for vendors and companies looking to capitalize on IoT.

Examples of these opportunities include:

- New business models: New value streams for customers, with a faster response.
- Diversification of revenue streams: Monetizing added services on top of traditional lines of business.
- Real-time information: Capturing data about products and processes more swiftly, improving market agility and allowing prompt decision making.
- Global visibility: Making tracking easier from one end of a supply chain to the other.

Elements of IoT

The following points provide an overview of the different elements that shape IoT ecosystems, namely the Things in the IoT, intelligent decision making, sensors and actuators, communications, and embedded systems.

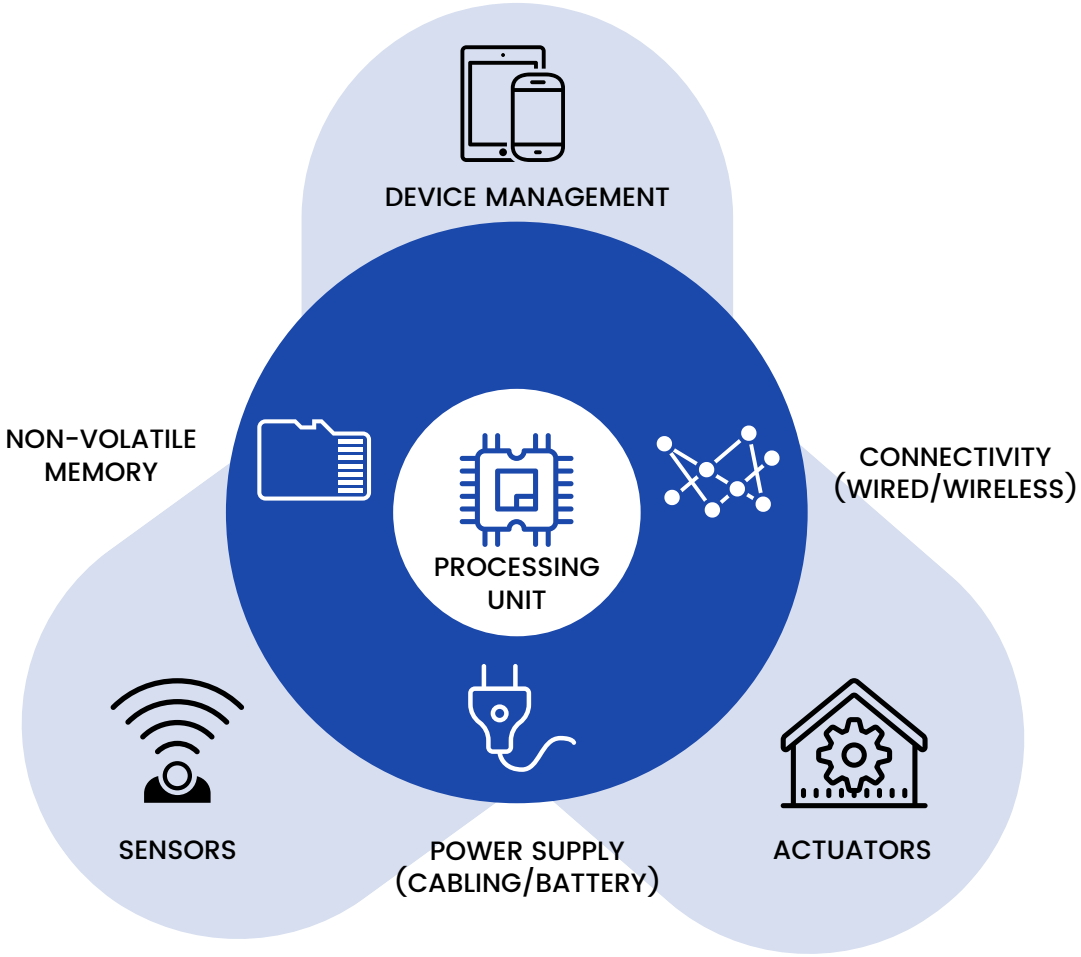


Figure 1. Structure of an IoT Embedded System

Examples of these opportunities include:

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLW, Wi-Fi, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Table 1. Indicative listing of Communication Protocols for IoT

1.2 Examples of IoT Applications

In this subsection, some examples of IoT applications shall be briefly presented.

Wearables

Wearable technology, sometimes referred to as "wearables," is a class of electronic devices that may be worn as accessories, attached to clothes, implanted in one's body, or even tattooed on the skin. The gadgets are hands-free devices with practical applications that are powered by microprocessors and can send and receive data via the Internet.
Wearable technology is considered an important section of IoT. Wearable devices are more prominent in the Healthcare sector. One example is the Fitbit. It helps us in maintaining a healthy lifestyle. It is a tracking device that helps track your sleep cycle, calories burned and tells us how much distance you travelled. Fitbit app also helps in viewing your key metrics such as oxygen saturation, skin temperature variation, Heart rate variability, resting heart rate, and breathing rate.

Smart Home

A smart home is a home with computer gadgets that allow for remote administration of appliances and systems like heating and air conditioning.
Due to IoT Home automation, home security measures have also evolved. Consumers may use their phones to watch CCTV security footage and operate their security systems from everywhere on the planet.

Smart Cities

Smart cities use IoT devices such as connected sensors, meters, systems, etc. to collect and analyze data. The cities then use this data to improve public utilities and services, infrastructure, and more.

IoT enabled smart cities' use cases spans across various areas like Smart Infrastructure, Air Quality Management, Traffic Management, Smart Parking, Smart Waste Management, Public Safety, etc.

Smart Grid

A smart grid is an electrical platform that allows for a two-way flow of electricity and data, as well as the ability to detect and respond to changes in usage and other concerns, thanks to digital communications technology. Smart grids are self-healing and allow power users to have an active role in the system.
IoT can be utilized in smart meters of the grids in order to measure various metrics like power consumption, network interoperability, etc., and also can help manage energy performance and power consumption.

Industrial

The usage of connected systems in industrial applications like automation, monitoring systems, and maintenance departments is termed as the Industrial IoT.

Connected Car

A connected car is a car that has an internet connection(owned), typically through a WLAN, which enables it to share the particular internet service and also the data associated with it, with other devices not only within the car but also outside the car.

Connected cars are linked to the network for enabling bi-directional communication among vehicles regulating the vehicle operations for enabling quick data transmission.

Smart Retail

Smart retail is a collection of smart technologies that are intended to provide consumers with a better, faster, and safer shopping experience. This revolution in retail has been facilitated by a society in which virtually everyone now carries a smart device – i.e., the smartphone.
Nowadays, consumers shop on their mobile devices and prefer products and services which offer discounts, faster delivery and a great shopping experience. Early adaptation of smart technologies by retailers can help them provide a seamless customer experience and ensure brand loyalty.

It is also possible to forecast **when** and **what** a client needs based on their purchase history, providing greater scope for targeted marketing.
IoT devices such as sensors are also being installed in teddy bears in hospitals to monitor the health of sick kids in a subtle and non-threatening manner.

Smart Supply Chain

Smart Supply Chain seeks to raise awareness for better decision-making by leveraging data from IoT devices and offering a detailed view of commodities and services from producer to store.
Clients may use Smart Supply Chain to automate not just shipping and delivery, but also to accurately anticipate product status in real-time and monitor key details that drive supply network productivity.

Smart Farming

Smart farming is a management concept that focuses on providing the foundation for the agricultural business to employ modern technology – such as big data, Internet of Things (IoT), etc. It is used to track, monitor, automate, and analyze activities. Smart farming, often known as precision agriculture, is controlled by software and monitored by sensors.
Smart farming is becoming more important as the world's population grows, as does the need for greater agricultural yields, the need to conserve natural resources and the growing need for climate-smart agriculture.
An example of a smart farming application includes temperature sensors which are used to scan the soil and control water, light, and humidity.

Connected Health

Connected health is an interactive-technical paradigm for managing and delivering healthcare that relies on technology to offer services offsite.
The Internet of Things (IoT) is a network of physical objects that employs connection to allow data to be exchanged. These gadgets aren't always the most advanced technological breakthroughs. They help healthcare professionals perform jobs more quickly by streamlining processes.

1.3 IoT Link Layer Connectivity

Several communication protocols are used in IoT to provide service to the network layer. The following are some of the prominent Standard IoT communication protocols.

Wi-Fi (Wireless Fidelity)

Wi-Fi is a local area network which is a wireless network proposed by Wi-Fi Alliance. Wi-Fi provides internet access to devices within a range of up to 100m. It uses high-frequency radio signals for sending and receiving data. It uses the IEEE 802.11 standard. The frequency and range of Wi-Fi are summarized in Table 3.
Wi-Fi data rate varies from 2Mbps (for Legacy 802.11) to 1.73Gbps (for 802.11ac wave 2). The quite common 802.11n has data speed up to 450 Mbps. We can set up PAN (Personal Area Network) or LAN (Local Area Network), or WAN (Wide Area Network) in IoT systems. By routing, we can increase the network area.

WI-FI PROTOCOL & SECURITY	802.11a/b/g/n/af
FREQUENCY	2.4 GHz, 3.6 GHz, and 4.9/5.0 GHz bands
RANGE	Common range is up to 100m but can be extended
EXAMPLES	Routers, Tablets, etc.

Table 3. Table Listing Frequency and Range of Wi-Fi

The data link layer within 802.11 consists of two sublayers: Logical Link Control (LLC) and Media Access Control (MAC). 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLANs.

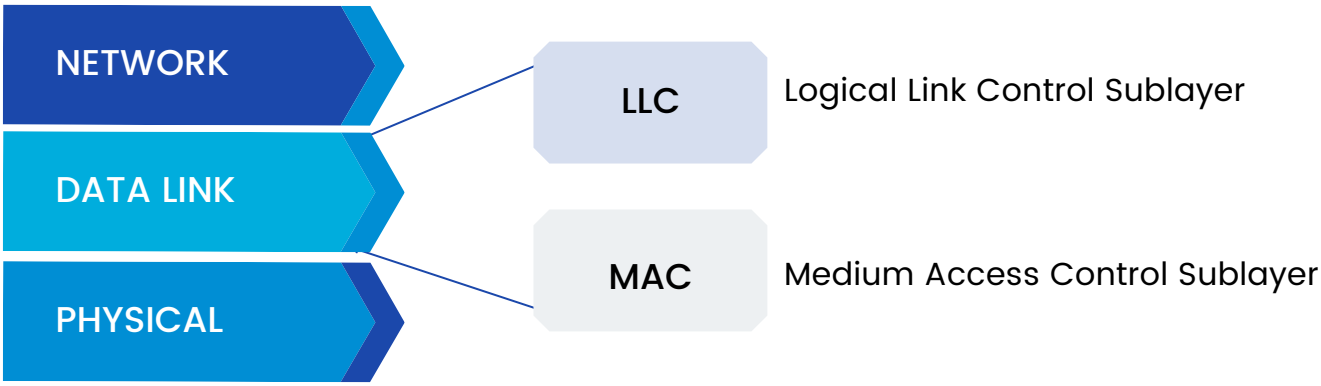


Figure 2. Data Link Layer

The 802.11 MAC is very similar in concept to 802.3 in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it. For 802.3 Ethernet LANs, the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol regulates how Ethernet stations establish access to the wire and how they detect and handle collisions that occur when two or more devices try to simultaneously communicate over the LAN.

The major drawbacks of Wi-Fi networking are latency and poor security. It is easier to hack a Wi-Fi hotspot and gain access to a physical link medium. However, a Wi-Fi network can be secured using WPA types and beacon packets management.

IEEE 802.11 provides for security via two methods: **Authentication** and **Encryption**. Authentication is the means by which one station is verified to have the authorization to communicate with the second station in a given coverage area. In the infrastructure mode, authentication is established between an Access Point (AP) and each station.

802.11 provides two methods of authentication: Open System or Shared Key. These methods are illustrated in Figure 3 and Figure 4. An Open System allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key authentication, on the other hand, requires Wired Equivalent Privacy (WEP) to be enabled and identical WEP keys on the client and AP (for more information on WEP keys, see below). The initiating endpoint requests a shared key authentication, which returns unencrypted challenge text (128 bytes of randomly generated text) from the other endpoint. The initiator encrypts the text and returns the data.

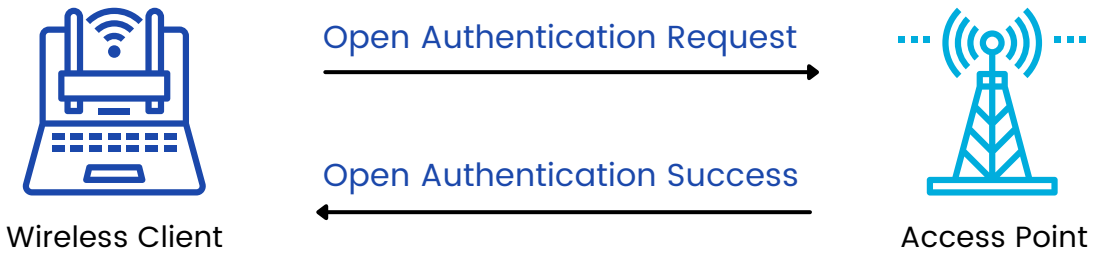


Figure 3. Open Authentication

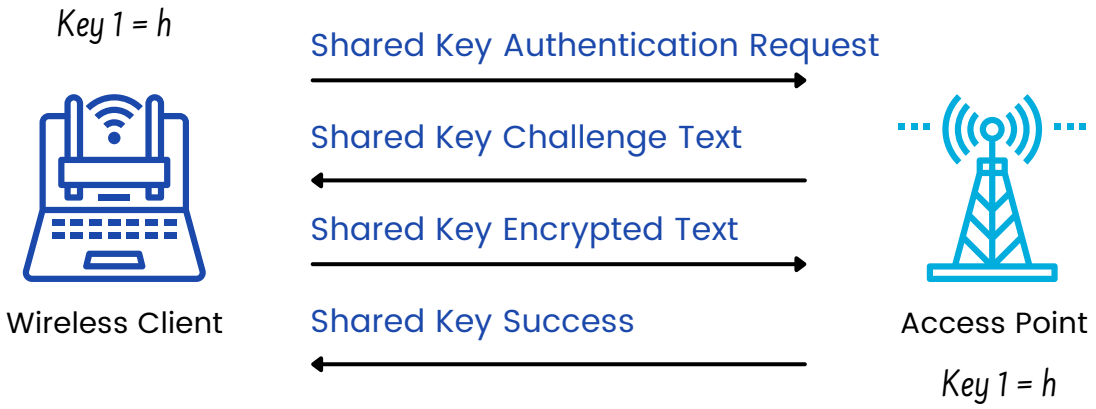


Figure 4. Shared Key Authentication

Encryption is intended to provide a level of security comparable to that of a wired LAN. The Wired Equivalent Privacy (WEP) feature uses the RC4 PRNG algorithm from RSA Data Security Inc. According to the protocol, WEP generally uses a 64-bit RC4 stream cypher (see information on 128-bit below). RC4 is a symmetric encryption algorithm, meaning the same key is used to encrypt and decrypt the data payload. This encryption key is generated from a seed value created by combining a 40-bit user-defined WEP key with a 24-bit Initialization Vector (IV). The WEP key generally takes the form of a 10-character hexadecimal string (0-9, A-F) or a 5-character ASCII string, which must be present on both ends of the wireless transmission. The protocol allows for up to four concurrently defined WEP keys.

The standard does not, however, currently define how the IV is established, so the implementation varies by vendor. When an encrypted wireless client starts transmitting data, the IV can start with a value of zero or another randomly defined starting value and generally increments upwards in a predictable manner with each successive frame. However, some vendors (such as Cisco) use a more sophisticated, random determination of the IV.

Although not yet part of the protocol specification, many 802.11b vendors also support 128-bit RC4 encryption. This requires a 104-bit WEP key (26-character hexadecimal or 13 characters ASCII) but uses the same 24-bit IV value.

Bluetooth

Bluetooth is a PAN (Personal Area Network), or it is a short-range wireless communication network for exchanging data between the connected devices through that network. It is economical in price and effective from a performance point of view for short-range distance. It is a 2.4GHz network that works well for personal wireless network communication. It provides a data transfer rate of 3Mbps in a range of 50m to 150m. Nowadays, Bluetooth is almost present in all smartphones, and it is highly used in wearable devices connected with mobile applications.

The Bluetooth Link Layer outlines the way Bluetooth devices can use the raw transmission facility given by the radio layer to exchange information. The link-layer characteristics of Bluetooth are summarized in Table 4.

MULTIPLE ACCESS SCHEME	TDMA
MAXIMUM PACKET SIZE	358 Bytes
ERROR CONTROL METHOD	ARQ, FEC
CHECKSUM LENGTH	1 Byte or 2 Bytes
IDENTIFIERS	14-bit public device

Table 4. Link Layer characteristics of Bluetooth

The functions of the Link Layer are very close to the MAC (Medium Access Control) sublayer of the OSI model. Functions of the Bluetooth Link Layer include:

- Defining procedures for discovering Bluetooth devices.
- Establishing logical links between the Bluetooth devices that are communicating. One of the devices is assigned as master, and the other is the slave.
- Broadcasting data to be sent. Managing the links between the devices throughout data communications.
- Sending data by converting the raw bit streams of the radio layer into frames and defining key formats.
- Considering the challenges of wireless transmission like interference, noise, and deep fades.

There are two main protocols in the link layer, namely, Link Manager Protocol (LMP) and Logical Link Control and Adaptation Protocol (L2CAP).

Link Manager Protocol (LMP)

LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.

Logical Link Control and Adaptation Protocol (L2CAP)

L2CAP provides adaption between the upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.

Zigbee

Zigbee is similar to Bluetooth technology with a 2.4Ghz frequency. It is a low power personal communication network. It is cheaper and is widely used for several applications. It is used for specific commercial and industrial applications. Its range varies from 10-100m. The link layer characteristics of Zigbee are summarized in Table 5. Mesh networking is one of the important advantages of Zigbee technology. Zigbee supports star or mesh network topology.

MULTIPLE ACCESS SCHEME	CSMA-CA, slotted CSMA-CA
MAXIMUM PACKET SIZE	133 Bytes
PROTOCOL EFFICIENCY (RATIO OF PAYLOAD TO TOTAL PACKET LENGTH)	102/133 = 0.76 (76 Percent Efficient)
ERROR CONTROL METHOD	ARQ, FEC
CRC LENGTH	2 Bytes
LATENCY	<16ms (beacon-centric network)
IDENTIFIERS	16-bit short address | 64-bit extended address

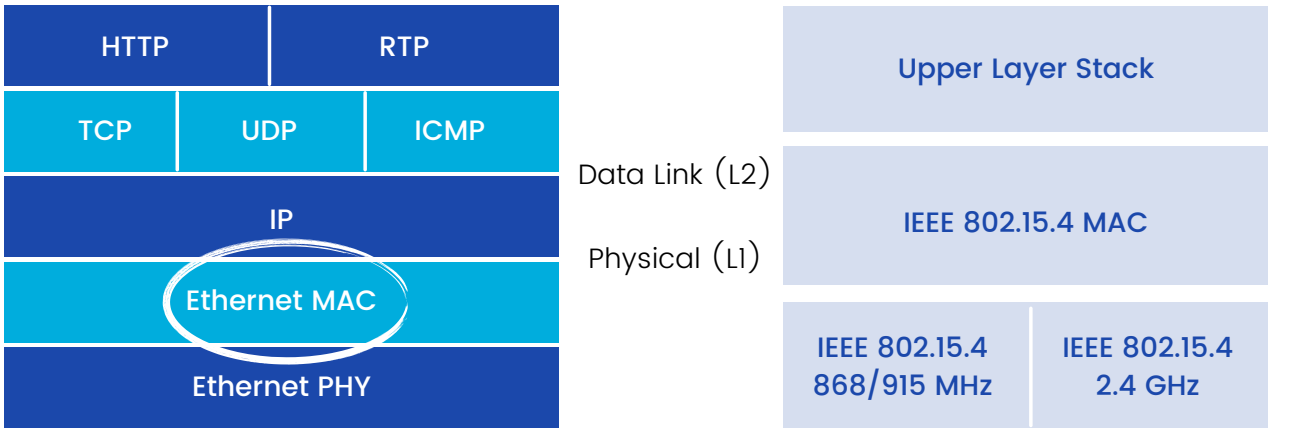
Table 5. Link Layer characteristics of Zigbee

6LoWPAN

6LoWPAN is an acronym for IPv6 over Low-Power Wireless Personal Area Networks (LPWAN). LPWAN is a wireless wide area network technology whose range varies from 2 km to 1000 km depending on the technology. The 6LoWPAN system is used for a variety of applications, including wireless sensor networks. This form of wireless sensor network sends data as packets and uses IPv6, providing the basis for the name, 6LoWPAN.

6LoWPAN has different features like support for 64 bit or 16-bit addressing, targeted at low power networks including Bluetooth low energy, header compression for IPv base as well as for UDP headers, network auto-configuration and neighbour discovery, support for multicast, unicast, and broadcast, supporting the concept of fragmentation. This makes 6LoWPAN the best-suited protocol for IoT.

Many low-power radio protocols are expected to use very small frame sizes. So, the frame size is dependent on the amount of payload or the data that need to carry and the amount of signalling data that is required to carry the packets. Figure 5 shows an example of a 15.4 standard frame where the payload, the actual user data, consists of 53 bytes whereas the total number of bytes to carry this packet is 127 bytes. One should realize that the addition of a header creates a fairly large amount of overhead.



(a) Link Layers and IP

(b) Link Layer: IEEE 802.15.4 for wireless

Figure 5. Link Layer of 6LoWPAN

LoRaWAN

LoRaWAN (Long Range Wide Area Network) is a wide area network protocol. It is a low power consumption protocol that targets wide-area network (WAN) applications with better security and mobility. It supports a large network with millions and millions of low-power devices deployed on public networks. It is a Media Access Control (Data Link or Network Access) protocol with some functions of the network layer also implemented. It is developed by LoRa Alliance. In this protocol stack, multiple end nodes (IoT devices) are connected to a gateway in Star Topology for M2M communication.

This protocol stack has been developed to cater to battery-powered IoT devices that need to connect wirelessly with a base station frequently. It is similar to Sigfox and Weightless technologies. The transceivers in this network typically have a coverage area of about 2 to 5 km in urban areas and 10 to 15 km in deep indoors. The IoT devices can communicate with a gateway at data speeds ranging from a few hundred bits per second to 50 Kbps.