Internet of Things (IoT) Guidelines

April 2022

Issuance and Distribution:

Issuing Authority	Email	Issuance Date
General Directorate of Policies and Governance Ministry of Transport, Communications and Information Technology	Governance@mtcit.gov.om	2022

Document Record

Version	Date	Issuing Authority	Notes
0.1	2022	Ministry of Transport, Communications and Information Technology	

Publication List	
1.	All units of the Administrative Apparatus of the State
2.	The Ministry's Website

Table of Contents

1. Introduction ……4
2. Definitions and Terms ……...4
3. Objectives……..……..…..5
4. Purpose ……...……...5
5. Scope ……...……..…5
6. Internet of Things Guidelines …… 5
6.1 Internet of Things Reference Model ……..……..……..…5
6.2 Internet of Things Ecosystem (IoT Ecosystem) ……..……..…9
6.3 Internet of Things Security Framework ……..……11
6.4 Obligations and Rights ……..……..12
7. Management ……..……..……13
8. Relevant Publications……..……..……13

1. Introduction

The Internet of Things (IoT) consists of billions of things (devices) connected to each other across the Internet Protocol such as sensors, Artificial Intelligence tools, and other units that use wireless technology to connect to the Internet and which has made a sweeping transformation in the way of our work and ways of connection, communication and using products and services.

However, the deployment and use of unprotected IoT devices everywhere may increasingly expose them to cyber-attacks and cyber crimes which may threaten data security or expose the privacy of their owners to danger. IoT security is considered complicated because it includes a wide variety of tasks, such as including data that is necessary for encryption during the processes of manufacturing devices, the provision of new encryption data during operation, developing control policies for access to services and networks, securing the processes of software development, the deployment of device security units, and managing the program development processes.

Therefore, the Ministry considered adopting a unified Reference Model for the target audiences in the Sultanate in order to design, plan and implement the solutions of IoT since these audiences can use this Guideline to develop the policy /framework of their IoT security. Furthermore, the IoT service providers can evaluate security weaknesses by examining the security features (or lack of them) of their IoT solutions in each layer of the IoT Reference Model to counter security threats that face the IoT.

2. Definitions and Terms

Ministry: Ministry of Transport, Communications and Information Technology

Authority: Telecommunications Regulatory Authority

Service Provider: The natural or juridical person who obtains a license to provide IoT services.

Internet of Things: A group of addressable devices in the Internet Protocol that interact with the physical environment and usually contain elements for sensing, communication, processing, and operation.

IoT System: All things, devices, equipment, software, and applications including monitoring and control devices, devices and means of data processing and storage, transceivers, and any auxiliary equipment.

Thing "Things": It is a device from the physical world (physical objects) or an application about the information world (virtual things) characterized by the capability of being integrated into telecommunications networks and usually contains software, the capability of connecting to telecommunications networks and Information Technology, the capability of collecting and transferring data via telecommunications networks through technologies included in it that help activate its internal systems and communicate with the external environment.

Customer: refers to the user of IoT applications provided by the Service provider.

IoT Identifiers: They are a group of numbers or symbols used to identify things to facilitate access to them, IoT Identifiers are used to identify the endpoints (source and final destination).

IoT Reference Model Framework: A wide design of a system or solution of IoT Ecosystem that works as reference Guidelines to enable entities to use a common language and a multi-layer structure to discuss the aspects related to the system such as security and privacy.

3. Objectives

1. Support innovation and encourage moving from traditional technological solutions to IoT-based models.
2. Provide a clear framework to develop IoT solutions in the Sultanate.
3. Direct the entities within the scope of applying these Guidelines to consider the IoT Reference Model as a basic model when making new decisions to invest in IoT.
4. Contribute to enhancing the local market growth in providing IoT-based solutions and promoting its participation in the regional and international markets.
5. Provide mechanisms that ensure providing safe use of IoT services.

4. Purpose

Adopting a Unified Reference Model for the target audiences in the Sultanate to design, plan and implement IoT solutions, and encouraging innovation by using IoT solutions.

5. Scope

These Guidelines apply to all those concerned with IoT inside the Sultanate, including but not limited to:

- Telecommunications Service Providers
- IoT Service Providers
- IoT Solutions and Devices Developers
- IoT Devices and Systems Providers.
- IoT Users (Individuals, Companies, Units of the Administrative Apparatus of the State)

6. IoT Guidelines

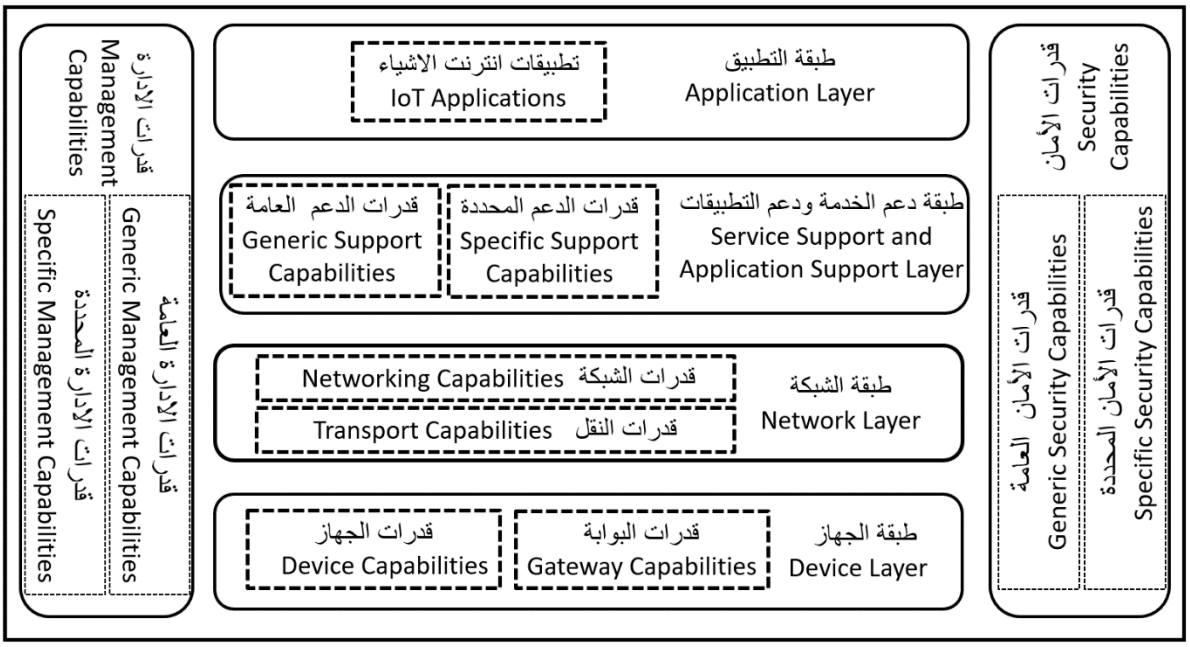
6.1 IoT Reference Model

The IoT Reference Model includes all components that enable companies, governments and users to connect to their own devices connected to the IoT. It consists of four layers in addition to the Management Capabilities and Security Capabilities that are connected to these layers which are:

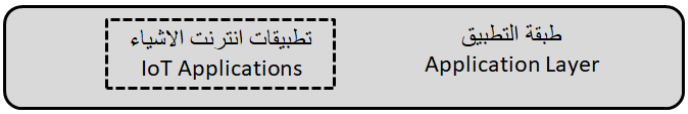
Physical Layer: It includes devices that constitute the IoT device, including sensors and network equipment.

Network Layer: It is responsible for transferring data that is collected by the physical layer to different devices.

Applications Layer: It includes protocols and interfaces used by the devices to identify and communicate with each other.
Service Support and Applications Support Layer: It includes remote control devices that enable the used devices to receive orders and other data via the control panel that displays information about the environment surrounding the users and allows the device to control it, then all that data is displayed to be analyzed by customized software systems before being saved. The following is a detailed explanation of each layer according to the Reference Model adopted by the International Telecommunication Union.

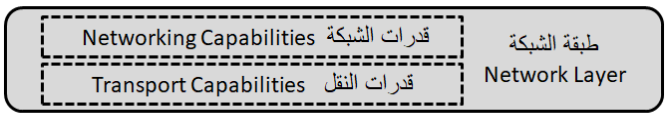


IoT Reference Model (the source is the International Telecommunication Union)
Application Layer: contains the IoT applications



Service Support and Application Support Layer: contains two types of capabilities

- Generic Support Capabilities: These are generic capabilities that can be used with different IoT applications such as data processing and storage. Moreover, they can be used if needed with Specific Support Capabilities for example when building additional specific support capabilities.
- Specific Support Capabilities: These are capabilities that meet the requirements of diversity in applications to provide support for the different IoT applications.
- Network Layer: It includes two types of capabilities as follows:



- Network Capabilities: They provide the control function relevant to the Network Connectivity such as the functions controlling the resources of access and transport, management and confirmation, authorization and accountability.
- Transport Capabilities: they provide connectivity related to transferring the IoT service and information of the application in addition to the information of IoT control and management.
- Device Layer: it is practically classified into two types of capabilities including Device Capabilities and Gateway Capabilities as follows:

- Device Capabilities: They may include the following capabilities for example:
    - Direct Interaction with the Telecommunication Network: Devices can collect and upload data directly to the telecommunication network (without using Gateway Capabilities) and they can receive information directly from the telecommunication network.
    - Indirect Interaction with the Telecommunication Network: Devices can collect and upload data indirectly to the telecommunication network via the Gateway Capabilities, and they can receive information indirectly from the telecommunication network.
    - Customized Networks: Devices may be capable of building networks following the way of customized networks in some scenarios that require an increase in scalability and speed of deployment.

- Power Saving: the device's capabilities may support “Sleep Mode” and “Wake Up Mechanism” to save power.

- Gateway Capabilities: based on the telecommunication technology type and/ or types of the used device IoT Gateway is not always considered necessary, since some devices will directly connect to the IoT Platform.

Gateways are used for several purposes such as:

- Supporting Multiple Interfaces: in the Device Layer, Gateway capabilities support devices that are connected via different types of wired and wireless technologies such as (Controller Area Network), (Bluetooth) and (Wi-Fi), while in the Network Layer, Gateway Capabilities can connect via different technologies such as the Public Switched Telephone Network (PSTN) and the (2G, 3G, 4G, and 5G) Networks, the Long Term Evolution (LTE), Ethernet, or Digital Subscriber Line (DSL), and Very Small Aperture Terminal (VSAT).
- Protocols Transfer: Gateway Capabilities are necessary in two cases:

First case: when telecommunications in the Device Layer use different protocols for the Device Layer.

Second case: When the telecommunications that include both the Device Layer and the Network Layer use different protocols.

Management capabilities: In a way similar to traditional telecommunication networks, IoT Management capabilities cover categories including: traditional Fault, Configuration, Accounting, Performance, Securities (FCAPS), i.e. Fault Management, Configuration Management, Accounting Management, and Security Management. They are classified into Generic Management Capabilities and Specific Management Capabilities.

Generic Management Capabilities: Basic Generic Capabilities in IoT include the following:

- Device Management such as activating the device remotely, diagnosis, firmware, and/or updating software and Device State Management.
- Local Network Topology
- Traffic and Congestion Management such as detecting the state of Network Overflow and reserving resources for critical data flow.

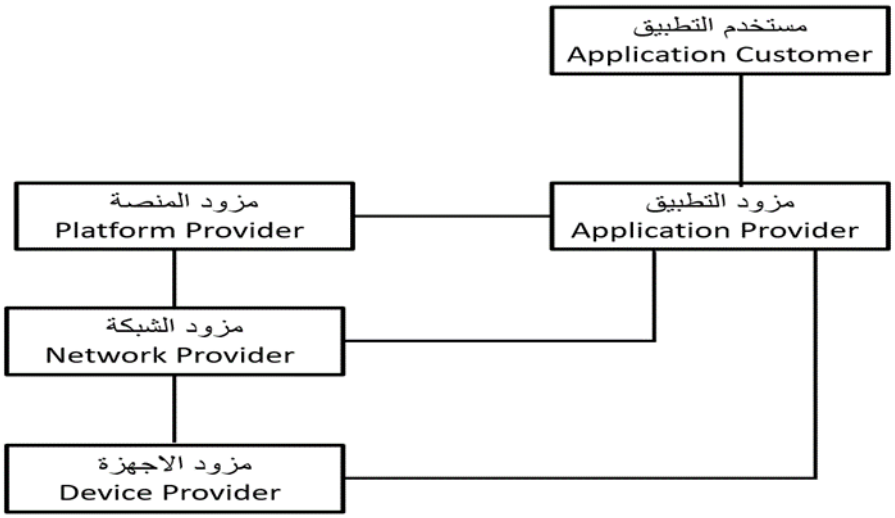
- Specific Management Capabilities: Specific Management Capabilities are closely connected to the application requirements, such as the requirements of monitoring the smart network power transmission line.
- Security Capabilities: There are two types of Security Capabilities including Generic Security Capabilities and Specific Security Capabilities.

Generic Security Capabilities are separate from applications and include:

- In the Application Layer: Authorization and Confirmation, Signalling Data and Use Data Confidentiality, and Signalling Integrity Protection.
- In the Device Layer: Confirmation, Authorization, Checking Device Integrity, Access Control Data Confidentiality, and protection of its integrity.
- Specific Security Capabilities: Specific Security capabilities are closely connected to the application requirements such as mobile payment and security requirements.

6.2IoT Ecosystem

As shown in the IoT Ecosystem below, the IoT System contains a variety of stakeholders, each of them performs one role at least and may perform more than one role according to the work model.



IoT Ecosystem (The source is the International Telecommunication Union)

Device Provider: The Device Provider is responsible for devices that provide the Network Provider and Application Provider with the primary data and/or the content according to the service type which may include devices from simple sensors to the most complicated independent devices such as tracking devices, smart meters etc, to devices embedded in complicated systems such as those in control systems, self-driving vehicles, etc.

Network Provider: plays a key role in the IoT Ecosystem since he performs the following key functions:

- Access and integrate into resources provided by other service providers.
- Support and control the basic infrastructure of IoT Capabilities.
- Offer IoT capabilities including Network Capabilities and view other providers' resources.

Platform Provider: One of the most important aspects of the IoT solution is the capability of a corporate to "operate and manage" its IoT solutions and devices is one of the most important aspects of the IoT solution through a variety of activities including Device Connection Management, Data Storage and Processing, Event Monitoring and Processing, and Analyses and External Systems Interfaces.

The definition of IoT Platform may mean a lot of different things in different contexts, therefore, this framework divides "IoT Platform" into three parts as follows:

- Application Enabling: a group of functions that have almost been gathered under the basic and comprehensive term Internet of Things (IoT) and are used to describe several IoT functions including: Application Programming Interface (API), Database Storage, visualization, Device Management, Application Server and others.
- Intelligence Enabling: It refers to using emerging technologies such as Analysis, Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) which adds value through smart analysis of a huge amount of data collected from IoT devices and other external devices.
- Connection Management: Connection Management refers to functions that manage the devices' connection, device ID and device configuration.

  Application Provider: The Application Provider uses capabilities or resources provided by the Network Provider, Device Provider and Platform Provider to provide the IoT Applications to the Application Customers, as he represents the relationship between the owner/ IoT Solutions Operator and the stakeholders who provide services or products for these solutions.

Application Customer: he is a user of IoT Applications provided the Applications Provider. IoT solutions may have various types of customers each type of them may have different requirements or consumption.

6.3 IoT Security Framework

This Framework provides high-level requirements that are related to security and privacy according to the International Telecommunication Union's Recommendation No. (ITU-T X.1361) which are:

Communications Security:

It provides secure, trusted and privacy-protected communication capability so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected during data transmission or transfer in IoT.

Data Management Security

It provides secure, trusted and privacy-protected data management capability so that unauthorized access to the content of data can be prohibited, the integrity of data can be guaranteed and privacy-related content of data can be protected when storing or processing data in IoT.

Service Provision Security:

Secure, trusted and privacy-protected service provision capability is provided, so that unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected.

Integration of security policies and techniques

The ability to integrate different security policies and techniques is provided, to ensure consistent security control over the variety of devices and user networks in IoT.

Mutual Authentication and Authorization:
Before a device (or an IoT user) can access the IoT, mutual authentication and authorization between the device (or the IoT user) and IoT is required to be performed according to predefined security policies.
Security Audit:
Security audit is required to be supported in IoT. Any data access or attempt to access IoT applications is required to be fully transparent, and traceable according to relevant regulations and laws. In particular, IoT is required to support security audit for data transmission, storage, processing and application access.

6.4 Obligations and Rights

General Obligations:

1. Compliance with all applicable laws and regulations in the Sultanate, such as Cloud Computing policies, and Cyber Crime Law.
2. Preserving the confidentiality of the beneficiary's service data and not disclosing that data except with the user's prior consent or based on an official request from the Judicial Authority or the authorized entities.
3. Obtaining the technical approvals required for all devices, systems and units to be used before their operation according to the instructions and procedures adopted by the Telecommunications Regulatory Authority.
4. Compliance with any procedures/ regulatory decisions approved by the concerned authorities related to using IoT identifiers such as Internet Protocol Addresses (IPv4/ IPv6) or any other identifiers such as (MAC address).
5. Compliance with providing servers used to provide IoT services in the Sultanate and storing data in them.
6. Compliance with providing technical capabilities in the IoT networks devices and equipment to save data for reference when needed for at least twelve months or as determined by the authorized entities.
7. Compliance with the published or future procedures/ regulatory decisions issued by the competent authorities in the Sultanate related to network security and customer data security and privacy.
8. Compliance with the new National Numbering Plans and Use of Scarce Resources and technical specifications in the Sultanate to cope with the latest developments in the Telecommunications and Information Technology Sector, taking into consideration the recommendations issued by the relevant international organizations.

Obligations of the Service Provider:

1. Obtaining a permit to provide IoT services from the competent authorities in the Sultanate before starting to provide the service.

2. Notifying the data subject of the methods and means of collecting, processing and sharing his data as well as the security measures to ensure data privacy according to the applicable regulations and policies in the Sultanate.
3. Notifying the data subject of the other sources used in the event of collecting additional data indirectly (from law enforcement agencies and civil society)
4. Collecting/ processing/ sharing data shall be limited to the minimum data that fulfills the purpose for which the data subject has implicitly or explicitly approved.
5. The use of data shall be limited to the purpose for which it is collected.
6. Preparing and documenting the policies and procedures for data retention according to the applicable policies and regulations.
7. Compliance with storing and processing data within the geographical boundaries of the Sultanate to preserve the digital sovereignty of national data, and it may not be processed or stored except after obtaining the approval of the competent authorities.
8. Developing a clear plan to manage data including (Data Collection Mechanism/Data Analysis Mechanism/ Data Classification Mechanism/Deployment and Sharing/ Usage/ Data Protection/ Data Ownership/ Data Retention/ Data Destruction)
9. Building security and privacy support systems as a key and integral part when designing the IoT system and ensuring that they are available and that the devices used in them are compatible.
10. Identifying types of high-level security risks to the system that require applying high-protection basics and taking security measures against them at different levels.
11. Taking all security measures to monitor and eliminate unauthorized access by a person/ persons/ entities to customer data.

Rights of Data Subject:

- The right to obtain his approval for data processing, unless there are lawful purposes requiring the contrary.
- The right to access his data with the Service Provider to review it, request to modify or update it, and request to destroy data that is no longer needed and obtain a copy of it.

7. Management

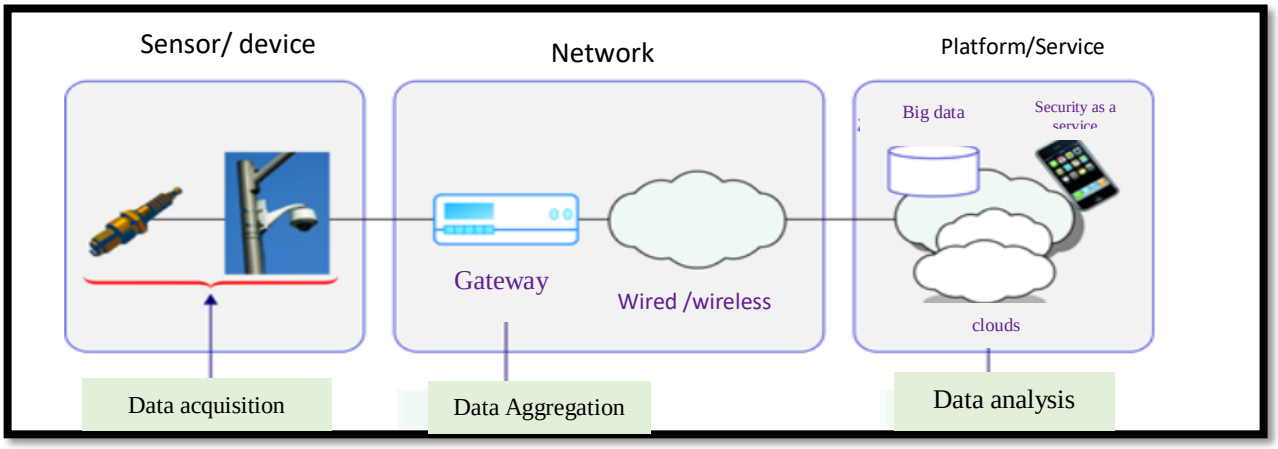
1. This Guideline is owned by the Ministry of Transport, Telecommunications and Information Technology and shall be subject to review as required.
2. This Guideline shall be applied as of its approval and circulation by the Ministry of Transport, Telecommunications and Information Technology.

8. Relevant Publications

1. Security Framework for the Internet of Things based on the Gateway Model- the International Telecommunication Union (2018).
2. IoT Security Compliance for European Union (2016)
3. IoT Reference Framework-Australia (2018)
4. IoT Regulatory Framework of the International Telecommunication Union (2017)
5. IoT Smart Government Framework (Study of IoT Cybersecurity Policies in the US Federal Government (2020).
6. IoT Policy- the Republic of India (2018)
7. Public Consultations on the Internet of Things - Telecommunications Regulatory Authority, Sultanate of Oman (2020)
8. IoT Regulatory Framework- Saudi Telecommunications Regulatory Authority(2019)
9. IoT System Requirements -Jordanian Telecommunications Regulatory Authority(2021)

Annex (1)

Some Security Threats that face the Internet of Things



IoT Functional Architecture (Source: the International Telecommunication Union)

Security Threats to IoT Sensors/Devices

- Device capture: Refers to a device being physically compromised or having its keys lost.
- Sinkhole attack: An intruder introduces a counterfeit device inside the network and uses it to attract all data traffic by sending fake routing information to its neighboring devices to attract network traffic to itself.
- Sybil attack: Refers to an attack in which a malicious device illegitimately takes on multiple identities. A malicious device's additional identity is referred to as a Sybil node. This attack is launched in conjunction with other attacks, to reduce the effectiveness of fault-tolerant mechanisms.
- Flooding attack: A flooding attack is a form of a denial of service (DoS) attack in which an attacker sends a succession of 'hello' packets to a targeted device in an attempt to consume enough of the device's resources to make the device unresponsive to legitimate traffic.
- Wormhole attack: Wormhole attacks occur in a tunnel (a data path between two networked devices that is established across an existing network infrastructure). A network that tunnels data to another network gets the data from one network and replicates it onto another network through the tunnel and that particular network may be confused due to this action.
- Impersonation of sensor/device. This attack happens when an attacker successfully masquerades as the identity of a legitimate sensor/device.

Security Threats to IoT Gateway

- Unauthorized Access: Unauthorized access to a gateway may cause the disclosure of sensitive information, data modification, Denial of Service and illicit use of resources. For example, once an attacker has accessed a gateway, this may result in monitoring of the now unencrypted data can result in user names, and passwords.
- Rogue gateway: Even if all wireless gateways are secure, it is easy for attackers to deploy a rogue gateway of their own. For example, an attacker might deliberately and covertly install a rouge wireless access point in order to grant easy access to another attacker on the network whether locally or remotely to replace an existing
- wireless access point with one on which they have full configuration and monitoring access or even configure a rogue wireless access point, with similar settings, but with a higher power ratio necessary to overcome the legitimate wireless access point's signal.

Denial of service attack: The wireless sensor network is particularly vulnerable to DoS attacks due to its features of an open medium, and dynamic changing topology.

Security Threats to the Network:

- Unauthorized access: Unauthorized access to a wireless sensor network can cause disclosure of sensitive information, data modification, DoS and illicit use of resources. For example, once an attacker has accessed a sensor network, monitoring of the now unencrypted data can result in user names and passwords being compromised.
- Packet sniffing: For wireless sensor networks that do not have encryption capabilities it is easy for attackers to eavesdrop on network communications. A network packet sniffer is a tool that sets the network card to "promiscuous mode". This means that the interface will receive and process all traffic rather than only traffic meant for it.
- Bluejacking: This type of attack is conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to users of Bluetooth-enabled devices to induce the user to respond in some fashion or to add the new contact to the device’s address book.
- Bluesnarfing: This means the unauthorized access of information from a targeted
wireless device through a Bluetooth connection, often between phones, desktops, laptops, and personal digital assistants (PDAs).

Security Threats to Platform/ Services

The main task of the application layer is to collect and process a large number of user data, including users' personal information or confidential information of various transactions. This data is an attacker's main target, stolen, tampered or damaged. It is necessary to protect data using privacy protection mechanisms. Application layer threats include: mass data processing, out-of-control smart devices, unauthorized human intervention, and the inability of devices to recover from disaster.

Platform/services specific threats:

- Profiling: Exploratory process used to gather information on the platform/services.
- Denial of service: An attack in which the platform/service is overwhelmed by massive service requests and becomes too busy to respond to client requests**.**
- Malicious code execution: Any part of a software system or script, that is intended to cause undesired effects, security or personally identifiable information breaches, or damage to a system.
- Network eavesdropping: An attack that captures packets transmitted from the network and reads the data content in search of sensitive information such as passwords.
- Inference attack: This attack occurs when an attacker is able to infer protected information from rightfully accessible information with lower classification.