**Assignment No. 3**

**Topic: “How IOT Technology & Protocols are helpful in making the system smart”**

**Submitted by:**

**Kashif Iqbal**

**Registration No. 2171581**

**Submitted to:**

**Dr. Sagheer Abbas**

**Department of Computer Science**

**National College of Business Administration& Economics**

# Internet of Things - Technology and Protocols

Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways. However, the journey is far from over. We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web. We are entering an era of the “Internet of Things” (abbreviated as IoT). We use these capabilities to query the state of the object and to change its state if possible. In common jargon, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network. We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.

For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers. IoT is not a single technology; rather it is a collection of various technologies that work together in tandem. IoT technologies have significantly been able to reduce human effort and improve the quality of life.

**Architecture of IoT**

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers.

The first architectural component of IoT is the perception layer. It collects data using sensors, which are the most important drivers of the Internet of Things. There are various types of sensors used in diverse IoT applications. The most generic sensor available today is the smartphone. The smartphone itself has many types of sensors embedded in it such as the location sensor (GPS), movement sensors (accelerometer, gyroscope), camera, light sensor, microphone, proximity sensor, and magnetometer. These are being heavily used in different IoT applications. Many other types of sensors are beginning to be used such as sensors for measuring temperature, pressure, humidity, medical parameters of the body, chemical and biochemical substances, and neural signals. A class of sensors that stand out is infrared sensors that predate smartphones. They are now being used widely in many IoT applications: IR cameras, motion detectors, measuring the distance to nearby objects, presence of smoke and gases, and as moisture sensors.

**Three level-Architectures**

The most basic architecture is a three-layer architecture. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

1. **The perception** **layer** is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
2. **The network layer** is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
3. **The application layer** is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, smart environment and smart health.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things.

**Software Support**

IoT software addresses its key areas of networking and action through platforms, embedded systems, partner systems, and middleware. These individual and master applications are responsible for data collection, device integration, real-time analytics, and applications and process extension within the IoT network. They exploit integration with critical business systems (e.g., ordering systems, robotics, scheduling, and more) in the execution of related tasks.

## Data Collection

This software manages sensing, measurements, light data filtering, light data security, and aggregation of data. It uses certain protocols to aid sensors in connecting with real-time, machine-to-machine networks. Then it collects data from multiple devices and distributes it in accordance with settings. It also works in reverse by distributing data over devices. The system eventually transmits all collected data to a central server.

## Device Integration

Software supporting integration binds (dependent relationships) all system devices to create the body of the IoT system. It ensures the necessary cooperation and stable networking between devices. These applications are the defining software technology of the IoT network because without them, it is not an IoT system. They manage the various applications, protocols, and limitations of each device to allow communication.

## Real-Time Analytics

These applications take data or input from various devices and convert it into viable actions or clear patterns for human analysis. They analyze information based on various settings and designs in order to perform automation-related tasks or provide the data required by industry.

## Application and Process Extension

These applications extend the reach of existing systems and software to allow a wider, more effective system. They integrate predefined devices for specific purposes such as allowing certain mobile devices or engineering instruments access. It supports improved productivity and more accurate data collection.

The hardware utilized in IoT systems includes devices for a remote dashboard, devices for control, servers, a routing or bridge device, and sensors. These devices manage key tasks and functions such as system activation, action specifications, security, communication, and detection to support-specific goals and actions.

## IoT − Sensors

The most important hardware in IoT might be its sensors. These devices consist of energy modules, power management modules, RF modules, and sensing modules. RF modules manage communications through their signal processing, WiFi, ZigBee, Bluetooth, radio transceiver, duplexer, and BAW.

The sensing module manages sensing through assorted active and passive measurement devices. Here is a list of some of the measurement devices used in IoT −

## Wearable Electronics

Wearable electronic devices are small devices worn on the head, neck, arms, torso, and feet.

Current smart wearable devices include −

* **Head** − Helmets, glasses
* **Neck** − Jewelry, collars
* **Arm** − Watches, wristbands, rings
* **Torso** − Clothing, backpacks
* **Feet** − Socks, shoes

## Standard Devices

The desktop, tablet, and cellphone remain integral parts of IoT as the command center and remotes.

* The **desktop** provides the user with the highest level of control over the system and its settings.
* The **tablet** provides access to the key features of the system in a way resembling the desktop, and also acts as a remote.
* The **cellphone** allows some essential settings modification and also provides remote functionality.

Other key connected devices include standard network devices like **routers** and **switches**.

## Standard Networks

IoT primarily exploits standard protocols and networking technologies. However, the major enabling technologies and protocols of IoT are RFID, NFC, low-energy Bluetooth, low-energy wireless, low-energy radio protocols, LTE-A, and WiFi-Direct. These technologies support the specific networking functionality needed in an IoT system in contrast to a standard uniform network of common systems.

## NFC and RFID

RFID (radio-frequency identification) and NFC (near-field communication) provide simple, low energy, and versatile options for identity and access tokens, connection bootstrapping, and payments.

* RFID technology employs 2-way radio transmitter-receivers to identify and track tags associated with objects.
* NFC consists of communication protocols for electronic devices, typically a mobile device and a standard device.

## Low-Energy Bluetooth

This technology supports the low-power, long-use need of IoT function while exploiting a standard technology with native support across systems.

## Low-Energy Wireless

This technology replaces the most power hungry aspect of an IoT system. Though sensors and other elements can power down over long periods, communication links (i.e., wireless) must remain in listening mode. Low-energy wireless not only reduces consumption, but also extends the life of the device through less use.

## Radio Protocols

ZigBee, Z-Wave, and Thread are radio protocols for creating low-rate private area networks. These technologies are low-power, but offer high throughput unlike many similar options. This increases the power of small local device networks without the typical costs.

## LTE-A

LTE-A, or LTE Advanced, delivers an important upgrade to LTE technology by increasing not only its coverage, but also reducing its latency and raising its throughput. It gives IoT a tremendous power through expanding its range, with its most significant applications being vehicle, UAV, and similar communication.

## WiFi-Direct

WiFi-Direct eliminates the need for an access point. It allows P2P (peer-to-peer) connections with the speed of WiFi, but with lower latency. WiFi-Direct eliminates an element of a network that often bogs it down, and it does not compromise on speed or throughput.