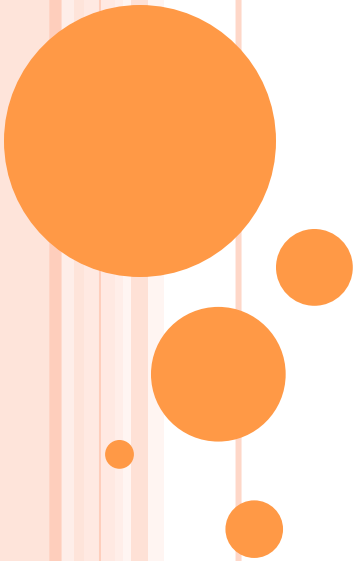

BLM5134 – WEEK 11

Internet of Things and Data Management

IoT – ONe PAradıgm, Many Vısıons

- Internet oriented
- Things oriented
  - RFID (Radio-Frequency Identification)
  - EPC (Electronic Product Code)
- Semantic oriented

IoT PAradıgm

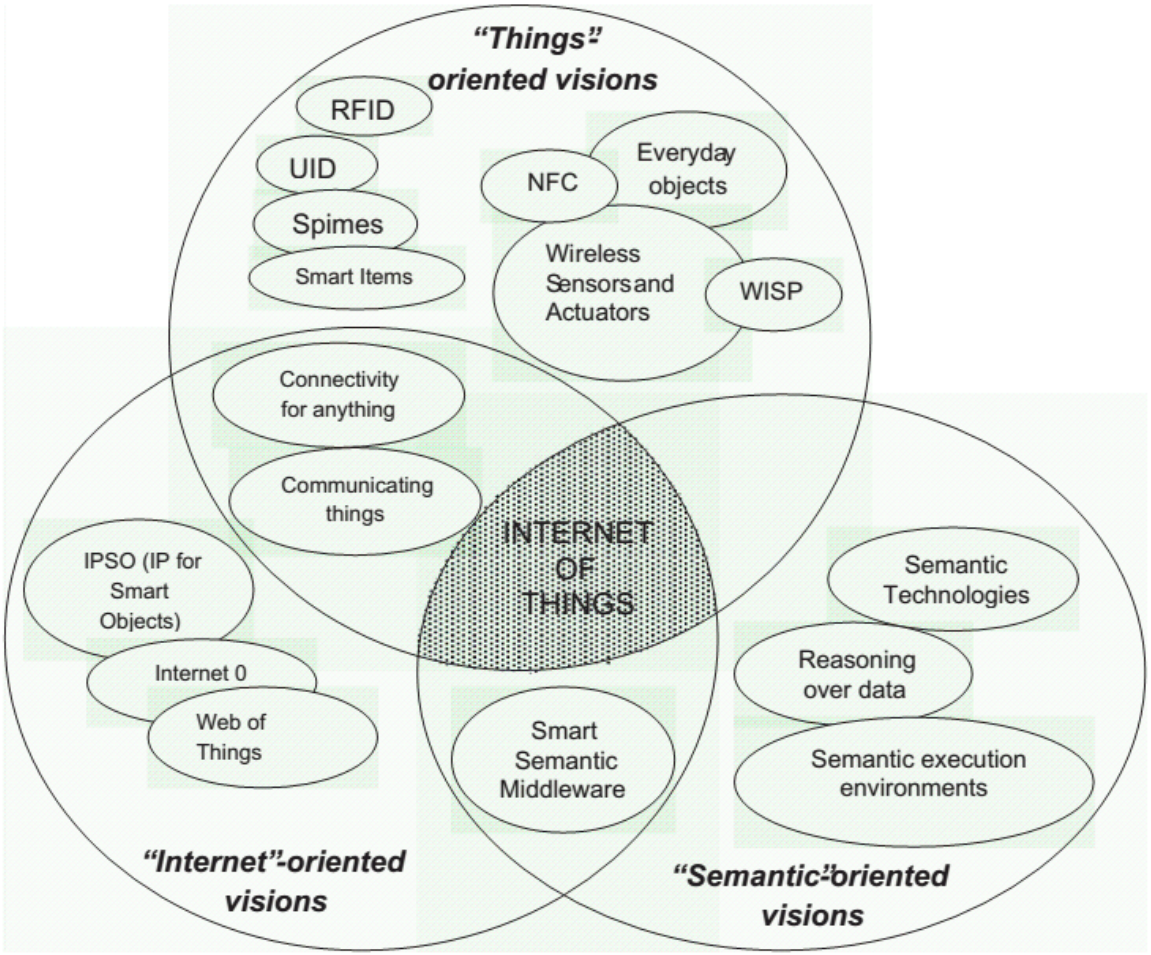

Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

SPIME

- a concept that emerged aside IoT is the spime,
- defined as an object that can be tracked
- through SPACE and TIME throughout its lifetime and that will be sustainable, enhancable, and uniquely identifiable

SOME VISIONS

- ITU vision

«from anytime, anyplace connectivity for anyone, we will now have connectivity for anything»

- European Commision Vision

"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"

ENABLED TECHNOLOGIES

- Identification, Sensing , Communication
- Middleware

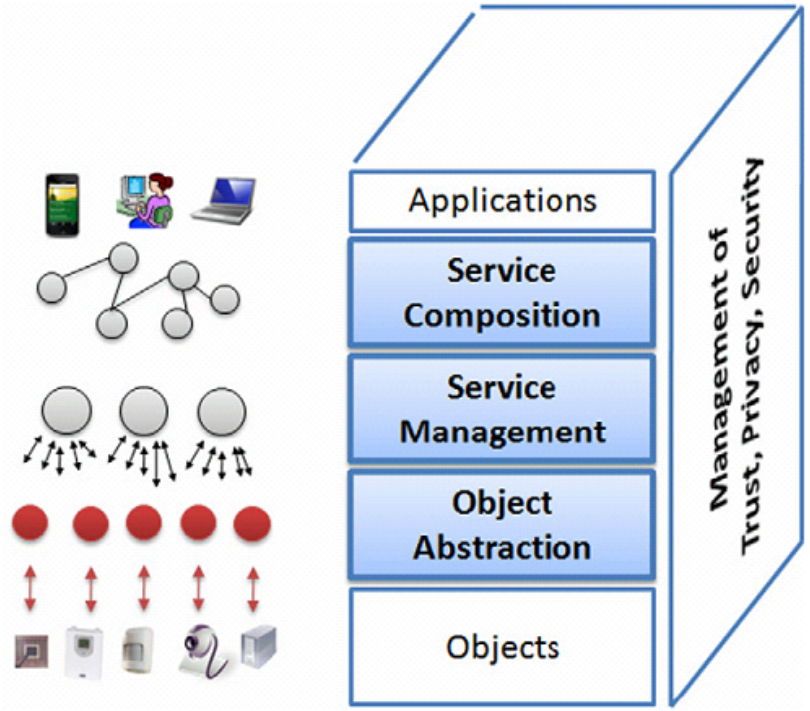

Fig. 2. SOA-based architecture for the IoT middleware.

IoT APPLICATION DOMAINS

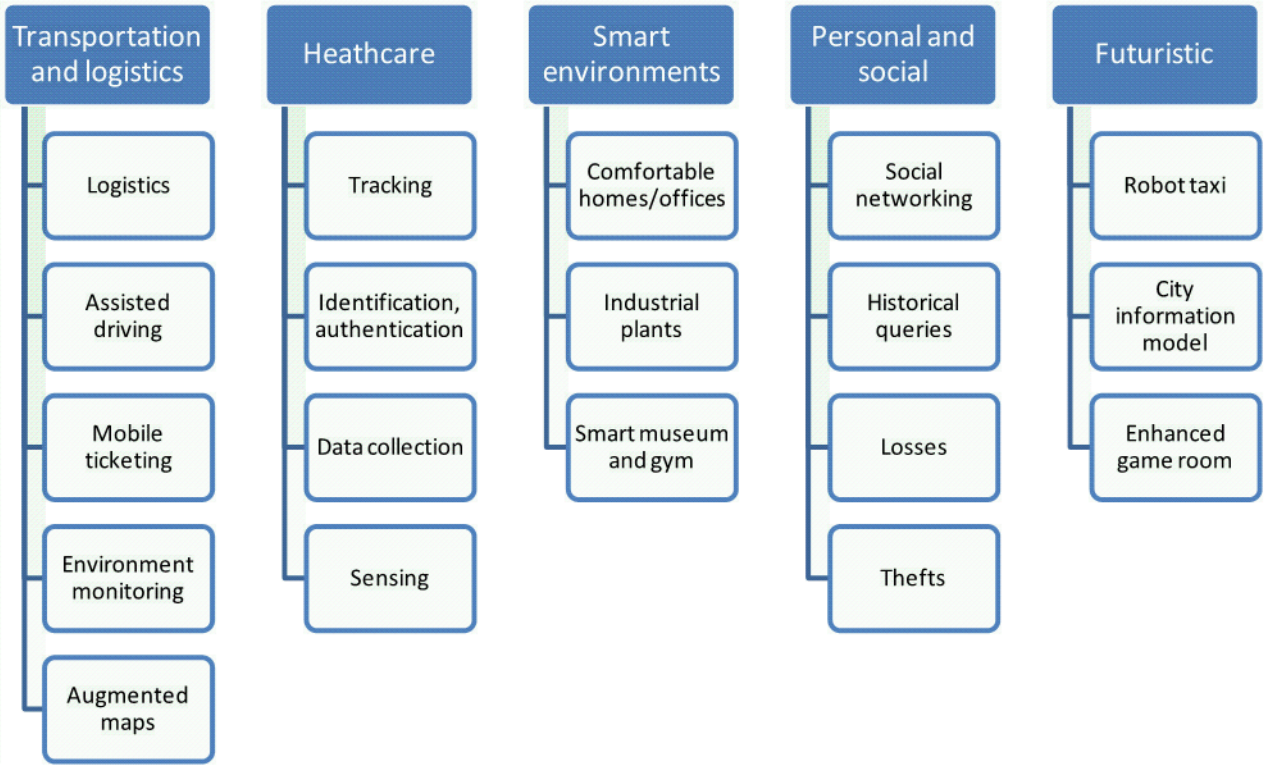

Fig. 3. Applications domains and relevant major scenarios.

OPEN ISSUES

Table 2
Open research issues.

Open issue	Brief description of the cause	Details in
Standards	There are several standardization efforts but they are not integrated in a comprehensive framework	Section 5.1
Mobility support	There are several proposals for object addressing but none for mobility support in the IoT scenario, where scalability and adaptability to heterogeneous technologies represent crucial problems	Section 5.2
Naming	Object Name Servers (ONS) are needed to map a reference to a description of a specific object and the related identifier, and *vice versa*	Section 5.2
Transport protocol	Existing transport protocols fail in the IoT scenarios since their connection setup and congestion control mechanisms may be useless; furthermore, they require excessive buffering to be implemented in *objects*	Section 5.2
Traffic characterization and QoS support	The IoT will generate data traffic with patterns that are expected to be significantly different from those observed in the current Internet. Accordingly, it will also be necessary to define new QoS requirements and support schemes	Section 5.2
Authentication	Authentication is difficult in the IoT as it requires appropriate authentication infrastructures that will not be available in IoT scenarios. Furthermore, things have scarce resources when compared to current communication and computing devices. Also man-in-the-middle attack is a serious problem	Section 5.3
Data integrity	This is usually ensured by protecting data with passwords. However, the password lengths supported by IoT technologies are in most cases too short to provide strong levels of protection	Section 5.3
Privacy	A lot of private information about a person can be collected without the person being aware. Control on the diffusion of all such information is impossible with current techniques	Section 5.3
Digital forgetting	All the information collected about a person by the IoT may be retained indefinitely as the cost of storage decreases. Also data mining techniques can be used to easily retrieve any information even after several years	Section 5.3

STANDARDIZATION ACTIVITIES

Table 3
Characteristics of the most relevant standardization activities.

Standard	Objective	Status	Comm. range (m)	Data rate (kbps)	Unitary cost ($)
Standardization activities discussed in this section					
EPCglobal	Integration of RFID technology into the electronic product code (EPC) framework, which allows for sharing of information related to products	Advanced	~1	~10^2	~0.01
GRIFS	European Coordinated Action aimed at defining RFID standards supporting the transition from localized RFID applications to the *Internet of Things*	Ongoing	~1	~10^2	~0.01
M2M	Definition of cost-effective solutions for machine-to-machine (M2M) communications, which should allow the related market to take off	Ongoing	N.S.	N.S.	N.S.
6LoWPAN	Integration of low-power IEEE 802.15.4 devices into IPv6 networks	Ongoing	10–100	~10^2	~1
ROLL	Definition of routing protocols for heterogeneous low-power and lossy networks	Ongoing	N.S.	N.S.	N.S.
Other relevant standardization activities					
NFC	Definition of a set of protocols for low range and bidirectional communications	Advanced	~10^{-2}	Up to 424	~0.1
Wireless Hart	Definition of protocols for self-organizing, self-healing and mesh architectures over IEEE 802.15.4 devices	Advanced	10–100	~10^2	~1
ZigBee	Enabling reliable, cost-effective, low-power, wirelessly networked, monitoring and control products	Advanced	10–100	~10^2	~1

ADDRESSING AND NETWORKING ISSUES

- IPv4 vs IPv6 (128 bits)
- RFID tags (64-96 bit identifiers)
- Domain Name Servers vs. Object Name Service
- Traffic Characterization(QoS)

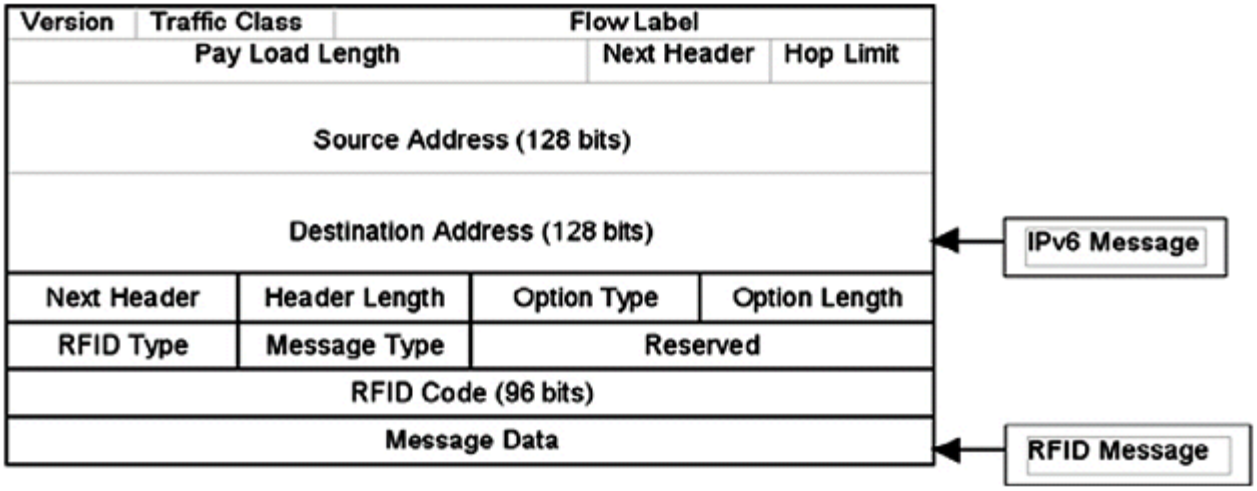

Fig. 4. Encapsulation of RFID message into an IPv6 packet.

TCP is INadequate For IoT

- Connection Setup
  - Small amount of data, Setup Phase, limited resources
- Congestion Control
- Data Buffering

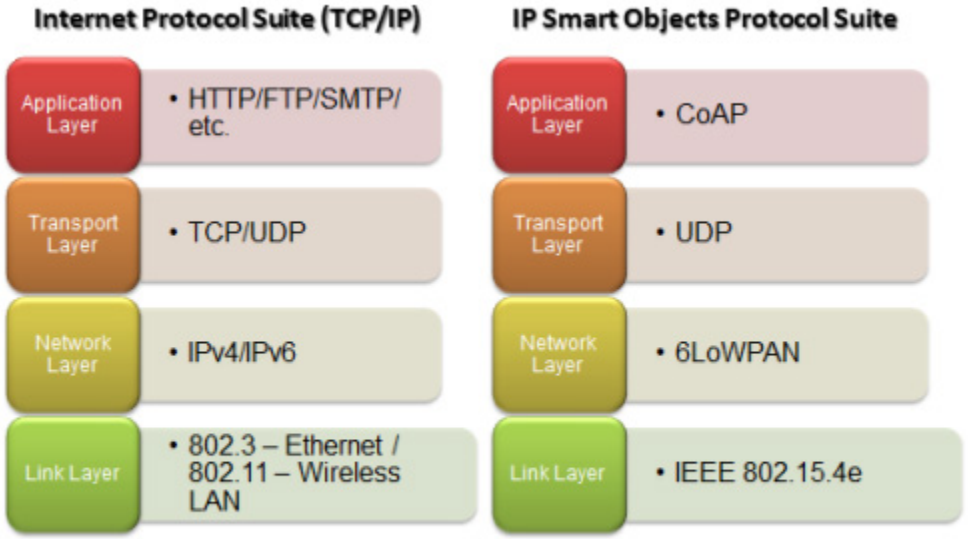

Figure 1 TCP/IP Stack and IP Smart Objects Protocol Stack

SECURITY BASICS IN IoT

- Resilience to attacks: The system has to avoid single points of failure and should adjust itself to node failures.
- Data authentication: As a principle, retrieved address and object information must be authenticated.
- Access control: Information providers must be able to implement access control on the data provided.
- Client privacy: Measures need to be taken that only the information provider is able to infer from observing the use of the lookup system related to a specific customer; at least, inference should be very hard to conduct.

SECURITY And PRIVACY

- it is easy to physically attack things
- most of the communications are wireless, which makes eavesdropping extremely simple.
- most of the IoT components are characterized by low capabilities in terms of both energy and computing resources (this is especially the case for passive components) and thus, they cannot implement complex schemes supporting security
- Data integrity solutions
  - memory is protected in most tag technologies and solutions have been proposed for wireless sensor networks

SECURITY AND PRIVACY

- Typical cryptographic algorithms spend large amount of resources in terms of energy and bandwidth both at the source and the destination. Such solutions cannot be applied to the IoT, given that they will include elements (likeRFID tags and sensor nodes) that are seriously constrained in terms of energy, communications, and computation capabilities.

- It follows that new solutions are required able

to provide a satisfactory level of security regardless of the scarcity of resources.

SECURITY AND PRIVACY

- In fact, as the cost of storage decreases, the amount of data that can be memorized increases dramatically. Accordingly, there is the need to create solutions that periodically delete information that is of no use for the purpose it was generated.
- Accordingly, the new software tools that will be developed in the future should support such forgetting functionalities.

BAR CODES AND QR CODES

Version 1(21*21) content 'version1'

Version 2(25*25) conte

Fig 3: QR code and Barcode

Version 3(29*29) content: 'version3 'version4'

Version 4(33*33) content:

QR-code'

QR-code'

DIFFERENT BAR CODES

Figure 3.1. Barcode: UPC (left) and Code-93 (right)

DIFFERENT QR CODES

Figure 3.3. QR Code (left), Data Matrix/Semacode (center) and MaxiCode (right).

Qr Code

- Numeric only Max. 7,089 characters
- Alphanumeric Max. 4,296 characters
- Binary (8 bits) Max. 2,953 bytes

2D Barcodes OvervIEw

Table 3.1. 2D barcodes overview.

Name	**QR Code**	**PDF417**	**Data Matrix**	**MaxiCode**
Type	Matrix	Stacked Bar Code	Matrix	Matrix
Developer	Denso	Symbol Technologies	RVSI Acuity CiMatrix	UPS
Numeric capacity	7,089	2,710	3,116	138
Alphanumeric capacity	4,296	1,850	2,355	93
Binary capacity	2,953	1,018	1,556	-

- Tags may be categorized by
  - power type (active or passive),
  - memory capacity / working mode (read only or read and write)
  - frequency range.

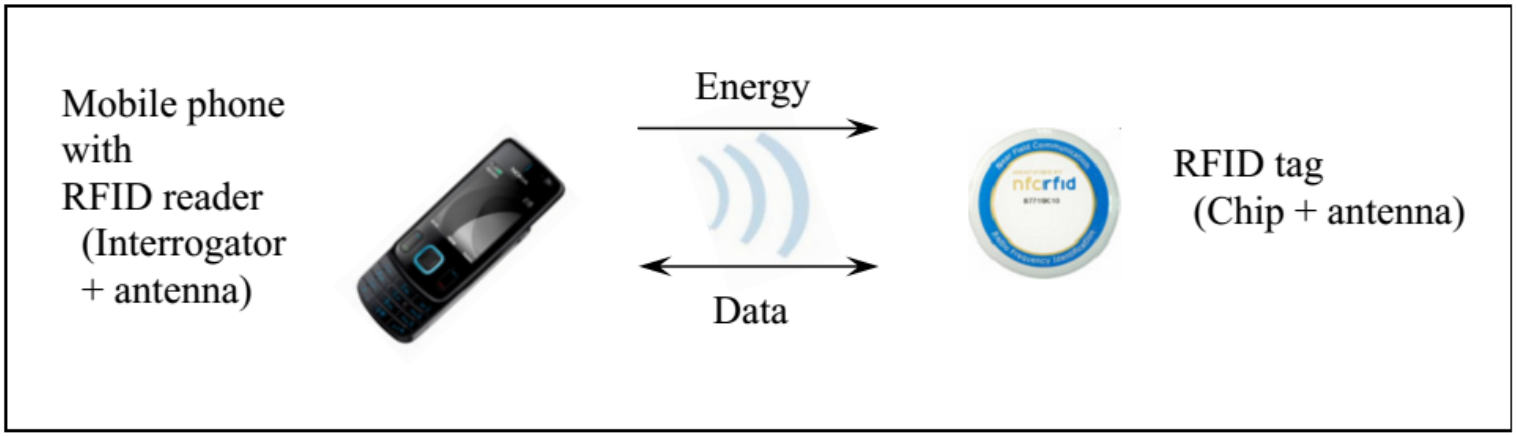

Figure 3.5. The mobile device as part of the RFID system.

RFID

- Active Tags
- Semi-Passive Tags
- Passive Tags

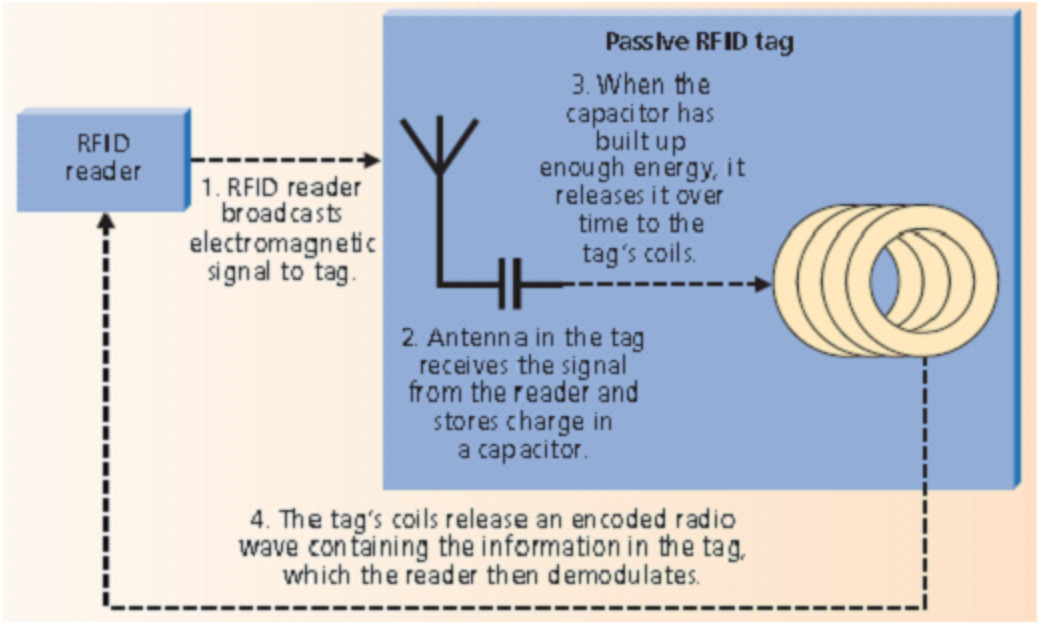

Fig5. Working of RFID

FREQUENCY RANGE

- Low Frequency(LF: 125 kHz to 134 kHz) tags are used in many applications. They are passive tags, thus providing the lowest reading distance (less that one third of a meter) and lowest data transfer rates among tags with other working frequencies. LF tags have limited anti-collision support; it is difficult to read a number of tags simultaneously. An advantage of such tags is ability to successfully operate near liquid environments.

- High Frequency(HF: 13.56 MHz) tags are passive tags too, but data transfer rate is better than in the case of LF. HF tags are cheaper to produce because of simpler antennas. Due to no limitations for HF frequency, such tags are the most popular [51]. The maximum reading distance is around one meter (information may be found in [30]). Near Field Communication technology (NFC) utilizes this operating frequency HF and LF tags are available for global use without licensing.

FREQUENCY RANGE

- Ultra High Frequency(UHF): 433MHz and 860 to 930 MHz) tags are implemented in several designs: 433MHz frequency is best suitable for active tags (fig. 3.7) and latter UHF frequency window is mostly used for passive and semi-passive tags. UHF tags support anti-collision protocols, which enables reading hundreds of tags at the same time. UHF tag must be isolated from substances with water or metal in order to be successfully read. The reading range varies depending on the power source of a tag and is up to 30 meters for active tags
- Microwave frequency tags are available using mostly 2.4 GHz and sometimes 5.8 GHz frequency. Higher frequency may carry more energy, therefore the reading range as well as the data transfer rate is much higher compared to tags with lower frequencies. The common issue is that radio waves of Microwave and UHF bands are easily absorbed, interferenced or reflected which causes certain troubles. The cost of equipment and usage restrictions make microwave solutions to be rarely used. Only few companies produce this type of equipment [54].

RFID FREQUENCY SPECTRUM DETAILS

Table 3.2. RFID frequency spectrum details.

	LF 125-134 kHz	**HF** 13.56 MHz	**UHF** 433, 860-930 MHz	**Microwave** 2.4, 5.8 GHz
Tag expense	High	High, Medium	Medium	High
Reader cost	Low	Medium	High, Medium	High
Work range (max.)	~30 cm	~1m	~30 meters (active)	More than 100 m (>300m active)
Data transfer rate	Low	Medium	High	High
Interference	Low	Low	Medium	High
Advantages	Low environment absorption	Available worldwide	Perfect for medium range applications	Wide access range
Common applications	Animal ID, security, engine immobilizers	Security, item tracking, ticketing.	Container, truck tracking	Access control, industry, production lines

Table 3.3. Applications for radio frequency identification.

Application	Purpose	References and examples
Supply chain	Retail inventory, shipping and receiving, warehousing, material management	Wal-Mart, Metro Group, Siemens, Mars, Wrigley. [5, 6, 50]
Consumer goods tracking	Tracking items inside stores	Prada. [8, 37]
Pharmaceutical	Drugs counterfeiting detection.	[3, 4]
Healthcare	Tracking patients, equipment, and services.	[1, 13]
Sports	Track timing	NASCAR. [34]
Library and media carriers	Track rental items, books, digital disks.	[2]
Access control	Control access to buildings, rooms and secured areas; passport and border control	USA, Japan, Holland, Norway, Malaysia. [13, 14, 15, 54]
Ubiquitous programming	Tagging objects and people for variety of applications.	[7, 9, 38, 50]
Contactless payment systems	Credit cards (MasterCard, American Express), smart cards, toll payment systems	USA. [16]
Entertainment	Amusement parks, clubs, event management, smart posters	Olympic Games. [9, 10, 11, 38]
Document management	Track documents in offices and hospitals	3M file tracking system.
Transportation management	Truck and containers tracking, rail ways, speed tracking, keyless start systems and engine immobilization systems.	Audi, Lexus, Toyota, Ford, Honda. [12, 54]
Ticketing	Public transport, bus, underground, railway, airline tickets	Washington, London Metro payment systems, ski pass
Wildlife and pets	Tracking animals.	[35]
Luggage tracking	Track baggage at airports and other transportation stations.	Hong Kong Airport, Globalbagtag. [18, 54]

ADvantages Of RfID

- Rewrite capability..
- No need for line of sight
- Increased the distance reading.
- Increased amount of data storage..
- Reading multiple tags.
- Reading RFID labels
- Working environment.
- Smart behaviour
- High Security

DISADVANTAGES OF RFID

- The complexity of production. (2D) barcode can be printed on any printer, while RFID tags production requires either industrial equipment or special printers.
- The cost of RFID system is higher than the one which is based on (2D) barcodes.
- Companies calculate business functions like Return On Investment to find out how technology improvement may benefit the company.
- Interference to electromagnetic fields. This is an issue that radio frequency equipment users have to deal with. However, LF and HF are less exposed to interference than higher frequency spectrum tags and readers.
- Lack of trust, ability to gather private information about people.
- The number of barcode based solutions is substantially greater than solutions based on RFID.
- Lack of open standards developed for RFID. Equipment produced by some manufacturers may have different standards. Thus there are compatibility issues.

Attribute	Barcode	QR code	RFID
Line of Site	Required	Required	Not required (in most of the cases)
Read Range	Several inches to feet	Several inches to feet	Passive RFID -Up to 30 feet Active RFID -Up to 100s feet
Identification	Most barcode only identify only type of item (not uniquely)	QR code can identify each item uniquely (Limited up to certain value)	It can uniquely identify each item
Read\Write	Only read	Only read	Read Write
Technology used	Optical (laser)	Optical (laser)	RF(Radio frequency)
Automation	Most barcode Scanners need humans to operate	QR scanners need humans to operate	Fixed scanners don't need human labor
Updating	Cannot be Updated	Cannot be Updated	New information can be written on old tag
Tracking	Manual tracking required	Manual tracking Required	No need of tracking
Information Capacity	Very less	Less	More than QR and Barcode
Ruggedness	No	No	Yes
Reliability	Wrinkled and smeared tags won't work	Wrinkled tags may work 30% data recoverable	Nearly flawless read rate
Data capacity	<20 characters with linear	up to 7,089 characters[9]	100s to 1000 characters
Orientation Dependent	Yes	No	No
Marginal Cost	0.01$	0.05$	0.05-1$