WIRELESS TECHNOLOGY FOR SMART CITIES AND URBAN PLANNING

Dr. Gunjan Mittal Roy

IILM University, Greater Noida campus

Greater Noida, India

[gunjan.mittal@iilm.edu](mailto:gunjan.mittal@iilm.edu)

Dr. Sambhavi Shukla

IILM University, Greater Noida campus

Greater Noida, India

[sambhavi.shukla@iilm.edu](mailto:sambhavi.shukla@iilm.edu)

Dr. Damyanti Singh (Corresponding Author)

IILM University, Greater Noida campus

Greater Noida, India

[damyanti.singh@iilm.edu](mailto:damyanti.singh@iilm.edu)

**ABSTRACT**

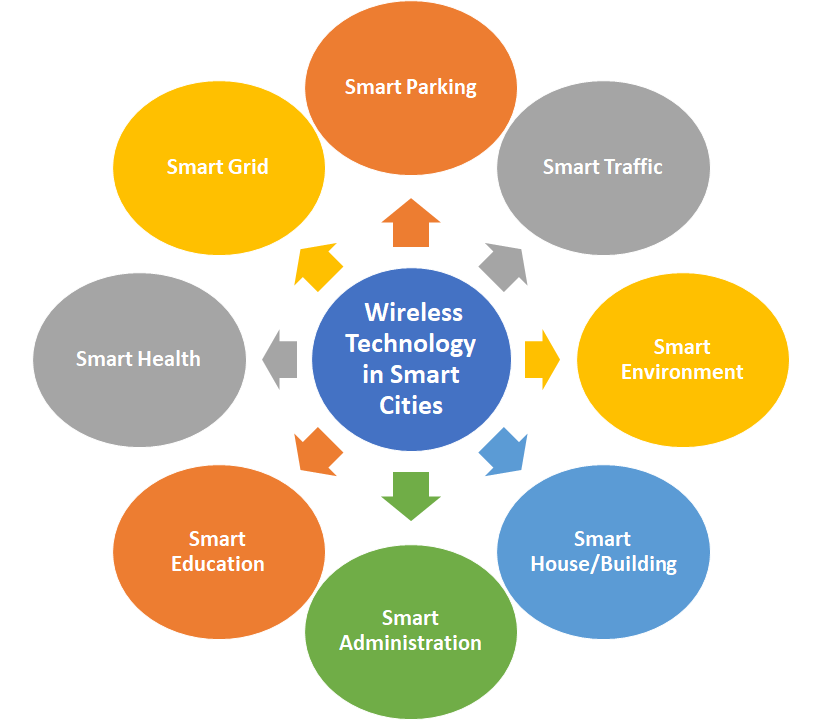
This chapter provides a comprehensive overview of wireless communication technologies related to IoT applications in smart cities and urban planning. In this context, it explains various wireless technologies used in IoT for smart cities and urban planning including Wi-Fi, Zigbee, LoRa, cellular networks (4G/5G), Bluetooth and other emerging standards, including the strengths and weaknesses of each protocol. It covers the fundamental theory of IoT and its architecture. The scope of the chapter covers various IoT applications in urban planning. This work emphasizes on the role of IoT in various aspects of urban planning, including transportation, energy management, environmental monitoring, public safety and infrastructure optimization. It highlights the transformative impact of wireless IoT technologies on urban development. The chapter also discusses various challenges with their advanced solutions in implementing IoT in smart cities.

**Keywords**—Wireless technologies; IoT; Smart Cities; Urban Planning

# INTRODUCTION

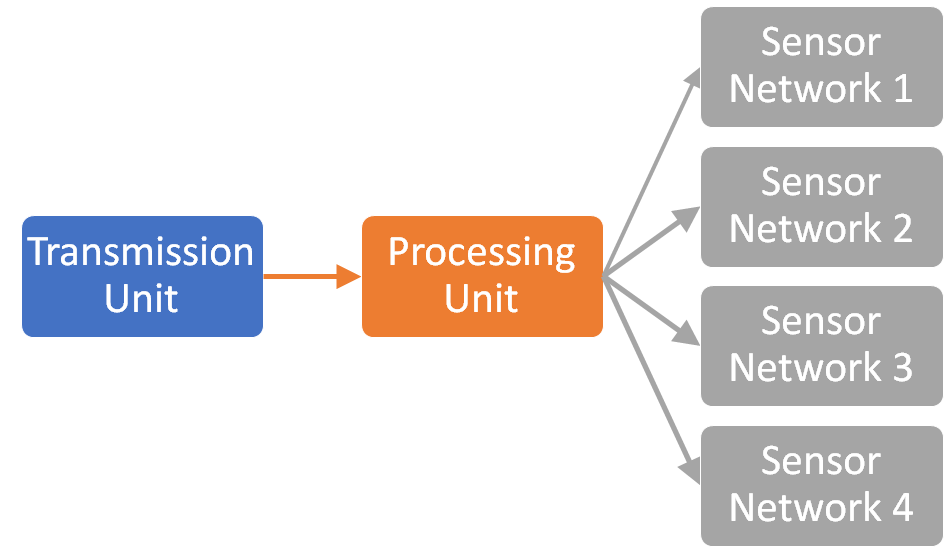
The growth of wireless technologies integrated with the Internet of Things (IoT) and Cloud computing has stimulated the development of smart cities and refurbished urban planning. This is because of faster communication and greater connectivity among the citizens in public spaces. The socio-economic definition of a smart city largely spans across building secure and adequate infrastructure. Efficient health sector and smart education are also some of the important indicators that need constant upgradation. It is these sensitive domains that call for immediate action on wireless sensor networks. The purpose of this study is to educate readers about wireless IoT technologies to provide a clear and accessible explanation of the various wireless technologies involved in IoT applications. The motivation for writing this chapter is to ensure that readers gain a solid understanding of the capabilities and limitations of each technique. In addition, it also shows the role of IoT in urban planning, showing the ways in which IoT promotes urban planning goals such as sustainability, efficiency and quality of life. The purpose of this chapter is to cover the challenges and solutions in this area. Raise awareness of the challenges of implementing wireless IoT in urban environments, offering practical solutions and strategies to address these challenges, encouraging problem solving. It also focuses on an overview of future trends. Section II of the chapter consists of the Wireless technologies in IoT and urban planning, section III covers the IoT Fundamentals and Architecture in Smart Cities, section IV focuses on the IoT Applications in Urban Planning, section V deals with the Challenges in Implementation of IoT (Internet of Things) in smart cities and urban planning with the respective solutions, section VI discusses about advanced solutions and innovations, section VII focuses on future trends and development of wireless technology and finally section VIII brings out the conclusion of the work.

Wireless technologies are the backbone of smart cities. Building a robust and high-speed wireless network is a quintessential step towards modern urban planning. A smart city is defined as the convergence of IOT and AI techniques built over wireless technologies. Wireless technologies have presented themselves as a solution to the rapid growth of devices that are connected to the network as well as the increasing demand of services that allow monitoring cities. IoT is gaining rapid popularity and it is being utilized for transport, health, environment, animal monitoring and smart metering applications [4,5]. Wireless technologies are varied and their utilization should be considered depending on the application. Some applications of wireless technology in smart cities are shown in Fig.1. Traffic type, distance, energy consumption or number of nodes are some of the factors that should be considered when deciding how to transmit the gathered data. Wireless Sensor Networks (WSNs) are discussed in the reported works with the approach being dependent on transmission, processing or the network itself which is shown in Fig.2. These networks are being employed all over the world as a low-cost and low-energy consuming method to provide a communication mechanism [6]. Wireless networks play a significant role at the time of first responders in the field operations. For emergency medical service, broadband data rate is required. This application highlights the sensitivity of an efficient wireless network [1]. Various algorithms are also reported in the past that act as a pre-encoder in the wireless surveillance systems. These applications require a trade-off between complexity of the coding modules and accurate object detection [2]. At the same time, the wireless video surveillance systems (WVSS) are highly susceptible to cyber- attacks. IoT-fuzzy inference system-based jamming detection system for detecting the presence of jamming [cited]. The efficiency of these proposed models is compared in detecting jamming signals. For example, for efficient transmission of power in a typical smart city, smart grids are utilized that are tapping the potential of IoT [3]. Utilizing the GPRS (General Packet radio Services) technology, one is able to identify the motion detection and accordingly send the snapshots to the server [4]. Défense artillery like drones and automatic missiles will eventually make IoT the heart of autonomy, which in turn will require ultra-reliable wireless networks.



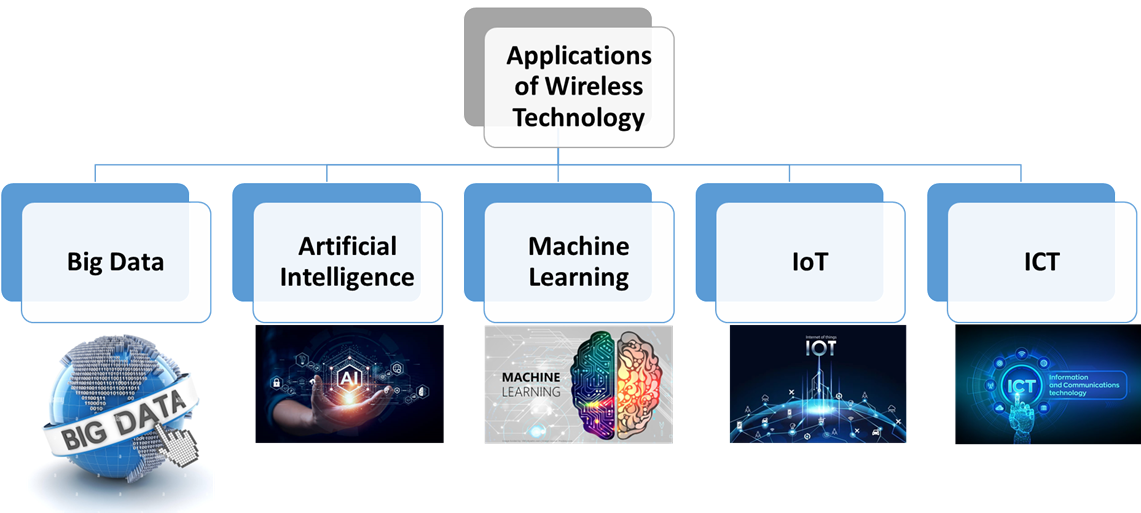
**Fig.1.** Applications of wireless technology in smart cities

Wireless technologies also depend on the environmental conditions and the parameters that are subject to change. For example, the education sector requires shorter ranges and higher bandwidth, while the agriculture domain needs long-distance communication [5]. The recent standards use IEEE 802.15.1 for the short-range wireless communication and low cost, but, at the cost of lower reliability and lower data rates [6]. Whereas, WiMax is employed for long distance communication. The sensors used in the smart cities store and process the acquired data to the cloud platforms. Even they require efficient and intelligent wireless services for the smooth flow of sensitive information [7]. Various IoT protocols use different wireless technologies depending on the usage in the real-world. Be it home automation, industrial automation or health care services. IoT networking technologies are also employed depending on the IoT architecture. For example, network layer encapsulation protocol uses Zigbee IP, while the data link layer protocol uses IEEE 802.15.4e [8].



**Fig.2.** General diagram of Wireless sensor networks

To build intelligent, adaptable and secure workplaces, wireless technologies, however efficient, are still in dire need of technological advancements like ICT and Artificial Intelligence and Machine Learning and Big Data Analytics, shown in Fig.3. The ML algorithms for communications should dynamically adapt to learn complex models that underlie wireless networks and devices. Rigorous research is underway for developing light-weight ML algorithms, especially deep learning models, for embedded systems [9]. An important application of AI and ML is to exploit big data analytics to enhance situational awareness and overall network operation. Herein, AI will provide the wireless network with the ability to parse through massive amounts of data, generated from multiple sources that range from wireless channel measurements and sensor readings to drones and surveillance images, in order to create a comprehensive map of a large number of devices within the network [10]. Data aggregation algorithm based on the Markov chain is used to resend the data after it fails to transmit the first time. This rectifies the issues that the sensor faces in an unreliable communication environment due to information transmission failure. The experimental results show that the system can realize information sharing, exchange and fusion between various sensing subsystems, solve the previous information island phenomenon and meet the actual needs of smart cities [11]. Moreover, the abuse of wireless technologies may derive in some domains. In the context of AI for IoT security, there will always be a challenge to generate high quality training data sets, keeping in account the large number of devices that are continuously generating large volumes of data. For the many challenges seen in the globally optimized network, there are reported works that account for localized IOT based AI yielding benefits such as low bandwidth and latency issues [12]. Apple’s Bluetooth feature of Live in, although comes with many unique advantages. However, it has the ability to listen to the sounds picked up by the phone. There are ample reports regarding hidden wireless cameras whose data can be recorded and directly accessed via smartphones. There is still limited research discussing the efficacy of detection tools to find the hidden wireless devices [13]. Rapid advancements in the field of emerging IoT techniques equally require attention towards IoT security parameters such as data authentication, protection and scalability. Hacking techniques such as Man in the middle attack, placing the attacker's device between the target IoT device and the intended receiver, this attack can be carried out in an IoT system, giving the attacker access to the communication between these two devices. Apart from this, Malware and Distributed Denial of Services are also some of the challenges faced by IoT security [14].



**Fig.3.** Applications of Wireless Technology

Since wireless transmissions are broadcast, the data being transferred is vulnerable to eavesdropping. For the secure data transition, new threats are motivating the organizations to secure not only their office environments but also individual employees working from home during the pandemic. This has caused maintaining cyber security costly and challenging, especially for smaller firms. A review paper recently listed the major security and privacy challenges incurred by the existing wireless networks [15]. Efficient routing protocols have been designed in order to enhance the efficiency with which the packets are being transmitted. Shanthi et al., have proposed a multi-link routing protocol combined with blowfish mode, so as to create a safe transmission of private data to travel among different sensor nodes. The proposed protocol designs are shown to have achieved better performance metrics in terms of data transfer rate, power consumption and latency [16]. Among the authentication protocols, lightweight authentication protocols, key management protocols as well as broadcast authentication protocols have the advantage of reduced computation overhead and minimum memory utilization, when applied to various applications, as listed by S. Raja Rajeswari and V. Seenivasagam [17].

The following technical research has to be enhanced in order to further advance the field of intelligent city information systems study: (1) System for the Internet of Things; (2) Information fusion from several sensors; (3) Sensing technology with intelligence; (4) Industry 4.05 Internet +. We think that in the future, smart cities will be much smarter and more efficient, as they are already steadily improving our lives [11]. Laser Power Transmission (LPT) provides increased safety, high efficiency, and contactless transmission. With the use of this technology, energy transmission efficiency could be greatly increased, energy loss could be decreased, and pollution to the environment could be reduced. Furthermore, LPT can give wireless power to robots, aerospace vehicles, and mobile devices, improving the lifespan and dependability of these systems. Here, this cutting-edge technology has the potential to completely transform the transmission and use of power, leading to significant advancements for the energy industry in the future [18]. Additionally, there is an equal need to develop eco-friendly and sustainable IoT. Various potential solutions towards building a “green IoT” have been listed by Alsharif et al. The energy-aware routing protocol, or EARP, is a "smart" routing technique intended for Internet of Things networks that possess the ability to harvest energy. Based on the energy availability and network characteristics of individual nodes, EARP uses a decentralized technique to dynamically modify network paths. Another illustration is the e-traffic-aware energy-efficient routing (TEER) protocol, which is intended for Internet of Things networks with constrained energy supplies. In order to dynamically modify network paths in response to traffic patterns and energy availability, TEER employs a centralized methodology [19].

# Wireless technologies in IoT and urban planning

Wireless technologies play a crucial role in facilitating Internet of Things (IoT) applications in smart cities and urban planning. These technologies provide the connectivity infrastructure necessary for IoT devices and sensors to communicate, share data, and contribute to the development of intelligent urban environments. The most popularly used wireless technologies in the domain of IoT and urban planning are shown in Fig.4.

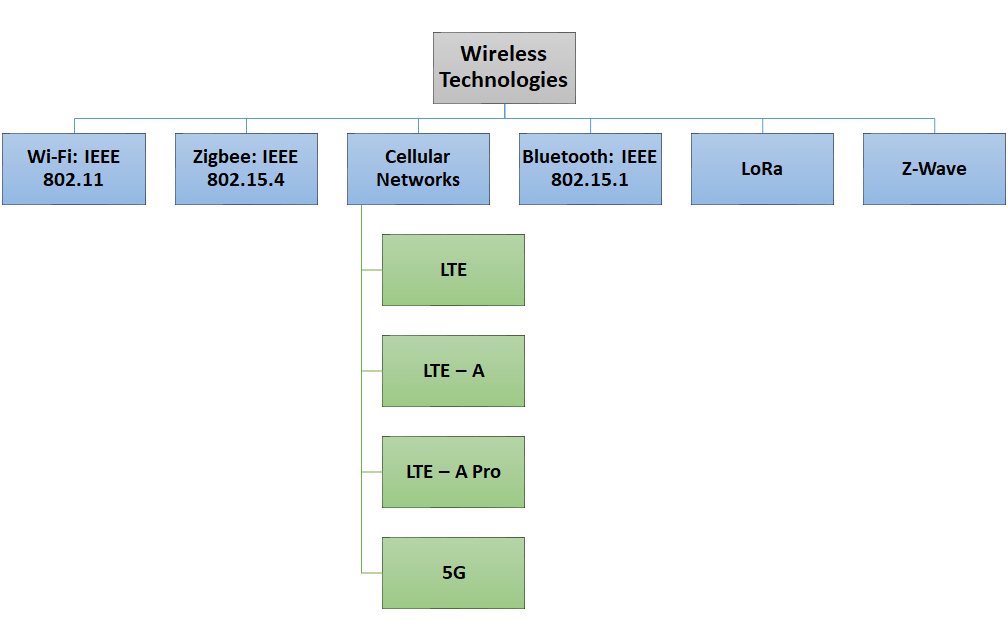


Fig.4. Types of wireless technologies used in IoT and urban planning

1. **Wi-Fi: IEEE 802.11:**

WiFi standards are the most employed for domestic and entrepreneurial environments to provide internet access to countless devices. It is also being employed to provide free internet access to citizens by deploying access points all over the city. All types of data can be transmitted with WiFi, although earlier versions of the standard may have difficulties transmitting high quality multimedia traffic. With the advent of wireless technologies and its new standards, the bit rates for IEEE 802.11 have been increasing. For instance in case of wireless standard 802.15.4, it is only 250 kbps while for 802.11AD it is 7 Mbps. Therefore, it is convenient for the users to move when connecting to other access points of the network without any troubles. The challenges in this technology are that the WiFi connections are less stable than wired ones, the service radius is limited, and it presents high signal attenuation [20]. WiFi radius has a medium range where the indoor coverage area ranges 20 to70 meters while the outdoor radius is in the range of 100 to 250 mtr. So within these ranges only the devices can pull away. The frequency band for all the WiFi standards varies from 2.4 GHz to 5 GHz. Between the standards IEEE 802.11a/b/n/g, IEEE 802.11b has a stronger signal for long distances. IEEE 802.11b and IEEE 802.11n are the better ones for close ranges [21,22]. It can be specially indicated for the governance, infrastructure, economy and people dimensions of a Smart City. The employed frequency bands are unlicensed, so precautions should be taken when designing the network. Interferences may detriment the Quality of Service (QoS) of the system being deployed.

1. **Zigbee: IEEE 802.15.4/ ZigBee:**

The motive behind making this working group was to standardize WPAN in the year 2003[23]. The Purpose of this wireless technology is to offer communication between numerous devices within an operating range of 10 meters at the expense of minimal power consumption with small size and low cost. The biggest advantage is that it can work for devices that need a battery life of several months or years and do not need high data transfer rates. In 2006 and 2011 the revisions IEEE 802.15.4-2006 and IEEE 802.15.4-2011 were introduced [24]. The latest one defines 12 PHY options where the 2450 direct-sequence spread spectrum (DSSS) is the most employed nowadays. Various types of personal area networks (PAN) are supported by IEEE 802.15.4 such as beacon-enabled PAN and non beacon-enabled PAN. Non Beacon-enabled PANs use Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) as the channel access mechanism while beacon-enabled PANs employ the slotted CSMA-CA mechanism.

The ZigBee technology is a standard that finds great similarities to IEEE 802.15.4. It explains the communication in the third level of the OSI (Open System Interconnection) model instead of describing the communication of the second level, as IEEE 802.15.4 does. Two types of devices can be operated in ZigBee that are: Full-function device (FFD) and reduced-function device (RFD). The FFD can operate as a PAN coordinator that can communicate with both FFD and RFD whereas RFD can only communicate with FFD and is suitable for simple activities such as light switches or passive sensors. A FFD can create its own network becoming the PAN coordinator and selecting a PAN ID in order to avoid conflicts with other PANs in the same area. Star topology, peer-to-peer topology and cluster topology are the three types of topologies that can be implemented with ZigBee.

1. **Cellular Networks (4G/5G):**

Fourth generation of cellular wireless standards is abbreviated to 4G. It is superseded to 2G and 3G families of mobile standards. 4G technology improves the prevailing communication networks by conveying a complete and reliable solution based on IP such as voice, data and multimedia. This system can be serviced to subscribers on every time and everywhere and at quite higher data rates as related to previous generations. Applications that are being made to use a 4G network include: Digital Video Broadcasting (DVB), Multimedia Messaging Service (MMS), High Definition TV and mobile TV. 4G can provide 100 Mb per seconds for high mobility like receiving the service from a moving car or train. 1 Gb per seconds for low mobility like when walking (pedestrian) [25].

* **LTE**

LTE is 3GPP radio interface. It is based on GSM/EDGE and UMTS/HSPA mobile network technologies, and it provides an increase to both capacity and data speed using new techniques for modulation. The carrier bandwidths are 1.4 MHz to 20 MHz and it supports both time-division and frequency division duplexing. Therefore, it provides peak download rates of 300 megabits per second and 75 megabits per second for upload rates, delay before a transfer of data begins following is less than five milliseconds. This technology is IP-based network architecture, which allows for seamless handoff for voice and data to older model cell towers. LTE offers average download and upload speed of 77.8 Mbps and 26.9 Mbps [25,26].

* **LTE-A**

The 3GPP Long-Term Evolution-Advanced (LTE-A) offers massive improvements over previous mobile network technologies such as Universal Mobile Telecommunications System (UMTS) and High-Speed Packet Access (HSPA) by introducing a novel physical (PHY) layer and reforming the core network (CN) [27]. LTE Advanced standard provides a heavy enhancement of the Long Term Evolution (LTE) standard. LTE-Advanced can achieve data download rates to three Gb per seconds and upload rates as high as 1.5 Gb per seconds. By the comparison, LTE is provided 300 Mb per seconds for downloads and 75 Mb per seconds for uploads. LTE-Advanced also includes new transmission protocols and multiple-antenna schemes that enable smoother hand over between different regions of cells, increase data throughput at the level of cell edges, and more bits per second into each hertz of spectrum. Consequently, the result can be higher network capacity, more consistent connections, and cheaper data [25,28].

* **LTE-A Pro**

It is a 3GPP release 13. Also known as LTE-Advanced Pro, which provided 4.5G, 4.5G Pro, 4.9G, Pre-5G networks system. The LTE-A Pro is an evolution of Long Term Evolution (LTE), it is able to function at speeds up to Gbps. This release incorporated numerous new technologies that may be utilized in the 5G network system standard, including: Massive MIMO, 256 Quadrature amplitude modulation, LTE-Unlicensed and LTE Internet of Things. This technology provides a wide range of enhancements of the challenges in existing services in addition to new and emerging use cases. Moreover, the major advances achieved in Release 13 includes Machine-Type-Communication (MTC) enhancements, carrier aggregation enhancements, Narrowband-IoT Low Power Wide Area (NB-IoT LPWA), public safety features, interworking with Wi-Fi, single cell-point to multi-point, licensed assisted access, 3D/FD-MIMO, indoor positioning and work on latency reduction [29,30].

* **5G**

The 5th generation wireless system is abbreviated to 5G. It continues on the path of LTE, with a massive increase in the demand of the mobile users, 4G networks will be easily changed to 5G with the advanced access technology named Beam Division Multiple Access (BDMA) and Filter Bank multi carrier (FBMC) multiple access. The concept behind BDMA technique considers that it serves multiple mobile users simultaneously. In this mechanism, an orthogonal beam allocates resources to each mobile based station and the BDMA technique divides the antenna beam according to the location of the mobile stations to provide multiple accesses to the base stations. This has led to an increase in the capacity of 5th generation wireless mobile networks. The 5G standard improves the network system and aims to provide a higher capacity than 4G networks, which allows massive connections of mobile users to base stations. It also carries out machine-to-machine, reliable, and density machine communications. The characteristics of 5G provides high data rates, which allows tens of megabits per second for tens of thousands of users, data rates of hundred megabits per second for metropolitan areas networks, one Gb per second can be provided simultaneously to numerous mobile users on the same connection point and, it can supply several hundreds of thousands of simultaneous connections for wireless network sensors [27, 30]. The existing spectrum of LTE is only 1 to 6 GHz while for mobile network services between both LTE and 5G technologies, it varies from 1 to 100 GHz for serving various applications.

1. **Bluetooth and BLE (Bluetooth Low Energy): IEEE 802.15.1 WPAN/Bluetooth:**

The standard IEEE 802.15.1 depicts the operation of WPAN. This standard is based on the technology created by the Bluetooth Special Interest Group. WPANs transmit information over short distances without requiring a big infrastructure, sometimes not being necessary at all, or a connection to the internet. Although it is not possible to communicate between IEEE 802.15.1 devices and IEEE 802.11 devices, some mechanisms were developed in order to allow the coexistence of both technologies [31]. A group of devices that share a physical radio channel are synchronized employing a common clock. One of the devices has the role of the master while the rest are the slaves. This topology is called piconet. In order to avoid interference, it utilizes a frequency hop transceiver. Some of the available frequencies for the hopping pattern are excluded to avoid interferences with static systems. IEEE 802.15.1 is a protocol for low power consumption short-range wireless communications [32]. It was designed to replace wired computer peripherals with wireless ones. Bluetooth can have two types of topologies, piconet and scatternet. The piconet topology was defined above. A scatternet is composed of several piconets that overlap in time and space. A device can be part of several piconets simultaneously but it can only be mastered in one of them. Up to 7 slaves can be part of the same piconet, although there can be devices on standby [33]. The number of slaves that can be put in park mode is 255. In the range of 10m up to 20 different piconets can be established. Only one packet at a time can be transmitted between slave and master.

The advantages of IEEE 802.15.1 are its low cost, mobility and that a device can join or leave the network dynamically [34]. The disadvantages include lower reliability, higher power consumption, security threats and lower data rates. Bluetooth is the proprietary solution of this standard. Version 1.0 and 1.1 were very problematic. Version 1.1 was adopted in 2002 as the IEEE 802.15.1 standard [35]. Bluetooth 1.2 adds the Adaptive Frequency Hopping (AFH) to the previous version and the maximum data transmission rate is 751 kb/s. It was adopted as the IEEE 802.15.1-2005 standard. Bluetooth 2.0 (2004) enhanced the data rate to 2.1 Mbps. Bluetooth 2.1 (2007) introduced secure simple pairing (SSP). It employs a sniff sub rating to reduce power consumption in the low-power mode. Bluetooth 3.0 (2009) improves data transfer speeds to 24 Mbps. Bluetooth 4.0 (2010) improves data transmission rates and security. The power consumption is greatly reduced. It does not allow devices to be part of several piconets as a slave device thus, the network topology is the star topology [36]. In Bluetooth 4.1 (2013), a slave is allowed to be connected to several piconets at the same time. Moreover, the device is able to take the role of slave in some intervals and master in others. Thus, the topology options expand. In Bluetooth 4.2 (2014) the internet connectivity, security and throughput are improved. Finally, in Bluetooth 5.0 (2016) range, data rate and advertising channel functionality are improved.

1. **LoRa (Long Range):**

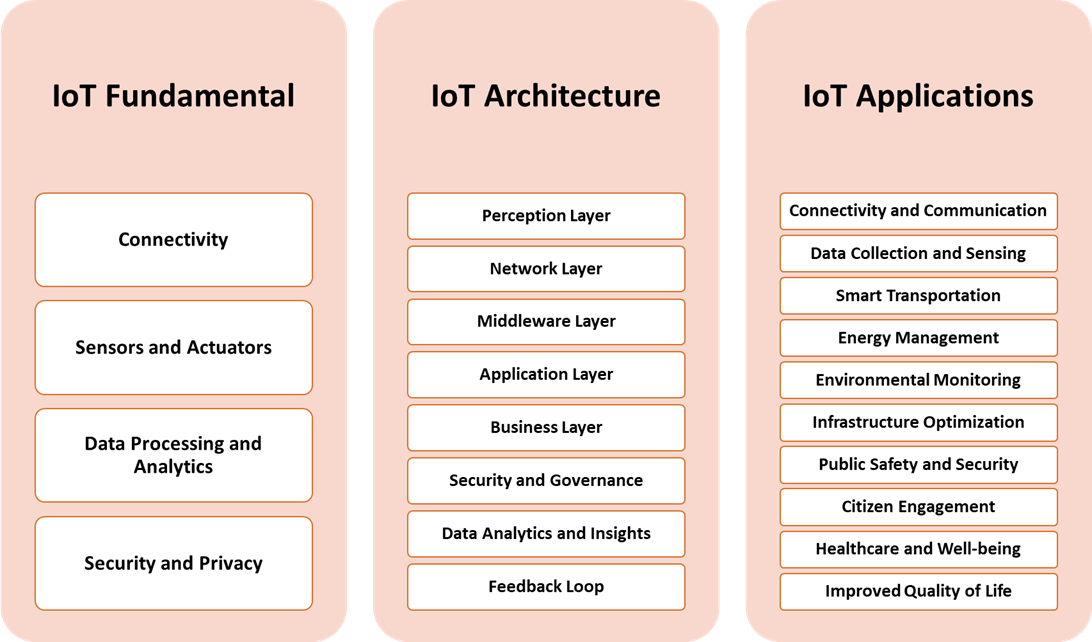
LoRa stands for Long Range and it is a proprietary technology. This spread modulation scheme was developed in 1940 and employs the unlicensed band below 1 GHz. Its advantages are its low cost, its robustness from interferences and its long-range transmissions. It is being employed in IoT solutions [37, 38]. The physical layer of LoRa modulates the signal in the SUB-GHz ISM band. It is using a proprietary spread spectrum technique, which is developed by Semtech Corporation. The network architecture of LoRa provides a variety of advantages. LoRa utilizes from the 868MHz to the 915 MHz ISM band. This band has a very wide coverage range, about 5 Km in urban areas and 15 Km in suburban areas. Therefore, LoRa is easy to deploy due to its network architecture and its gateway is designed to service thousands of end devices. The data rate transmission can be from 0.3 kbps to 27 Kbps for 125 KHz of bandwidth. It is widely used for M2M of IoT applications. Thus, LoRa modulation has constant envelope modulation which is similar to the FSK modulation type. LoRa technology provides low power with high efficiency at a low cost.

1. **Z-Wave:**

“Z-wave” (Z-Wave Alliance ZAD12837 / ITU-T G.9959) may not be a name you hear every day, but is proving to be one of the most popular wireless technologies for IoT products. [Z-wave is a special protocol used specifically for home automation and connectivity.](http://www.z-wave.com/) Perhaps the most famous example of Z-wave technology right now is Amazon’s Echo, which has revolutionized the way tech-savvy consumers shop and use media. There are over 2000 Z-wave products on the market, allowing connectivity for household products ranging from smart garage door openers, fire alarms, fans and blinds, to remote-controlled front door locks and thermostats. Z-wave systems generally have a range up to 30 meters, and operate in the frequency band below 1 GHz.

**Table 1: Strengths and Weaknesses of Each Wireless Technology**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Characteristics** | **Wi-Fi (IEEE 802.11)** | **Bluetooth** | **Zigbee** | **Mobile Networks (4G LTE and 5G)** | **Z-Wave** | **LoRa (Long Range)** |
| Power Consumption | Moderate to High, especially during data transmission | Low to Moderate, especially in Bluetooth Low Energy (BLE) versions. | Low, especially in low-power sleep modes. | Moderate to High, especially during data-intensive activities. | Low to Moderate, especially in low-power sleep modes. | Low, especially in low-power, wide-area networks. |
| Range | Moderate to High, typically within a hundred meters | Short to Moderate, typically within tens of meters. | Short to Moderate, typically within tens of meters. | Long, providing wide-area coverage. | short to Moderate, typically within tens of meters. | Long, typically several kilometers. |
| Scalability | Good scalability, suitable for environments with a large number of devices. | Moderate scalability, suitable for personal area networks and applications with a moderate number of devices. | High scalability, suitable for large-scale sensor networks and home automation. | High scalability, suitable for wide-scale deployments. | High scalability, suitable for home automation and smart building applications. | High scalability, suitable for large-scale deployments covering extensive areas. |
| Data Rates | Up to several Gbps (Wi-Fi 6) | Up to 2 Mbps (Bluetooth 5.0) | Up to 250 kbps | Up to several hundred Mbps (4G LTE), potentially several Gbps (5G) | Up to 100 kbps | Typically ranges from 0.3 kbps to 50 kbps, depending on spreading factor and modulation |
| Suitability | Well-suited for applications with higher data rates, such as video streaming, and in environments with reliable power sources | Ideal for low-power, short-range applications such as wearables, health monitoring, and smart home devices. | Well-suited for low-power, low-data-rate applications in home automation, industrial automation, and smart lighting | Ideal for applications requiring high data rates, mobility, and connectivity over long distances, such as smart cities and mobile IoT devices | Well-suited for low-power, low-data-rate applications in smart home and building automation. | Ideal for low-power, long-range applications such as smart agriculture, environmental |



**Fig.5.** IoT fundamentals, its architecture and applications

# IoT Fundamentals and Architecture in Smart Cities

In the development of a smart city, the Internet of Things (IoT) behaves as a technological backbone that enables the seamless integration of diverse devices, systems, and services to enhance the life of urban citizens. The study of fundamentals and architecture of IoT is necessary to understand the basic functioning of IoT and its role in the formation of the smart cities in urban planning. Figure 5 shows the IoT fundamentals, its architecture and applications.

## **IoT Fundamentals:**

## **Connectivity:**

IoT devices depend on various wireless technologies, such as WiFi, Bluetooth, Zigbee, and cellular networks, for connectivity. To accommodate battery-operated devices, low-power communication protocols like MQTT and CoAP are commonly used.

## **Sensors and Actuators:**

IoT employs a network of sensors to collect data on environmental conditions, traffic flow, energy consumption, and more. These sensors collect the data from the physical world. The actuators are the devices that are capable of performing actions based on data received, such as adjusting streetlights or controlling irrigation systems.

## **Data Processing and Analytics:**

Once the data is collected, it is processed at the edge of the network to reduces latency and enable real-time decision-making.This is called Edge Computing. With the help of cloud computing for which the centralized cloud platforms are utilized, the data is stored and complex analytics, and machine learning applications.

## **Security and Privacy:**

To secure the data during transmission and storage the encryption on the data is performed. Authentication is another important aspect so as to verify the identity of devices and users within the IoT ecosystem. To ensure the protection of personal and sensitive data various privacy measures are considered.

## **IoT Architecture in Smart Cities:**

## **Perception Layer:**

The function of the Perception Layer is to collect data from the physical environment and perform actions based on the received information. Within the domain of this layer, the gateways and edge computing devices process and filter data before transmission.

## **Network Layer:**

This is the next layer in the ToT architecture after the Perception Layer. It is responsible for providing Connectivity through wireless networks facilitating communication between devices. For this the standardized set of communication protocols ensure interoperability. Protocols like MQTT and CoAP are commonly used. Interconnected devices create robust mesh networks for improved coverage.

## **Middleware Layer:**

The middleware Layer processes and manages data, transforming raw sensor data into actionable insights. It allows device management by encompassing tasks such as provisioning, configuring, and updating IoT devices.

## **Application Layer:**

This layer offers smart city applications for which a large number of the implementations are there varying from traffic management and waste monitoring to healthcare and public safety. It also provides the user interfaces where the dashboards and applications provide users with real-time information and control over connected services.

## **Business Layer:**

This layer handles the integration with urban planning by aligning IoT implementations with city planning goals. For the monetization modeling it explores business models for sustainable IoT deployments in smart cities.

## **Security and Governance:**

This layer facilitates access control by regulating access to devices and data. The blockchain technology is incorporated to ensure secure, transparent, and tamper-proof transactions. It also adheres to data protection and privacy regulations.

## **Data Analytics and Insights:**

For the data analytics the layer offers big data analysis by processing large volumes of data for trend analysis and pattern recognition. The layer is also responsible for predictive modeling in which the forecasting of the future events is based on historical data.

## **Feedback Loop:**

It has the closed-loop systems where feedback from IoT applications leads to dynamic adjustments and improvements. In order to seek continuous improvement, iterative processes for refining and optimizing smart city solutions is followed.

# IoT Applications in Urban Planning

## **Connectivity and Communication:**

Wireless technologies, such as Wi-Fi, Zigbee, and LoRa, enable seamless connectivity among a myriad of IoT devices spread across a city. It also offers real-time communication where wireless communication protocols facilitate real-time data exchange between sensors, devices, and central systems.

## **Data Collection and Sensing:**

Wireless-enabled sensors gather data on various urban parameters, including air quality, traffic flow, energy consumption, and more. The wireless networks not only provide a wide coverage but with the flexibility to deploy sensors over a large geographical area, covering diverse aspects of urban life.

## **Smart Transportation:**

Wireless technologies support intelligent transportation systems (ITS) that enhance traffic flow and reduce congestion. Wireless communication between vehicles and infrastructure ensures that the traffic optimization is achieved with safety.

## **Energy Management:**

The smart grids are used for wireless networks to facilitate communication between devices ensuring energy optimization, distribution and consumption. Wireless technologies allow remote monitoring and control of energy infrastructure, contributing to efficiency and sustainability.

## **Environmental Monitoring:**

Wireless sensor networks are exploited to monitor environmental parameters such as air and water quality, noise levels, and temperature. For environmental hazards, the early warning systems provide rapid data transmission.

## **Infrastructure Optimization:**

Wireless connectivity in IoT for smart cities and urban planning, allows for real-time monitoring of critical infrastructure, such as bridges, buildings, and utilities. It also offers predictive maintenance by acquiring the data from IoT sensors enabling reduced downtime and improved infrastructure resilience.

## **Public Safety and Security:**

Wireless technologies support surveillance cameras and IoT-enabled security systems for public safety. Along with this the emergency response facility caters to real-time data transmission to enhance emergency services to aid crisis management.

## **Citizen Engagement:**

Wireless connectivity enables citizens to engage through mobile applications for reporting issues, accessing services, and providing feedback. Community Participation: Wireless technologies foster citizen involvement in urban planning and decision-making processes.

## **Healthcare and Well-being:**

Wireless IoT applications contribute to remote healthcare monitoring and emergency response systems. Apart from this it enables wearable devices with wireless connectivity to collect health data, contributing to personalized well-being services.

## **Improved Quality of Life:**

Wireless technologies optimize service delivery, contributing to a more efficient and livable urban environment. Overall, wireless-enabled IoT applications enhance the quality of life for residents by improving services, sustainability, and resource management.

In essence, wireless technologies form the backbone of IoT in smart cities, enabling the continuous flow of data and communication needed for intelligent decision-making, efficient resource management, and the creation of more sustainable and livable urban spaces.

# Challenges in Implementation with respective mitigations

The implementation of IoT (Internet of Things) in smart cities and urban planning comes with various challenges that need to be addressed to ensure a successful and secure deployment. Some of the key challenges include:

### **Scalability Issues:**

With the increment and growth of IoT devices, managing and scaling the infrastructure becomes a significant challenge. It may result in the poor handling of a growing number of devices and may lead in performance degradation and reduced system responsiveness. To mitigate this challenge, the robust architecture design, use of scalable cloud platforms, and optimization of communication protocols can be exploited.

### **Security Concerns:**

The IoT devices are vulnerable to security threats, including unauthorized access, data breaches, and malicious attacks. This may lead to security breaches with compromised data integrity, privacy violations, and disruptions in critical services. By implementing robust encryption, authentication mechanisms, regular security audits, and keeping devices and software up-to-date can enhance security and mitigate these issues.

### **Interoperability Challenges:**

IoT ecosystems largely consist of devices from various manufacturers using different communication protocols and standards, leading to interoperability challenges. Here the possible implication could hinder seamless communication and integration of devices leading to limited effectiveness of the IoT system. To mitigate this challenge, the adoption of common standards, development of interoperability frameworks, and collaboration between industry stakeholders can be useful.

### **Data Privacy and Ethics:**

Now a-days a bulk of personal data is available on the cloud. Therefore, the collection, storing, and processing of vast amounts of data from IoT devices raise concerns about individual’s privacy and the ethical use of data. As a consequence of it there is a huge possibility of mishandling of sensitive data that can erode public trust and lead to legal and regulatory challenges. In order to handle this implementation, privacy-by-design principles, transparent data handling practices, and adherence to data protection regulations can be done.

### **Reliability and Resilience:**

IoT systems must be reliable and resilient to handle disruptions, outages, or failures in devices or network connectivity. Any unreliability of the systems can result in service interruptions and can negatively impact critical applications. To handle this problem the redundancy, failover mechanisms, and proactive maintenance can be trusted.

### **Power Consumption and Battery Life:**

Many of the IoT devices operate on battery power, and optimizing energy consumption is crucial for extended battery life. The short battery life can lead to frequent replacements and increased maintenance costs. In order to overcome this problem, the low-power design, energy-efficient communication protocols, and the use of energy harvesting technologies can be utilized.

### **Cost Considerations:**

The initial deployment and ongoing maintenance costs of IoT infrastructure can be significant. So the budget constraints may hinder the widespread adoption of IoT solutions in smart cities. The possible mitigation techniques could be cost-benefit analyses, public-private partnerships, and gradual, phased deployments.

### **Regulatory and Compliance Issues:**

Compliance with various regulations and standards, especially in areas like data protection, can pose challenges. Therefore, the non-compliance may lead to legal issues and hinder the acceptance of IoT solutions. Thorough understanding of regulatory requirements, proactive compliance measures, and engagement with regulatory authorities, the regulatory challenges can be addressed.

### **Lack of Skill Sets:**

The complexity of IoT systems requires skilled professionals for design, implementation, and maintenance. So, the shortages in skilled personnel can lead to challenges in effectively managing IoT deployments. In order to meet the challenges, the training programs, educational initiatives, and collaboration with academic institutions are helpful to build a skilled workforce.

Addressing these challenges requires a multi-faceted approach involving technology, policy, and collaboration among stakeholders. By proactively addressing scalability, security, interoperability, and other challenges, smart cities can maximize the benefits of IoT for improved urban living.

# Advanced Solutions and Innovations

To overcome the challenges in implementing IoT in smart cities and urban planning, various solutions and innovations have been developed. Here are some key advancements in security measures, interoperability standards, and computing paradigms like edge computing and fog computing:

### **Security Concerns:**

These concerns can be addressed by the three advanced solutions that are, blockchain technology, zero trust architecture and AI-driven security analytics. The integration of blockchain for secure and transparent transactions ensures data integrity and prevents unauthorized access. The zero trust architecture adopts a zero-trust model, where devices and users are continuously authenticated and verified to enhance overall security. The AI-driven security analytics utilizes artificial intelligence to analyze patterns and anomalies in real-time, identifying potential security threats.

### **Interoperability Challenges:**

The interoperability challenges are addressed by techniques such as open standards and protocols, IoT platforms and industry alliances. The open standards and protocols increase adoption of open standards and communication protocols to enhance interoperability among diverse IoT devices. The IoT platforms offer the development of comprehensive IoT platforms that provide a common framework for integrating and managing diverse devices and applications. Finally, the industry alliances cater to the collaboration among industry stakeholders to establish common standards and ensure compatibility across different IoT ecosystems.

### **Edge Computing:**

For edge computing, three major techniques are deployed that include distributed edge architecture, edge analytics and edge security. The distributed edge architecture technique pushes the processing closer to the data source, reducing latency and enhancing real-time decision-making. The edge analytics performs data analytics at the edge to filter and process relevant information locally, minimizing the need for extensive data transfer. The edge security is used to implement security measures directly at the edge to protect data at its source.

### **Data Privacy and Ethics:**

Data privacy and ethics usehomomorphic encryption and differential privacy approaches. The homomorphic encryption allows computations on encrypted data without decrypting it, ensuring privacy in data processing while the differential privacy technique introduces noise to individual data points to protect user privacy while still allowing aggregate analysis.

### **Fog Computing:**

To accomplish the fog computing technique, various new approaches are adopted such as fog-to-cloud continuum, proximity-based services and resource orchestration. The fog-to-cloud continuum combines fog computing (distributed edge computing) with cloud resources to create a continuum for data processing and storage. In proximity-based services the utilization of fog computing is there to provide location-based and context-aware services, enhancing user experiences. In the third technique which is the resource orchestration, the dynamic allocation of computing resources across fog and cloud layers based on workload demands is done.

### **Secure Device Onboarding:**

The secure device onboarding is done by using different techniques such as device identity management and device authentication are exercised. The device identity management is used to implement robust identity management for IoT devices to ensure secure onboarding while device authentication offers leveraging advanced authentication mechanisms, including biometrics and multi-factor authentication, to enhance device security.

### **AI-driven Threat Detection:**

The AI-driven threat detection can be done by behavioral analytics where the machine learning algorithms are used to analyze and identify abnormal behavior patterns, helping detect security threats. The other way to resolve this issue is the anomaly detection in which the AI-driven anomaly detection is employed to identify deviations from normal behavior and potential security breaches.

### **Self-Healing Systems:**

The Self-Healing Systems include autonomous security measures by implementing self-healing capabilities in IoT systems to automatically respond to and mitigate security threats. The self healing can also be catered by using predictive maintenance which uses AI and machine learning to predict potential security vulnerabilities.

### **Standardized Data Models:**

The standardized data models include semantic interoperability and data description standards. The semantic interoperability establishes standardized data models and semantic interoperability to ensure consistent and meaningful communication among diverse devices on the other hand the data description standards defines standardized metadata and descriptions for IoT data to enhance understanding and compatibility.

### **Edge-to-Cloud Integration:**

The edge-to-cloud integration technology includesseamless data flow and hybrid architectures. The seamless data flow ensures smooth integration and data flow between edge devices and cloud platforms at the same time the hybrid architecture technique implements hybrid architectures that balance computing tasks between edge and cloud resources based on specific requirements.

### **Regulatory Compliance Frameworks:**

For the regulatory compliance and frameworks the adopted methodologies are adherence to standards that develop and adhere to regulatory frameworks and standards to ensure compliance with data protection and privacy regulations. The other method in this regard is transparency and accountability which establishes transparent practices and mechanisms for accountability in handling and securing IoT data.

### **Dynamic Resource Allocation:**

The dynamic resource allocation includes resource-efficient algorithms that develop algorithms that dynamically allocate resources based on real-time demand, optimizing computing resources and energy consumption. The other approach is load balancing that implements effective load balancing mechanisms for distributed computing environments.

### **Secure Device Lifecycle Management:**

To achieve the secure device lifecycle management, an end-to-end Security mechanism is deployed that ensures security measures throughout the entire lifecycle of IoT devices, including manufacturing, deployment, and decommissioning. The device firmware updates are the other technique that implements secure mechanisms for updating device firmware to patch vulnerabilities and enhance security.

Advancements in these areas contribute to building a more secure, interoperable, and efficient IoT ecosystem for smart cities and urban planning. Continuous innovation and collaboration among industry stakeholders are essential to addressing the evolving challenges and ensuring the sustainable growth of IoT in urban environments.

# Future Trends and Developments

The future of IoT in smart cities and urban planning is poised for continued growth and innovation, driven by advancements in technology, evolving urban challenges, and the increasing demand for smarter, more sustainable cities. Several trends and developments are expected to shape the future landscape of IoT in urban environments that is shown in Fig.6:

### **5G Integration:**

The rollout of 5G networks will significantly enhance connectivity, enabling faster data transfer, lower latency, and support for a massive number of devices. Accelerated adoption of IoT applications in smart cities, especially those requiring real-time communication and high data throughput.

### **Edge Computing Maturity:**

Edge computing will mature, becoming more widespread and sophisticated, allowing for more processing at the edge of the network. Improved real-time decision-making, reduced latency, and enhanced overall system efficiency in IoT deployments.



**Fig.6.** Future trends of IoT in smart cities and urban planning

### **AI and Machine Learning Integration:**

Increasing integration of AI and machine learning into IoT systems for advanced analytics, predictive modeling, and automation. Smarter and more adaptive systems capable of learning and evolving, leading to improved resource optimization and decision-making.

### **Digital Twins for Urban Planning:**

The use of digital twins—virtual replicas of physical assets or systems—for comprehensive urban planning and simulation. Enhanced visualization, monitoring, and predictive modeling for urban infrastructure, enabling more informed decision-making.

### **Autonomous Vehicles and Traffic Management:**

Advancements in autonomous vehicle technology and intelligent traffic management systems for safer, more efficient urban mobility. Reduced traffic congestion, improved transportation efficiency, and enhanced safety through automated and connected vehicle systems.

### **Smart Health and Well-being Solutions:**

Expansion of IoT applications in healthcare, including remote patient monitoring, wearable devices, and smart health infrastructure. Improved healthcare accessibility, personalized medicine, and enhanced public health monitoring.

### **Blockchain for Security and Trust:**

Increased adoption of blockchain technology for enhancing security, data integrity, and trust in IoT ecosystems. Strengthened security measures, transparent transactions, and improved trust among stakeholders in smart city environments.

### **Sustainable and Resilient Infrastructure:**

Growing emphasis on IoT solutions for sustainable and resilient urban infrastructure, addressing environmental challenges and climate change. Implementation of IoT-driven solutions for energy efficiency, waste reduction, and sustainable urban development.

### **Augmented Reality (AR) in Urban Services:**

Integration of augmented reality technologies for enhanced citizen engagement, navigation, and interactive urban services. Improved user experiences, increased civic participation, and more intuitive interaction with smart city services.

### **Privacy-Preserving Technologies:**

Continued development and adoption of privacy-preserving technologies, such as homomorphic encryption and federated learning. Enhanced protection of user privacy while still allowing for valuable data analysis and insights.

### **Quantum Computing Impacts:**

Exploring the potential impacts of quantum computing on IoT applications, particularly in solving complex problems and optimizing algorithms. Accelerated data processing, improved encryption methods, and advancements in optimization algorithms.

### **Resilience in the Face of Disasters:**

IoT solutions designed to enhance urban resilience and response during natural disasters and emergencies. Improved early warning systems, efficient evacuation planning, and enhanced disaster response and recovery.

### **Human-Centric Design:**

Emphasis on human-centric design principles to ensure that IoT applications prioritize user experiences, inclusivity, and accessibility. More user-friendly and inclusive smart city solutions that cater to diverse needs and demographics.

### **Regulatory Frameworks and Governance:**

Development of robust regulatory frameworks and governance models to address ethical considerations, data privacy, and security in smart city deployments. Clearer guidelines, increased trust, and responsible implementation of IoT technologies in urban environments.

The future trends in IoT for smart cities reflect a dynamic landscape where technology continues to evolve, and cities strive to become more connected, efficient, and sustainable. As these trends unfold, collaboration among stakeholders, regulatory frameworks, and a focus on ethical considerations will play crucial roles in shaping the successful and responsible implementation of IoT in urban environments.

# Conclusion

The chapter on wireless technologies in IoT and urban planning explores the pivotal role that wireless communication plays in shaping the future of smart cities. The integration of wireless technologies within the Internet of Things (IoT) framework presents a transformative approach to urban planning, enhancing connectivity, efficiency, and the overall quality of life for city residents. The purpose of this chapter was to cover wireless technologies exploited in IoT and urban planning along with the comparison of each technology’s strengths and weaknesses. The IoT fundamentals and architecture in smart cities are considered with the focus on the IoT applications in urban Planning. It included awareness of the challenges of implementing wireless IoT in urban environments along with the practical solutions and strategies to address these challenges. It also focused on an overview of future trends and finally the conclusion of the work.

##### REFERENCES

[1] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, “Survey of wireless communication technologies for public safety,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 2, pp. 619–641, 2014, doi: 10.1109/SURV.2013.082713.00034.

[2] A. Aliouat, N. Kouadria, S. Harize, and M. Maimour, “An Efficient Low Complexity Region-of-Interest Detection for Video Coding in Wireless Visual Surveillance,” *IEEE Access*, vol. 11, no. January, pp. 26793–26806, 2023, doi: 10.1109/ACCESS.2023.3248067.

[3] S. Tanwar, S. Tyagi, and S. Kumar, “The Role of Internet of Things and Smart Grid for the Development of a Smart City,” *Lect. Notes Networks Syst.*, vol. 19, no. September, pp. 23–33, 2018, doi: 10.1007/978-981-10-5523-2\_3.

[4] “J2ME-BASED WIRELESS INTELLIGENT VIDEO SURVEILLANCE SYSTEM USING MOVING OBJECT RECOGNITION,” *Int. J. Multidiscip. Eng. Curr. Res.*, vol. 8, no. 10, 2023.

[5] L. Garcia, J. M. Jiménez, M. Taha, and J. Lloret, “Wireless Technologies for IoT in Smart Cities,” *Netw. Protoc. Algorithms*, vol. 10, no. 1, p. 23, 2018, doi: 10.5296/npa.v10i1.12798.

[6] F. P. ERINA FERRO and ISTI, “Bluetooth and Wi-Fi Wireless Protocols :,” *IEEE Wirel. Commun.*, pp. 1–24, 2004.

[7] D. Kim, Y. Yoon, J. Lee, P. J. Mago, K. Lee, and H. Cho, “Design and Implementation of Smart Buildings: A Review of Current Research Trend,” *Energies*, vol. 15, no. 12, 2022, doi: 10.3390/en15124278.

[8] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, “Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends,” *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018, doi: 10.1155/2018/5349894.

[9] C. Wang *et al.*, “Artificial Intelligence Enabled Wireless Networking for 5G and Beyond : Recent Advances and Future Challenges Artificial Intelligence Enabled Wireless Networking for 5G and Beyond : Recent Advances and Future Challenges,” *IEEE Wirel. Commun.*, vol. 27, no. 1, pp. 16–23, 2020.

[10] M. Chen, U. Challita, W. Saad, and C. Yin, “Machine Learning for Wireless Networks with Artificial Intelligence : A Tutorial Machine Learning for Wireless Networks with Artificial Intelligence : A Tutorial on Neural Networks,” no. October, 2017.

[11] D. Jiang, “The construction of smart city information system based on the Internet of Things and cloud computing,” *Comput. Commun.*, vol. 150, pp. 158–166, 2020, doi: 10.1016/j.comcom.2019.10.035.

[12] I. Ahmad, S. Shahabuddin, T. Kumar, E. Harjula, M. Meisel, and M. Juntti, “Challenges of AI in Wireless Networks for IoT,” *IEEE Ind. Electron. Mag.*, no. April, 2020, doi: 10.1109/MIE.2020.2979272.

[13] S. Stephenson, “Abuse Vectors : A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse,” 2023.

[14] N. A. Zaimy, M. F. Zolkipli, and N. Katuk, “A review of hacking techniques in IoT systems and future trends of hacking on IoT environment,” *World J. Adv. Res. Rev.*, vol. 17, no. 02, pp. 723–731, 2023.

[15] H. Azam *et al.*, “Wireless Technology Security and Wireless Technology Security and Privacy : A Comprehensive Study,” 2023, doi: 10.20944/preprints202311.0664.v1.

[16] T. Shanthi, M. S. Sheela, J. J. Jayakanth, M. Karpagam, G. Srividhya, and T. V. S. Gowtham Prasad, “A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission,” *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 455–460, 2023.

[17] S. R. Rajeswari and V. Seenivasagam, “Comparative Study on Various Authentication Protocols in Wireless Sensor Networks,” *Sci. World J.*, vol. 2016, no. iii, 2016, doi: 10.1155/2016/6854303.

[18] Y. Zheng, G. Zhang, Z. Huan, Y. Zhang, and G. Yuan, “Space Solar Power and Wireless Transmission Wireless laser power transmission : Recent progress and future challenges,” *Sp. Sol. Power Wirel. Transm.*, no. June 2023, 2024, doi: 10.1016/j.sspwt.2023.12.001.

[19] A. H. K. 3 and R. K. Mohammed H. Alsharif 1,\* , Abu Jahid 2,\*, “SS symmetry Green IoT : A Review and Future Research Directions,” *Symmetry (Basel).*, vol. 15, no. 757, pp. 1–37, 2024

[20] I. Yaqoob, I. Abaker, T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar and S. Guizani, “Enabling Communication Technologies for Smart Cities”, IEEE Communications Magazine, January 2017, pp. 112-120. DOI: https://doi.org/ 10.1109/MCOM.2017.1600232CM

[21] S. Sendra, M. Garcia, C. Turro and J. Lloret, “WLAN IEEE 802.11 a/b/g/n Indoor Coverage and Interference Performance Study”, International Journal on Advances in Networks and Services, Vol. 4, no 1, pp. 209-222, 2011. DOI: https://doi.org/ 10.1109/ICWMC.2010.46

[22] S. Sendra, P. Fernandez, C. Turro and J. Lloret, “IEEE 802.11 a/b/g/n Indoor Coverage and Performance Comparison”, The Sixth International Conference on Wireless and Mobile Communications. ICWMC 2010, Valencia, Spain, 20-25 September 2010, pp. 185-190. DOI: https://doi.org/ 10.1109/ICWMC.2010.46

[23] S. C. Ergen, “ZigBee/IEEE 802.15.4 Summary”, UC Berkeley, Vol. 10, September 2004, pp. 17.

[24] K. Mikhaylov, N. Plevritakis and J. Tervonen, “Performance Analyss and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI'', Journal of Sensor and Actuator Networks, Vol. 2, no 3, August 2013, pp. 589-613. DOI: https://doi.org/ 10.3390/jsan2030589

[25] E. Dahlman, S. Parkvall and J. Skold, “4G: LTE/LTE-Advanced for Mobile Broadband”, 1st Edition, Academic press, 2013

[26] W. Jung and Y. Kwon, “Differences between LTE and 3G service customers: Business and policy implication” , Telematics and Informatics, Vol. 32, no. 4, pp. 667-680, 2015. DOI: https://doi.org/ 10.1016/j.tele.2015.03.001

[27] E. Kammoun, F. Zarai, and M.S. Obaidat “Chapter 6 – LTE and 5G systems”, Smart Cities and Homes, Key Enabling Technologies, pp. 111–129, 2016. DOI:<https://doi.org/10.1016/B978-0-12-803454-5.00006-7>

[28] S. Ahmadi, “LTE-Advanced: a practical systems approach to understanding 3GPP LTE releases 10 and 11 radio access technologies”, Academic Press, 2013.

[29] H. Ji, Y. Kim, J. Lee, E. Onggosanusi, Y. Nam, J. Zhang, B. Lee and B. Shim, “Overview of full-dimension MIMO in LTE-advanced pro”, IEEE Communications Magazine, Vol. 55, No. 2, pp.176-184, 2016.

[30] A. Haidine, and S. El Hassani, "LTE-a pro (4.5 G) as pre-phase for 5G deployment: closing the gap between technical requirements and network performance", International Conference on Advanced Communication Systems and Information Security (ACOSIS), Marrakesh, Morocco, 17-19 October 2016, pp. 1-7. DOI:<https://doi.org/10.1109/ACOSIS.2016.7843933>

[31] IEEE Computer Society, “Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)”, 14 June 2005

[32] J. Lee, Y. Su and C. Shen, “A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee and WiFi”, 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), Taipei, Taiwan, 5-8 November, 2007, pp. 46-51. DOI: https://doi.org/ 10.1109/IECON.2007.4460126

[33] C. Bisdikian, “An Overview of the Bluetooth Wireless Technology”, IEEE Communications Magazine, Vol. 39, no 12, December 2001, pp 86-94. DOI: https://doi.org/ 10.1109/35.968817

[34] E. Ferro and F. Potortì, “Bluetooth and Wi-Fi wireless protocols: A survey and comparison”, IEEE Wireless Communications, Vol. 12, no 1, February 2005, pp. 12-26. DOI: https://doi.org/ 10.1109/MWC.2005.1404569

[35] S. Vyas, U. Chaudhari, V. C. Nandini and B. Thakare, “State of the Art Literature Survey 2015 on Bluetooth”, International Journal of Computer Applications, Vol. 131, no 8, December 2015, pp. 7-10. DOI: https://doi.org/ 10.5120/ijca2015907391 [29] S. Darroudi and C. Gomez, “Bluetooth Low Energy Mesh Networks: A Survey”, Sensors, MDPI, Vol. 17, no 7, 22 June 2017, pp. 1467. DOI:<https://doi.org/10.3390/s17071467>

[36] S. Darroudi and C. Gomez, “Bluetooth Low Energy Mesh Networks: A Survey”, Sensors, MDPI, Vol. 17, no 7, 22 June 2017, pp. 1467. DOI: https://doi.org/10.3390/s17071467

[37] R. S. Sinha, Y. Wei and S. Hwang, “A survey on LPWA technology: LoRa and NB-IoT”, ICT Express, Vol. 3, No. 1, pp. 14-21, March 2017. DOI: https://doi.org/ 10.1016/j.icte.2017.03.004

[38] A. Augustin, J. Yi, T. Clausen and W. M. Townsley, “A Study of LoRa: Long Range & Los Power Networks for the Internet of Things”, SENSORS, Vol. 16, No. 9, p. 1466, 2016. DOI: https://doi.org/10.3390/s16091466