The Research Monograph Series in Computing, Electrical & Communication Networks
Vol. 1 (01), June 2023, pp. 18–23

CHAPTER 5

SMART CITY AND INTERNET OF THINGS FOR SMART CITIES

5.1 SMART CITY COMPONENTS

Smart cities are designed to improve the quality of life of their citizens through the integration of technology and data-driven decision-making. A smart city is made up of several components which are illustrated in Figure 7.

Below are some of the key components of a smart city:

Smart Energy Management: This involves the integration of renewable energy sources and smart grids to optimize energy consumption and reduce carbon emissions.

Intelligent Transport Systems (ITS): These systems leverage real-time data and analytics to optimize traffic flow, reduce congestion, and improve public transportation.

Smart Buildings: These are structures equipped with sensors and automation systems that monitor and manage lighting, temperature, and other systems to improve energy efficiency and occupant comfort.

Smart Waste Management: This involves the use of IoT sensors and data analytics to optimize waste collection and reduce the environmental impact of waste.

Digital Infrastructure: This includes the development of high-speed broadband networks, cloud computing services, and other digital infrastructure that enable data-driven decision-making and the delivery of smart city services.

Public Safety and Security: This involves the use of technology, such as surveillance cameras, facial recognition systems, and predictive analytics, to enhance public safety and prevent crime.

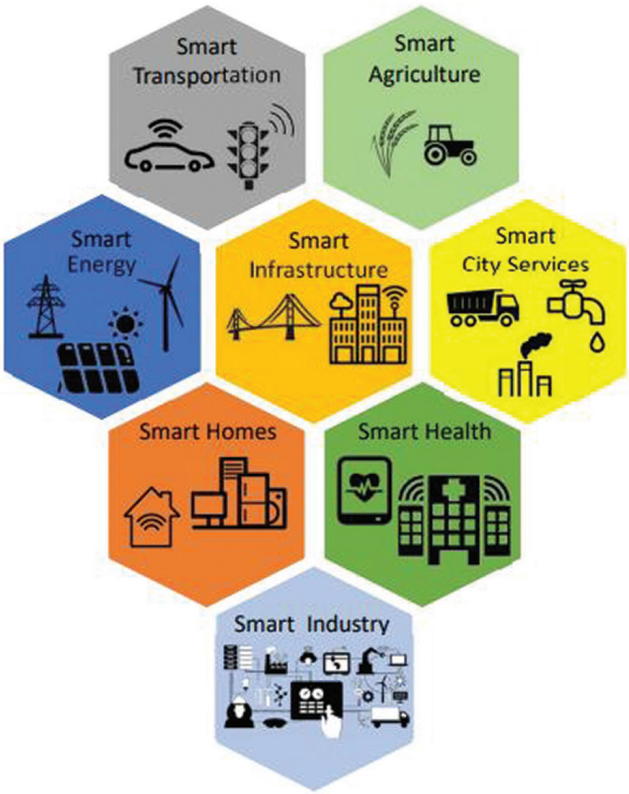

Figure 7. Smart city components.

Citizen Engagement and Participation: This involves the use of digital tools and platforms to engage citizens and enable them to participate in the decision-making processes that affect their lives.

Smart Water Management: This involves the use of sensors and analytics to optimize water supply and distribution, reduce leaks and waste, and improve water quality.

Smart Health: This involves the use of technology and data analytics to improve the quality of healthcare services, promote healthy living, and prevent the spread of diseases.

Smart Education: This involves the use of technology to enhance learning experiences, improve access to education, and increase the efficiency of educational institutions.

5.2 INTERNET OF THINGS FOR SMART CITIES

The Internet of Things (IoT) has enormous potential to transform the way cities operate, making them more efficient, sustainable, and livable. Smart cities leverage IoT technologies to connect various systems and devices, such as sensors, cameras, and other smart devices, to collect and analyze data in real-time, helping city managers make informed decisions and take proactive measures.

Here are some ways IoT can be used in smart cities:

Smart Traffic Management: IoT sensors can be installed on roads, bridges, and tunnels to monitor traffic flow, detect accidents, and optimize traffic signals based on real-time data. This can help reduce congestion, improve safety, and save time for commuters.

Environmental Monitoring: IoT sensors can be used to monitor air quality, noise pollution, and water quality in real-time, allowing cities to take measures to reduce pollution levels and improve the quality of life for residents.

Waste Management: IoT sensors can be used to optimize waste collection schedules and routes, reducing the number of garbage trucks on the road and saving costs.

Energy Management: IoT sensors can be used to monitor energy usage in buildings and public spaces, enabling cities to optimize energy consumption and reduce carbon emissions.

Public Safety: IoT sensors and cameras can be used to monitor public spaces, detecting and responding to incidents such as crime or emergencies in real-time.

IoT technologies can help cities become more sustainable, resilient, and livable, improving the quality of life for residents and visitors alike. However, it is important to ensure that the collection and use of data is done in a responsible and ethical manner, respecting privacy and security concerns.

5.3 IOT ARCHITECTURES FOR SMART CITIES

Internet of Things (IoT) technology has a significant role to play in the development of smart cities. An IoT architecture for smart cities should be designed to meet the unique requirements of the city's

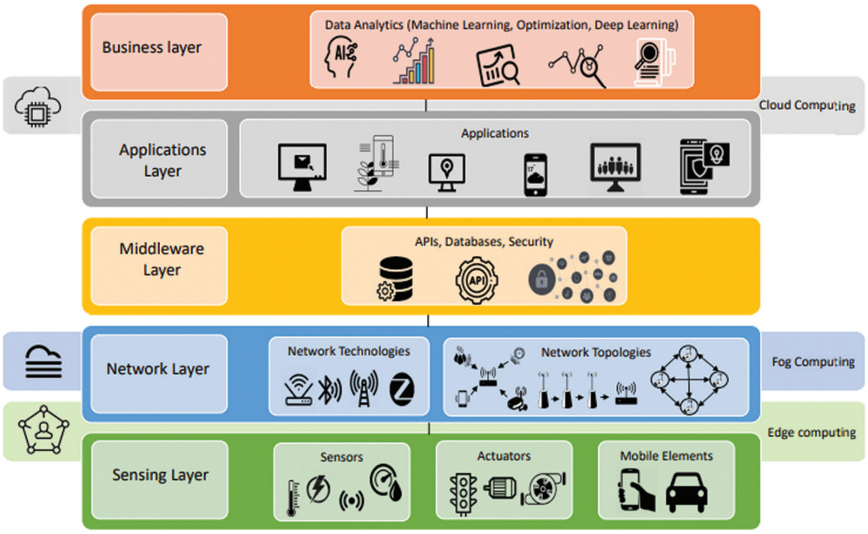

Figure 8. IoT architecture Syed et al., [53].

infrastructure, environment, and its citizens. Shown in Figure 8. IoT Architecture [53].

Here are some common IoT architectures that are used in smart cities:

Centralized Architecture: In this architecture, all the devices in the city are connected to a central server or cloud. The data collected from these devices is processed and analyzed centrally, and the insights are used to improve the city's infrastructure and services.

Decentralized Architecture: In this architecture, the devices are connected to local servers or gateways, which are connected to a central server or cloud. The data is processed locally, and only the relevant information is sent to the central server. This architecture is more suitable for cities with limited connectivity.

Hybrid Architecture: This architecture combines the centralized and decentralized architectures. The devices are connected to local servers, which process the data and send it to the central server for further analysis. This architecture is more suitable for cities with a mix of high and low connectivity areas.

Edge Computing Architecture: In this architecture, the devices are connected to edge nodes, which process the data locally. The processed

data is then sent to the central server or cloud for further analysis. This architecture is useful for cities with limited bandwidth and high latency.

In addition to these architectures, there are also other considerations that should be taken into account when designing an IoT architecture for smart cities. These include data privacy and security, scalability, interoperability, and energy efficiency.

5.4 COMPARISON OF CLOUD, FOG AND EDGE COMPUTING MODELS

Cloud, fog, and edge computing are three different models for computing that differ in terms of their architecture and function. Here's a brief comparison of these three models:

Cloud Computing: Cloud computing is a model in which computing resources, such as servers, storage, and applications, are delivered to users over the internet. These resources are typically provided by large-scale data centers operated by cloud service providers. Cloud computing is characterized by its scalability, as users can easily scale up or down their resource usage depending on their needs. This model is most appropriate for applications that require significant computing resources, such as big data analytics, machine learning, and high-performance computing.

Fog Computing: Fog computing is a model in which computing resources are distributed between the cloud and the edge of the network, closer to the end-users. Fog computing aims to improve performance, reduce latency, and increase efficiency by processing data closer to where it is generated. This model is most appropriate for applications that require low latency and high reliability, such as the internet of things (IoT) devices.

Edge Computing: Edge computing is a model in which computing resources are located at or near the devices that generate data. Edge computing is designed to address the limitations of cloud computing, such as high latency and limited bandwidth, by performing computation closer to the data source. This model is most appropriate for applications that require real-time processing, such as autonomous vehicles, drones, and augmented reality.

In summary, cloud computing is most appropriate for applications that require significant computing resources, fog computing is most

appropriate for applications that require low latency and high reliability, and edge computing is most appropriate for applications that require real-time processing.

	Cloud Computing	Fog Computing	Edge Computing	Mist Computing
Architecture	✧ Central processing based model ✧ Fulfils the need for large amounts of data to be accessed more quickly, this demand is ever-growing due to cloud agility ✧ Accessed through internet	✧ Coined by CISCO ✧ Extending cloud to the edge of the network ✧ Decentralized computing ✧ Any device with computing, storage, and network connectivity can be a fog node, can be put on railway track or oil rig. ✧ Fog computing shoves intelligence down to the local area network level of network architecture, processing data in a fog node or IoT gateway	✧ Fog computing usually work with cloud and Edge can work without cloud or fog. ✧ Edge is limited to smaller number of peripheral layers ✧ Edge computing pushes the intelligence, processing power and communication of an edge gateway or appliance directly into devices like programmable automation controllers (PACs)	✧ Middle ground between cloud and edge/fog ✧ Lightweight computing residing in the network fabric using micro-controllers and microchips ✧ Not a mandatory layer of fog computing
Pros	✧ Easy to scale ✧ Low cost storage ✧ Based on Internet driven global network on robust TCP/IP protocol	✧ Real time data analysis ✧ Take quick actions ✧ Sensitive data remains inside the network ✧ Cost saving on storage and network ✧ More scalable than edge computing ✧ Operations can be managed by IT/OT team	✧ Edge computing simplifies internal communication by means of physically wiring physical assets to intelligent PAC to collect, analysis and process data. ✧ PACs then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis	✧ Local decision making data ✧ Works with fog computing and cloud platform
Cons	✧ Latency/Response time ✧ Bandwidth cost ✧ Security ✧ Power consumption ✧ No offline-mode ✧ Sending raw data over internet to the cloud could have privacy, security and legal issues	✧ Fog computing relies on many links to move data from physical asset chain to digital layer and this is a potential point of failure.	✧ Less scalable than fog computing ✧ Interconnected through proprietary networks with custom security and little interoperability. ✧ No cloud-aware ✧ Cannot do resource pooling ✧ Operations cannot be extended to IT/OT team	
Misc.		✧ Less sensitive and non-real-time data is sent to the cloud for further processing ✧ Fog node can be deployed in private, community, public or hybrid mode	✧ PACs [programmable automation controllers] then use edge computing capabilities to determine what data should be stored locally or sent to the cloud for further analysis ✧ intelligence is literally pushed to the network edge, where our physical assets are first connected together and where IoT data originates ✧ The current Edge Computing domain is a sub-set of Fog Computing domain.	✧ Architecture may not require Cloud