Smart Cities: A Survey on Data Management, Security and Enabling Technologies

Ammar Gharaibeh, *Member, IEEE,* Mohammad A. Salahuddin, *Member, IEEE,* Sayed J. Hussini, *Student Member, IEEE,* Abdallah Khreishah, *Member, IEEE,* Issa Khalil, *Member, IEEE,* Mohsen Guizani, *Fellow, IEEE,* and Ala Al-Fuqaha, *Senior Member, IEEE*

***Abstract*—Integrating the various embedded devices and systems in our environment enables an Internet of Things (IoT) for a smart city. The IoT will generate tremendous amount of data that can be leveraged for safety, efficiency and infotainment applications, and services for city residents. The management of this voluminous data through its lifecycle is fundamental to the realization of smart cities. Therefore, in contrast to existing surveys on smart cities we provide a data-centric perspective, describing the fundamental data management techniques employed to ensure consistency, interoperability, granularity and reusability of the data generated by the underlying IoT for smart cities. Essentially, the data lifecycle in a smart city is dependent on tightly coupled data management with cross-cutting layers of data security and privacy, and supporting infrastructure. Therefore, we further identify techniques employed for data security and privacy, and discuss the networking and computing technologies that enable smart cities. We highlight the achievements in realizing various aspects of smart cities, present the lessons learnt and identify limitations and research challenges.**

***Keywords*-Smart Cities, Internet of Things (IoT), data management, data security, Network Functions Virtualization (NFV), Software-Defined Networking (SDN), cloud computing.**

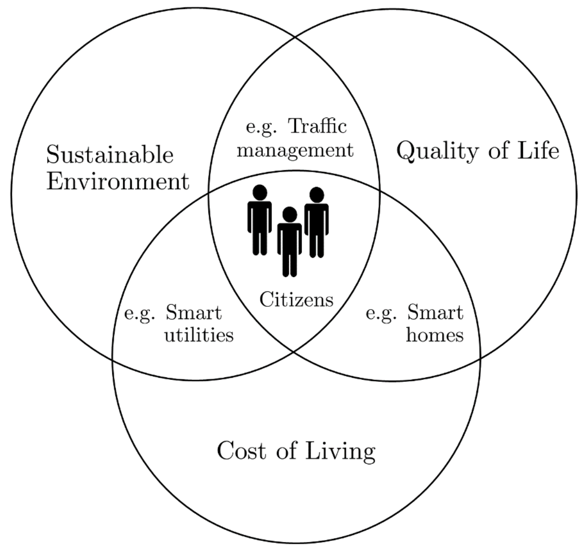


Fig. 1: Fundamental objectives of smart cities.

I. Introduction

TODAY, more than half of the world's population lives in cities [1] with more than six devices per person connected to the Internet [2]. This implies that billions of devices and systems are embedded in a city's infrastructure. These range from end-user devices to municipal systems for smart lightning, road traffic and pedestrian management, water and gas monitoring, structural monitoring and waste management, to smart healthcare system, just to mention a few. Therefore, the de facto expectation from a smart city is utilization of idle computation and communication resources, integration, management and analysis of the tremendous data to increase safety, efficiency, productivity and quality of life for its citizens. Smart city applications mutually benefit the citizens and the underlying environment, as illustrated in Figure 1. They include: smart economy, smart governance, smart people, smart mobility, smart environment, and smart living [3].

Though, a formal definition of a smart city exists [4], we propose a new definition from a data management perspective. A smart city employs a combination of data collection, processing, and disseminating technologies in conjunction with networking and computing technologies and data security and privacy measures encouraging application innovation to promote the overall quality of life for its citizens and covering dimensions that include: utilities, health, transportation, entertainment

Ammar Gharaibeh is with German Jordanian University, Amman 11180 Jordan. (e-mail: ammar.gharaibeh@gju.edu.jo)
Mohammad A. Salahuddin is with the University of Waterloo, Waterloo, ON, N2L 3G1, Canada. (e-mail: mohammad.salahuddin@ieee.org)
Sayed J. Hussini and Ala Al-Fuqaha are with Western Michigan University, Kalamazoo, MI, 49008, USA. (e-mail: {sayedjahed.hussini, ala.al-fuqaha}@wmich.edu)
Abdallah Khreishah is with New Jersey Institute of Technology, Newark, NJ, 07102, USA. (e-mail: abdallah@njit.edu)
Issa Khalil is with Qatar Computing Research Institute, Doha, Qatar. (e-mail: ikhalil@hbku.edu.qa)
Mohsen Guizani is with the University of Idaho, Moscow, ID, 83844, USA. (e-mail: mguizani@uidaho.edu)

and government services.

A unified framework for data management is critical and fundamental to a smart city and all its applications. An essential requirement of the smart city is seamless, efficient management and delivery of high quality and tightly coupled Food, Energy, and Water (FEW) resources. For instance, the smart integration of food and agriculture administration with seamless monitoring of raw and processed food quality delivered to the city can greatly limit or detect the spread of deadly diseases and bacteria like semolina poisoning. Similarly, the smart management of water can ubiquitously detect harmful bacteria and pollutants in water and alert municipal authorities before spreading of diseases (e.g., using water turbidity sensors). Also, smart energy sectors can manage energy production based on variable demands in the city. However, there are major obstacles [5] hindering smart cities.

Data management is an integral component in realizing the IoT for enabling the smart cities. Primarily, it consists of data acquisition, processing and dissemination. Data acquisition includes data standards, quality and use. These are essential for managing the myriad data. Data standards ensure consistency across different data acquisition techniques. For example, sensory data acquired from Wireless Sensor Networks (WSNs) and Mobile Ad hoc Networks (MANETs) must be in the same type and format to enable data integration along with efficient and useful processing. Data quality dictates the sufficient dimensions of data, the necessary granularity for effective functioning and leads to the quintessential arguments regarding data fusion and decision fusion. Data fusion recommends using all the raw data collected in the final processing, whereas decision fusion aggregates raw data in clusters for information processing.

Apart from data acquisition and processing, various data access patterns and data analysis tools are necessary so as to monitor and improve performance of applications and services for efficient dissemination of information within the smart city. For example, the dimensions and granularity of the raw data necessary for optimal functioning of IoT and smart city applications. To infer the weather, that is, humidity, pressure, wind and direction, and temperature of a region of observation, is it necessary to query an entire embedded WSN, a subset of the WSN or a single more powerful node, such as the one employed by meteorologists? The large scale granularity of the raw data gives insight to variation and detailed analysis of weather conditions across the area of interest whereas, probing a single more powerful node gives faster and reliable information. Data quality measures will strike a balance between efficiency and overhead based on the objective of independent IoT and smart city applications. Data use ensures reusability of acquired data by identifying the applications and services that require same set of data. The data use can also ensure accuracy of the data collected for sharing amongst a large number or critical applications and services. It can enforce redundancy of acquired data for reliability and resilience. These different aspects in data acquisition are tightly coupled and require critical tradeoff analysis of accuracy and efficiency versus overhead for cost, computation and communication.

Last but not least, a smart city consists of various categories of end-users, such as, citizens, government agencies, industrial partners, etc. Each end-user has its own set of requirements for smart city application and services and the accepted quality of service (QoS). For example, citizens in a smart home primarily require high-speed connectivity to social networking sites with high-resolution streaming on rich video content, whereas public healthcare clinics may require secure connections to servers in the cloud for storing and retrieving sensitive patient healthcare information. Therefore, data management must not only offer differentiated data distribution amongst the different classes of end users, but also prioritize data distribution based on the different categories of end-users in the smart city.

The cross-layer challenge in realizing smart cities is achieving resilience in data management against security and privacy threats. Here, negligence in data security and privacy is amplified in folds and can not only result in faulty applications and services, but also in paralyzing the entire city, as demonstrated by the Distributed Denial of Service (DDoS) attack on Dyn in October 2016, in which attackers used unsecure IoT devices [6]. Therefore, networking and computing technologies are tightly coupled across layers to enable smart cities that are built for efficient data management and to withstand security and privacy breaches and failures.

These facets are not mutually exclusive and may overlap significantly. Therefore, the realization of smart cities is dependent upon an interoperable holistic approach [7]. In this survey, we take a new perspective on smart city. As illustrated in Figure 2, we view the journey of data through a smart city beginning from the different technologies for data collection, information processing and distribution. This includes cross-layer challenges of data security and privacy, and include softwarization and virtualization techniques that enable different networking and computing technologies to facilitate smart cities.

The rest of the survey is organized as follows. We start with a comparison to the related surveys on Smart Cities and highlight our contributions in Section II. In Section III, we present a set of use cases deployed for smart cities, noting the achievements and lessons learnt. In Sections IV, V, and VI, we discuss the data

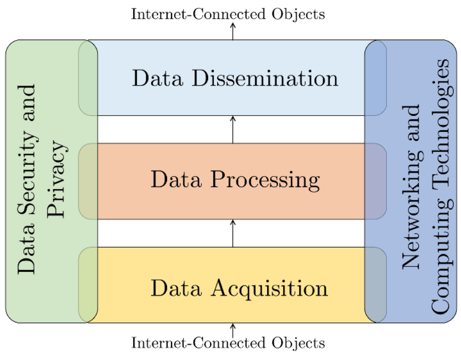


Fig. 2: A holistic view of the data lifecycle, including data management, data security and privacy, and network and computing technologies in smart cities.

management techniques employed for acquisition, processing and dissemination, identifying their limitations and research challenges. Data security and privacy techniques employed for smart cities to incorporate resilience to threats are presented in Section VII. We review the softwarization and virtualization of networking and computing technologies that enable smart city deployment and its applications and services in Section VIII. Finally, we summarize and conclude this study in Section IX. A list of the acronyms used in the survey is presented in Section X. To facilitate reading, Figure 3 provides a detailed structure of the survey.

II. Related Work and Contributions

Tables I and II delineate the closely related surveys on smart cities and demonstrate the novelty of our survey. The literature review begins with a scrutiny of the various definitions of a smart city presented by Fernandez-Anez [4]. Arasteh et al. [8] discuss the relationship between IoT and a smart city, while Luong et al. [9] survey the economic and pricing theory and their applications in data collection and communication for IoT. Da Silva et al. [10] survey the architecture for smart cities, while El Baz and Bourgeois [11] discuss the architecture of a specific smart city application (Logistic Mobile Application). Ijaz et al. [12] survey security aspects of a smart city. Pellicer et al. [3] present an overview of smart city deployments around the globe. Petrolo et al. [13] provide a survey of the semantics used by sensors in the Cloud for IoT applications in order to bridge the gap between the Internet of Things and the Cloud of Things. Perera et al. [14] discuss the role of Fog computing in smart city applications. Shuai et al. [15] provide a survey for a specific smart city application called Electric Vehicles Charging. Wang and Sng [16] survey the different deep learning algorithms, with video analytics as a target smart city application. Rashid and Rehmani [17] survey the application of Wireless Sensor Networks in smart cities.

This survey is intrinsically different, due to its data-centric view of smart city applications and services. Djahel et al. [18] provide similar survey of data life cycle in the context of Traffic Management Systems (TMS) for smart cities, but is limited in its applicability to smart city deployment, applications and services, since it is focused on TMS only. Specifically, the contributions of this survey can be delineated as:

1) We illustrate representative use cases from various application domains including traffic management, smart grids and smart healthcare. The presented use cases are thoroughly explained, highlighting the main components required by these applications.
2) We discuss preliminary deployments of the presented use cases in smart cities and highlight their achievements and the lessons learnt.
3) We provide an in-depth review of data management, including acquisition, processing and dissemination from algorithmic perspective (*i.e.*, the algorithms that can be used for data management) and platform perspective (*i.e.*, the computing platforms to run the different algorithms).
4) We evaluate the state-of-the-art data management techniques, data security and privacy techniques and networking and computing technologies that enable smart cities.
5) Throughout the survey, we draw higher-order insights and discuss research challenges regarding data management, security and enabling technologies in support of smart cities.

Our survey is beneficial for future research on smart cities, as it comprehensively serves as a resource for data management, data security and privacy and networking and computing technologies enabling smart cities.

III. Smart City Application Deployments

In this section, we discuss five representative examples of smart city applications that cover the six aspects of smart cities as outlined in [3]. Specifically, we discuss smart street light, smart traffic management, virtual power plants in smart grids, smart emergency systems and smart health. We also highlight the challenges faced by these applications.

A. Smart Street Lights

Smart street lights are one of the many applications that a smart city should target. By deploying smart street lights, a smart city can reduce the energy consumption by dimming lights depending on the time of day or the location where traffic/pedestrian activities are low.

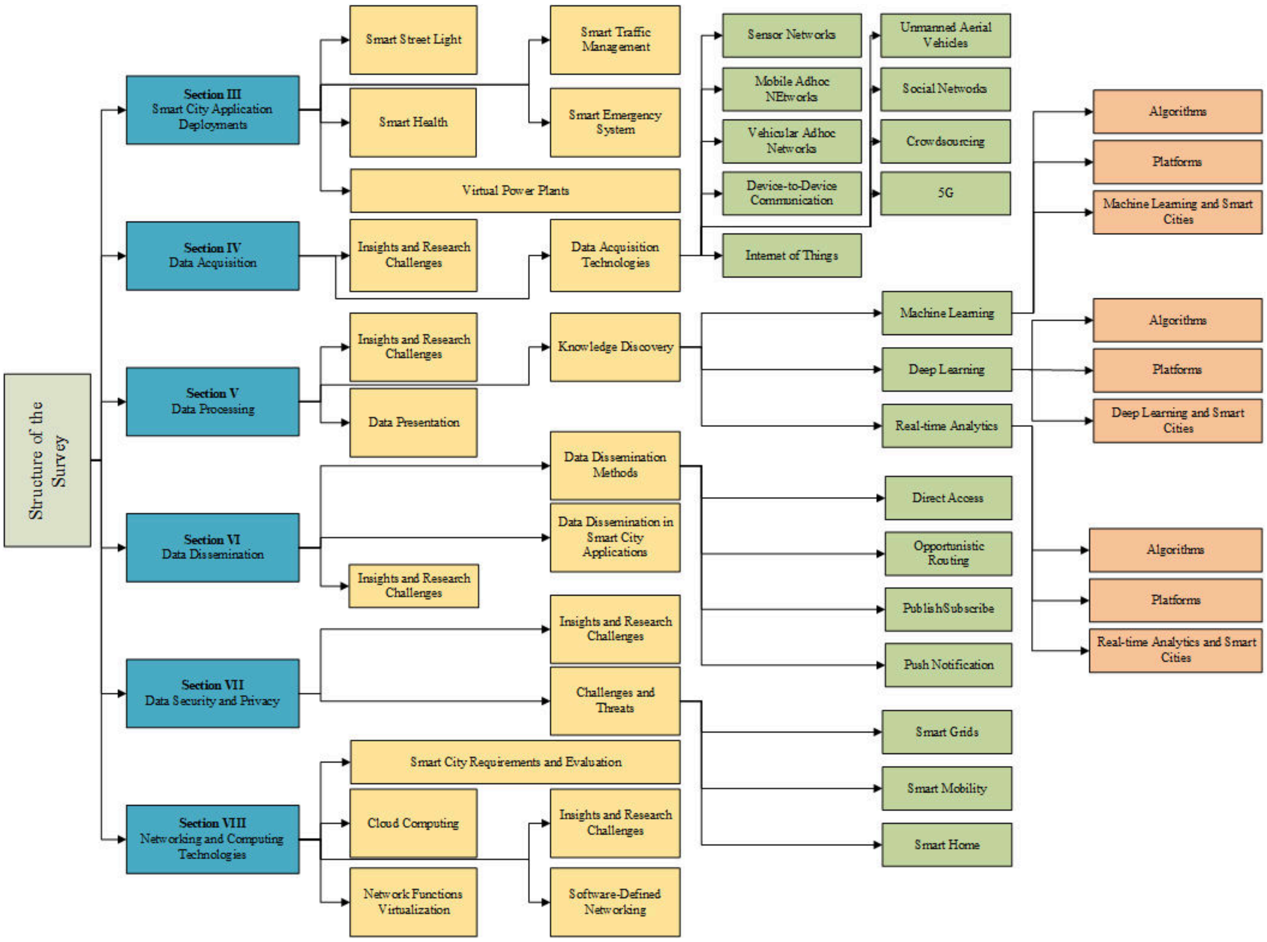


Fig. 3: Structure of the survey.

TABLE I: COMPARISON OF RELATED WORK ON SMART CITY SURVEYS IN TERMS OF SMART CITY DEFINITIONS, DATA MANAGEMENT, DATA SECURITY AND ENABLING TECHNOLOGIES

Reference	Smart City	Data	Data Processing			Data	Networking and Computing Technologies			Data Security
	Definitions	Acquisition	Machine Learning	Deep Learning	Real-Time Analytics	Dissemination	SDN	NFV	Cloud Computing	and Privacy
Fernandez-Anez [4]	✓									
Ijaz et al. [12]										✓
Djahel et al. [18]		✓								✓
Petrolo et al. [13]									✓	
Perera et al. [14]									✓	
Wang et al. [16]				✓						
This work	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

TABLE II: COMPARISON OF RELATED WORK ON SMART CITY SURVEYS IN TERMS OF SMART CITY APPLICATIONS

Reference	Smart Lighting	Smart Traffic Management	Smart Grid	Smart Emergency	Smart Health
Djahel et al. [18]		✓			
Shuai et al. [15]			✓		
This work	✓	✓	✓	✓	✓

The saved energy can be used in support of different functionalities such as pollution monitoring or weather monitoring. An example of this scenario is depicted in Figure 4.

To realize such a scenario, the street lights should be equipped with sensors in order to collect the necessary data for efficient functionality. The collected data can either be processed locally if the street lights are equipped with computing capabilities, or propagated through a network to a management and control system that determines the proper action to perform. Actions could include which lights to dim, which lights are approaching their end-of-life, or which lights need to be replaced.

Smart street light systems have been studied in the literature. For example, Veena et al. [20] propose a smart street light system, which is a hardware application that takes video as input and detects movement of vehicles and human beings to switch on only a number of street lights ahead of it (vehicle and human), and to switch off the trailing lights to save energy. This is achieved by processing the image of an approaching object using Object Level Frame comparison methodology and then sending a control message to the street light block. Sheu et al. [21] design a Light Emitting Diode (LED) street light system, which integrates multi-color LED, power driving IC and embedded image processing. The embedded system is used to monitor the road status and output control instructions. For example, if fog or rain is detected, the embedded system immediately instructs the power IC to drive multi-color LEDs for generating the lower color temperature light to improve the road visibility for pedestrians and drivers. Jain and Nagarajan [22] propose a smart light system that incorporates an LED array and a micro-controller, which are powered by solar panels and battery packs. The micro-controller daily estimates the sunrise and sunset times based on the Real-Time Clock (RTC) running on the controller along with the hard coded coordinates and time zone of any given location. The micro-controller also has the ability to dim the lights during late night hours. Bellido et al. [23] propose a smart light system based on wireless communications over the Digital Addressable Lighting Interface (DALI) protocol. The authors designed a wireless node based on the IEEE 802.15.4 standard with a DALI interface, developed a network layer that considers the topology of the lighting network and developed user-friendly applications for the control and maintenance of the system.

Moving from traditional to smart street lights has many advantages. The smart street lights can be easily monitored through a management and control system while a scouting team has to visually do the monitoring in case of traditional street lights. Moreover, smart street lights can be easily maintained, their brightness can be adjusted remotely and it is easier to monitor their energy consumption [24]. These differences are highlighted in Table III.

TABLE III: MOVING FROM TRADITIONAL TO SMART STREET LIGHTS [25]

Traditional Street Light	**Smart Street Light**
Physical Failure Inspection • A scouting team drives during night to visually inspect failures.	Remote Monitoring • The lighting failures are automatically reported by the system.
Undifferentiated Lighting Level • Lights burn at full intensity throughout the night.	Smart Dimming • Lights dimmed during low traffic hours to save energy.
Estimation-based Metering • Energy consumption is roughly estimated.	Smart Metering • Energy consumption is accurately calculated through smart meters.

In the following, we identify the components required by a smart street light system and list some of smart street light project examples from smart cities around the world.

1) Components of Smart Street Light Systems

In order to deploy smart street light systems, three main components must be identified: smart lamp, network infrastructure and management and control system. Figure 5 shows these three components and their intersection to create smart street lighting. Next, we present a brief description of each component.

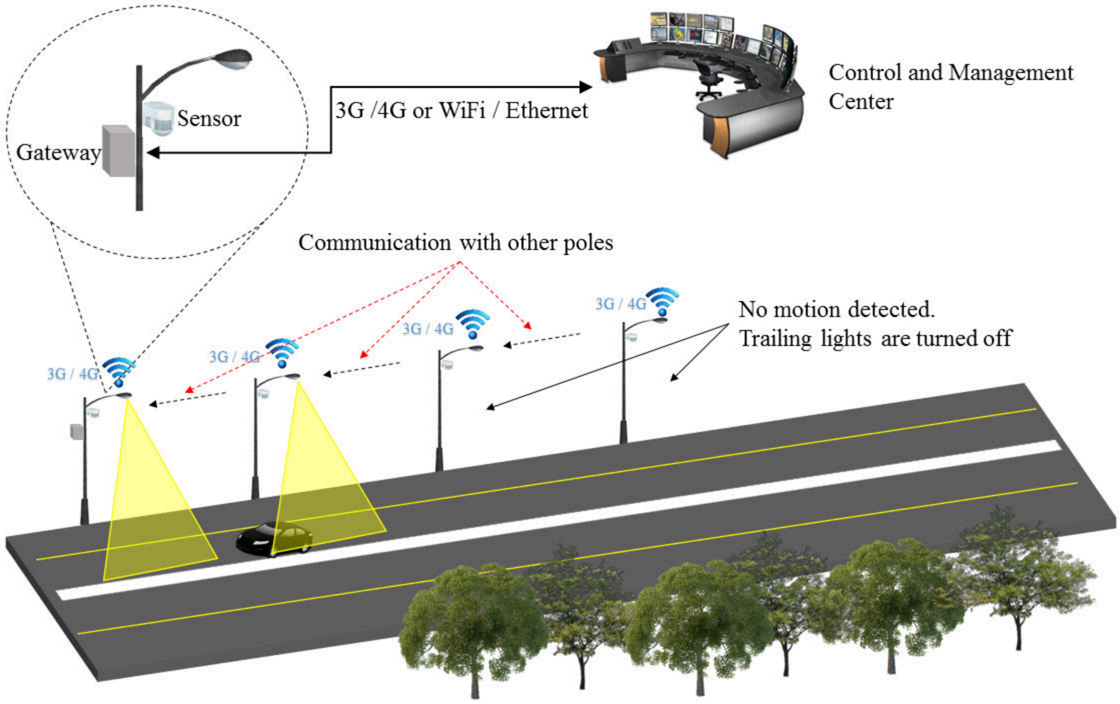


Fig. 4: Example of smart street light scenario [19].

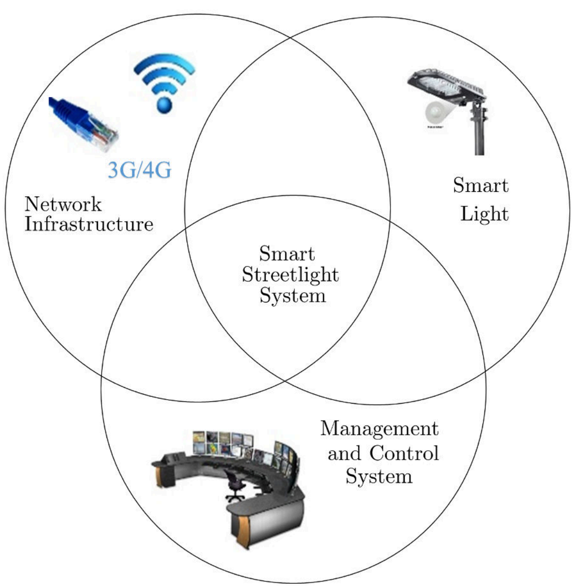


Fig. 5: Components of smart street light systems.

a) The Smart Light

A Smart Light is a light source that is equipped with sensors to collect environmental parameters. These parameters can be sent to a control system to identify the proper action.

There are different types of light sources that can be used for street lighting. The choice of the light source depends on many factors such as energy consumption and lifetime. According to [26], LEDs can reduce the energy consumption by up to 50% while maintaining the same illumination level when compared to incandescent lamps. Moreover, LEDs have a longer lifetime, are easier to control and maintain and have a shorter Return of Investment period.

b) Network Infrastructure

To enable remote monitoring and management of the street lights, the street lights need to be connected through a network to a management and control system. The lights can be connected using wireless technologies such as WiFi [27], ZigBee [28]–[30], 2G/3G/4G [31]. They can also be connected using wired technologies such as Ethernet cables [32], or Power Line Communication (PLC) technology [33], [34].

c) Management and Control System

The management and control system role is to monitor and control the street lights. Monitoring includes looking for failures and observing the energy consumption of the street lights among other actions. The street lights can be controlled by adjusting their brightness level according to different situations (time of day, weather conditions) to reduce the energy consumption.

The management and control system can be either centralized or distributed. Bruno et al. [35] propose a centralized control system for smart street lights that allows facility managers to remotely control street lights while keeping track of electrical power consumption in the lamps and in the driving circuits. Badgaiyan and Sehgal [36] propose a centralized monitoring system with the purpose of reporting failures and measuring the energy consumption. The controlling of the lights is done at the light's premises using wireless and pyro-electric infrared sensors. On the other hand, Fujii et al. [37] propose the concept of an autonomous-distributed controlled light system, in which the lights turn on before pedestrians or vehicles come and turn off or reduce brightness to save electric power when there is no traffic. A distributed sensor network is used to detect pedestrians or vehicles. Leccese [27] separates the management from the control part by assigning the management part to a centralized server, while allowing the lights to automatically perform the controlling part through the use of different sensors.

2) Smart Street Light in Smart Cities

In this section, we present some examples of smart street light systems developed by smart cities.

a) Amsterdam, Netherlands:

In 2007, the city of Amsterdam started its smart city project. The city considered proposals by tech companies on how IoT technologies can be utilized to promote the overall city operations and enhance the quality of life for the citizens. To this end, officials from the city's IT infrastructure management office and from the electricity grid management office have considered upgrading their infrastructure and adopting an open architecture platforms that can be used in future IoT projects [38].

After adopting an open architecture platforms for both the IT infrastructure and the electric grid, pilot projects were initiated by the city. These projects aimed at offering new data and access to increase the efficiency of the city services and to reduce the consumption of resources. One of the important projects is the smart street lighting. In this project, lamp posts are equipped with cameras, environmental sensors and WiFi connections, among other technologies. As part of the project's openness, different models and access control have been tested to allow citizens and companies to access camera information and control lighting levels in their vicinity [38].

The city started deploying the smart street light system at Hoekenrodeplein, a large modern square near Amsterdam Arena. In collaboration with Philips, Cisco and Dutch utility Alliander, a connected lighting system and public WiFi connection have been installed. This collaboration allowed different applications to become a reality. One of these applications is adaptive lighting, where the lights can be adjusted automatically through sensors based on different conditions, such as sporting events or weather conditions.

The smart street light uses wired and wireless connections in order for the users to be able to remotely and dynamically adapt the lighting properties such as brightness and color. The lamp posts are also equipped with multiple sensors that can provide data on different aspects of the city. Examples include providing data on crowds, traffic, parking conditions and air quality. These data are then shared with other parties who can benefit from them.

b) San Jose, USA:

Approximately 62,000 street lights are owned and maintained by the city of San Jose, with around 65% of these lights being either low pressure or high pressure sodium lights. San Jose is one of the first cities in the U.S. to adopt smart street lighting project. This project involves replacing the current lights with energy-efficient LED lights and deploying a control and management system for efficient operation of these lights [39].

The smart street light system is part of the city's Green Vision, where the city has partnered with the industry for new LED designs. The installed LED lights are energy-efficient, longer-lasting, can be programmed to optimize, monitor and report energy consumption, as well as produce minimal to no hazardous waste upon disposal. The adopted control and management system allows for light dimming during late night hours and reporting malfunctioned lights to expedite repairs.

B. Smart Traffic Management

Providing innovative traffic and transportation services is one of the key goals of smart cities [3]. This is realized through Smart Traffic Management. Smart Traffic Management aims at empowering users with data in order to be better informed, which leads to safer and smarter decisions on using the transportation network. Different technologies can be applied to enhance traffic management, ranging from basic systems like car navigation and controlling traffic signals, to monitoring applications using security Closed-Circuit Television Cameras (CCTV) and motion sensors, to integrating live data and feedback for use in advanced applications like parking guidance. Figure 6 shows an example of a smart traffic management scenario.

In order to obtain traffic data, smart traffic management can use either floating car data or sensing technologies. Floating car data is obtained through either *triangulation methods*, which exploits the presence of mobile devices in vehicles travelling along streets, highways, motorways (freeways) and other transport routes, *vehicle's re-identification* where travel times and speeds are calculated by comparing the time at which a specific device in a vehicle is detected by pairs of sensors, *GPS based methods*, or *smartphone-based rich monitoring* by exploiting the sensors embedded in smart phones.

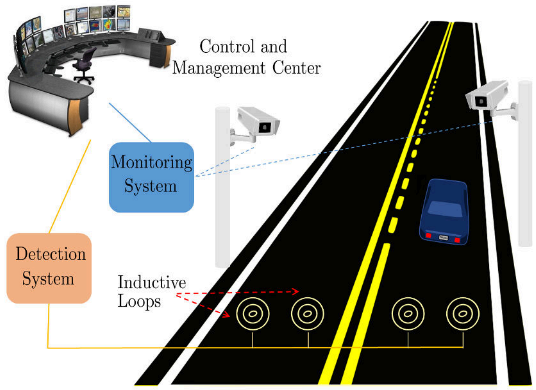


Fig. 6: Example of smart traffic management scenario.

The other method to obtain traffic data is by using sensing technologies. Sensing technologies include, but are not limited to, inductive loop detection where vehicles are detected as they pass through the loop's magnetic field, video vehicle detection by using cameras mounted on poles or structures above or adjacent to the roadway, audio detection where traffic density on a road is estimated using the audio signals generated from the vehicles traversing the road, bluetooth detection, or by collecting data from different sensors.

In the following, we review some of the traffic management systems deployed in smart cities.

1) Smart Traffic in Boston, USA:

Boston was one of the 33 cities selected to receive a Smarter Cities Challenge grant from IBM in 2012 as part of IBM's citizenship efforts to build a Smarter Planet [40]. To tackle key challenges identified by the Mayor and his team, a group of six IBM experts worked to provide recommendations on how to counter these challenges. The main challenge was to unlock, share and analyze data to support Boston plans to improve climate and traffic. Other specific transportation challenges included:

- Reducing carbon emissions associated with transportation: Boston's traffic accounts for about 25% of the city's carbon emissions. The mayor's Climate Action Plan called for significant greenhouse gas reduction.
- Analyzing and reducing vehicle miles traveled (VMT): This will reduce traffic congestion and carbon emissions.
- Make data accessible by residents: When citizens can access the traffic data, intelligent and informed decisions can be made.

The traffic data collected through manual traffic count, inductive loops and video cameras are currently not accessible, shared, or analyzed. The data is neither standardized or exploited to its full potential. Therefore, unlocking, sharing and analyzing these data are required to realize the Smart Traffic Management project.

The recommendations of the IBM team focused on establishing a platform to connect the different traffic systems. This will enable innovation of smart applications using data analytics and data visualization. The recommendations fall within four categories. The first category is *Unlocking data* which pertains to providing the data in a standard format. The second category is *Sharing data*, where the process of transferring traffic count data from the Traffic Management Center (TMC) to Department of Innovation and Technology (DoIT) is automated and access to the data is provided. The third category is *Analyzing data*. This is related to accessing and visualizing the data by Boston residents, developing an intelligent traffic control infrastructure, providing different technologies for analytics and CO_2 emission estimates. The last category is *Future vision*, which provides a roadmap for including state-of-the-art technologies in the infrastructure and providing advanced analytics and visualization technologies.

To see if the team could meet the above-mentioned recommendations, the city requested a demonstrable prototype. Table IV illustrates the goals and objectives of this Smarter Cities Challenge from a technological perspective. Within the domain of transportation and the scope of this project, the goals in the first row of the table are supported by the objectives in the remaining rows, from the highest layer of visualization to the lowest layer of the infrastructure. The columns on the right specify whether the corresponding items were included in the prototype or will be incorporated in the future.

2) Smart Traffic in New York City, USA:

Midtown in Motion, a congestion management system for New York city was launched in 2011 [41]. The system aims at providing the traffic engineers with the ability to quickly identify and respond in real-time to traffic conditions. The project expanded in 2012 in two phases to cover wider areas of the midtown. In the first phase, 100 microwave sensors, 32 traffic video cameras and E-Z Pass readers at 23 intersections were deployed to measure traffic speeds. Advanced Solid State Traffic Controllers (ATSCs) connected to the network were used to remotely control the traffic signals to alleviate congestion issues. As a consequence, a 10% improvement in travel times was observed. The second phase targeted service expansion to cover more than 270 blocks with additional 110 microwave sensors, 24 traffic video cameras, and 36 E-Z Pass readers.

The city of New York is using the ATSCs, which are connected to the network to facilitate remote operations. Traffic engineers can adjust the signals for even distribution of the traffic flow, relieving congestion and clearing isolated backups caused by collisions or double-

TABLE IV: GOALS AND OBJECTIVES OF BOSTON SMART TRAFFIC PROJECT FROM A TECHNOLOGICAL PERSPECTIVE [40]

Component	**Example**	**Presented in Prototype**	**Future Plan**
Goals	• Unlock Data • Share Data • Analyze Data	✓	✓
	• Future Vision Roadmap		✓
Visualization	• Intersection traffic view • Traffic count displays from multiple data sources • Histograms of car, bicycle and pedestrian traffic at intersections	✓	✓
Analytics	• Peak hour and in/out directional flows • Road classification based on distribution of traffic volume and patterns • Travel conditions • Video camera-based vehicle counts • CO_2 measurements	✓	✓
	• Standards-based traffic state indicators • Traffic growth rate estimation • Travel time estimation to particular landmarks • Traffic simulation technologies • Alternative routes computation		✓
Data	• Inductive loop traffic counts • Manually collected traffic counts • Pneumatic tube traffic counts • Common data model • Aggregated data from sources listed above	✓	✓
	• Video cameras • Mobile devices • GPS data from public and private vehicles • Parking data • Hubway bike sharing • Electric vehicle charging stations • Public transit data • Regional highway data • EZ Pass transponders		✓
Instrumentation	• Inductive loops • Existing manual count reports • Pneumatic tube counts	✓	✓
	• Video cameras • GPS • Public transit data • Other		✓

parked vehicles. The ATSCs also allow the engineers to adjust the signal timing to either a simultaneous signal progression, where all signals change at the same time, or a traffic signal progression, where green lights are encountered by drivers travelling at constant speeds. Other advantages of deploying ATSCs include weather resistance, tamper-proof and requiring less maintenance.

Having the goal of making the data accessible by different parties, real-time Midtown in Motion traffic information is available on the Department of Transportation website and through smart phone applications. This also leads to innovating different applications by New York's technology industry. The data transmission is realized through the use of New York City Wireless Network (NYCWiN), developed by the Department of Information Technology and Telecommunications.

3) Smart Traffic in Louisville, USA:

In their goal towards an "open government," the city of Louisville is adopting crowdsourcing as a way to encourage the citizens to participate in smart city applications. To this end, the city of Louisville has joined Waze's Connected Citizens Program [42], [43]. Through this program, Waze exchanges traffic data with the city of Louisville, which is used to identify congestion spots and traffic patterns to improve the traffic situation and provide a better road experience for the citizens. Using this approach, the citizens of Louisville who are using Waze are effectively participating in making their city a smart one.

C. Virtual Power Plants

The introduction of new technologies such as smart grid and smart meter have changed the operation of the utility companies in the last decade. To tackle challenges imposed by regulatory bodies such as reducing carbon emissions and providing higher customer flexibility, utility companies are required to create a balance between these challenges and provide reliable services to the customers at a reasonable price [44].

To address challenges like pricing, load reduction and demand response, Virtual Power Plants (VPPs) have been proposed. VPPs are a collection of customers (*i.e.*, residential, commercial or industrial) under a shared program that can include shared pricing, demand response, or distributed energy resources. Customer aggregation and classification allows the utility companies to better forecast and analyze the customers' demands and brings forth the value that the customers contribute to the companies.

Distributed energy resources for load reduction, an aspect of VPP, can be achieved by adding energy storage capabilities to households in the smart city. Energy stored from renewable sources or the main grid when the price is low can be used later to close the gap between the available energy and the energy demand. Moreover, the excess stored energy can be distributed to other households in a way that reduces the cost to the consumer. Figure 7 shows an example of a virtual power plant.

There are three main components that constitute a VPP project [45]:

- Distributed Energy Resources (DER): Distributed Generation (DG) within the VPP premises can be classified according to the type of the primary energy source, capacity of DG units, ownership of DG units and DGs operational nature.
- Energy Storage Systems (ESS): Energy stored during off-peak hours can be used during peak hours to close the gap between the supply and the demand. To this end, efficient storage elements are required.
- Information and Communication System: The system includes a control system to manage DER and ESS to ensure the efficient operation of the VPP through bidirectional communication. The control system is also responsible for load forecasting, monitoring and coordination between the VPP components.

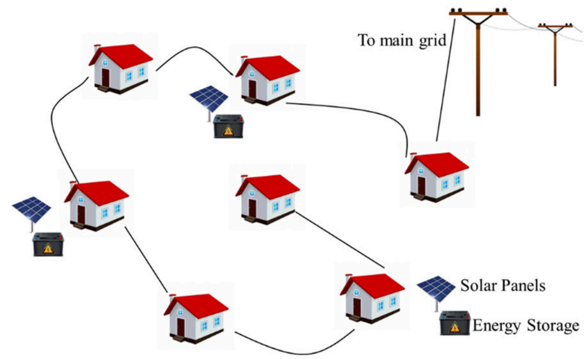


Fig. 7: Example of virtual power plant scenario.

In the following, we introduce examples of smart cities efforts in developing VPPs.

1) VPP in Rheintal, Switzerland:

Part of Smart Grid project in Rheintal is partnering with Bosch Software Innovations to develop a Virtual Power Plant for energy management and monitoring. Using load distribution, the city is able to provide load balancing and support new services. Currently, Bosch Software Innovations is implementing three key projects for the Virtual Power Plant smart city project in Rheintal [46]:

- Monitoring power generation of Photo-Voltic (PV) systems: To facilitate a local energy supply, a group of PV systems is deployed. Predicting a day-ahead power generation from these systems is accomplished through measuring the system capacity and using weather forecast data.
- Load management for charging infrastructure of electric vehicles: The increased interest in electric vehicles requires the integration of the charging infrastructure into the current grid. By exploiting Vehicle-related data, such as latest state of charge, along with using the Open Charge Point Protocol (OCPP) [47], an optimized schedule for charging is obtained.
- Control and energy management of in-house consumers: Controlling the energy consumption of household appliances is performed by an Energy Management System (EMS) that decides whether to switch a device on or off based on predicted consumption and pre-determined threshold values.

The VPP management system is also responsible for prioritizing the activation of plants based on their properties and contracts by using data from external sources such as weather forecast and electricity prices. This is done in two ways:

- Trading optimization: Based on the chosen optimization strategy, the properties of the individual VPPs, and electricity prices, the VPP Manager determines the amount of power generated, sold, or stored at each point in time.
- Grid optimization: To maintain the stability of the grid, the optimum strategy for the grid is identified by the VPP Manager based on data drawn from the grid. This will conciliate between the power demand and generation and stabilize the voltage levels.

2) VPP in Hamburg, Germany:

Hamburg city in Germany has started a VPP project called Smart Power Hamburg [48]. The project aims at developing and demonstrating new approaches to city heating and electricity supply for the city, in order to support the goal of reducing CO_2 emissions by 40% by 2020 compared to 1990. The holistic approach of this project is to incorporate buildings with demand side management, combined heating and power plants (CHPs) and thermal storage systems to constitute a VPP operated with an advanced EMS, which can supply energy to the consumers and provide ancillary services to the electricity grid [48].

The heat supply of the city of Hamburg is provided by distribution networks that reside in a district heating network by using the network as a heat storage. The district heating network is operated by HAMBURG ENERGIE (HE). HE upgraded its facilities to distinguish their capabilities to create extra income by utilizing adaptability to go amiss from the heat driven CHP-operation. Furthermore, the development of the district heating system is planned. A subsequent increment of the heat demand prompts to a more adaptable and higher electrical generation, while a bigger district heating system with a decentralized generation structure permits more conceivable outcomes of adaptable plant operation.

The management system is a centralized controller responsible for analyzing the operation of distributed energy resources. This is done by collecting data from the schedule management and the VPP operators. The management system can also be used for trading personnel requests regarding future generation, or setting energy profiles to be met by the VPP. This control system is depicted in Figure 8.

D. Smart Emergency Systems

One of the smart city goals is to promote safety and security for its citizens. To this end, a smart emergency system is required that can be used for law enforcement, crime detection and prevention and dealing with accidents and natural disasters. For these applications, having an accumulation of intelligence through data collection and the ability to respond quickly and swiftly is very important. Different technologies for data collection can be used such as CCTV installations and smart traffic sensors. These data, along with predictive analysis, hold the potential to improve the quality of information used by the police, fire department and hospitals. According to [49], the focus of law enforcement agencies is shifting from identifying individual criminals to classifying groups based on threat levels.

Without a doubt, mass surveillance in smart cities brings forth multiple benefits in terms of safety and security. These benefits are achieved through the aggregation of data collected by sensors, cameras and tracking applications [50]. However, the continuous surveillance raises privacy issues, as all the collected data is analyzed by a single agency.

To realize a smart emergency system, sensors, big data analytics and information exchange technologies need to be combined. In case of accidents or natural disasters, acquiring the proper information, analyzing the data in a fast and efficient manner and relaying the information to the proper agencies are of great importance to save as much lives as possible. Therefore, it is crucial to create an efficient information exchange system that shares information between the rescuing agencies, allows for faster response and provides operation instructions for the rescue parties. An example of a smart emergency system is shown in Figure 9.

One of the cities currently deploying a smart emergency system is the city of Bhubaneswar in India. The city of Bhubaneswar has teamed with Honeywell Building Solutions to build a city-wide camera and video system to provide security, prevent crime and control traffic for visitors and more than 800,000 residents.

The installed system includes integrated CCTV cameras, automatic number plate reading cameras (ANPR) and a command and control center. A total of 114 CCTV cameras have been installed at strategic locations in the city, including high-traffic junctions, during the first phase. After completion, more than 350 CCTV cameras are envisioned to be installed at 90 locations, which can be controlled from the command and control center via a video wall interface. Police cars were also equipped with cameras [51].

Various scenarios can be handled by the system to notify the operators of different situations. Examples include: notifications when people are lingering around high-security areas and objects left unattended for a prolonged period of time. This enables the law enforcement agencies to quickly respond to these events. Moreover, detecting traffic violations through analyzing the video

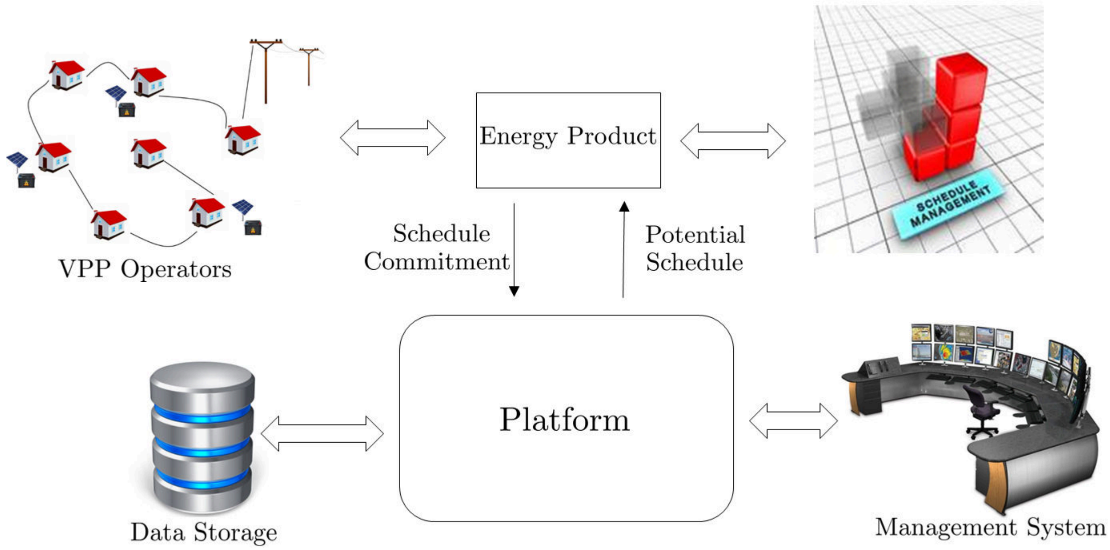


Fig. 8: Hamburg's virtual power plant platform.

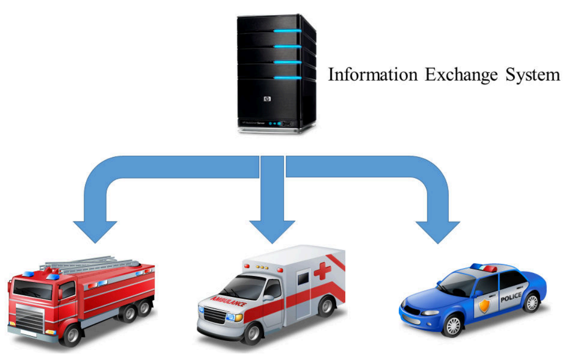


Fig. 9: Example of smart emergency system.

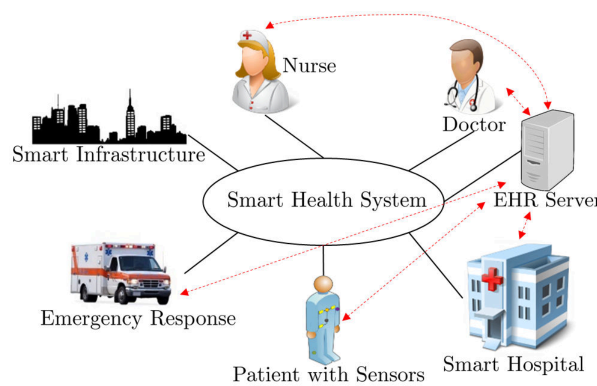


Fig. 10: Example of smart health system.

stream from the cameras is currently deployed and being expanded to multiple areas [51].

E. Smart Health

The current healthcare system faces significant challenges in providing quality and low-cost healthcare services. These challenges are also aggravated by the increasing elderly population, which translates into a horde of chronic diseases and higher demand for healthcare services [52]. Moreover, it is difficult in some cities to obtain a proper healthcare service due to limited resources. Due to this, the current healthcare system needs to evolve into a smart healthcare system. Smart healthcare is a concept involving various entities and technologies, including: sensors, wearable devices, Information Communication and Technology (ICT) and much more [53].

Other components of smart healthcare include: emerging on-body sensors, smart hospitals and smart emergency response. In smart hospitals, different technologies for their operation are used, including ICTs, cloud computing, smartphone applications and advanced data analysis techniques. The patients' data can be accessible in real-time from multiple offices within the hospital or multiple hospitals within the city. This allows the test data to be shared among multiple doctors, nurses and technicians, resulting in real-time decisions on patient health conditions and corresponding medication. An example of smart health systems is shown in Figure 10.

The current vision for a smart health system revolves around sensors that are deployed close to the patient's body [54], [55], or in the surrounding environment [56], [57]. Different body sensors can capture different physiological signs such as blood pressure and heart rate, while sensors deployed in the environment (home, clothes, etc.)

are used to observe the patient's activities or behaviors. In order to develop enhanced healthcare applications, sensor networks need to be combined with technologies such as activity recognition [58], [59], behavioral pattern discovery [60], [61], anomaly detection [62] and decision support [63].

The last building block of a smart health system is a user application platform. For example, the healthcare application platform SMART [64] is an open, standards-based technology platform that allows for seamless and secure operation of healthcare applications. The SMART standard is supported by an Electronic Health Record (EHR) system, which allows different parties to exploit various applications to improve the overall health system.

In the following, we present two examples of smart health projects from around the world.

1) Smart Health 2.0 Project:

The project is currently deployed in multiple cities in Italy. Despite being divided into multiple directions of research, the project's main goal is the innovation of technology infrastructure (specially in the Cloud) to develop beneficial services in the area of health and welfare. The project intends to work within the following areas of intervention:

- Prevention to reduce the incidence and progression of disease complications and comorbidities associated with it.
- Early diagnosis and treatment in the early stages of the disease which may improve outcomes.
- The integration and continuity of prevention and care.
- Monitoring and self-management.

The project's objective, from an infrastructure point of view, is to develop a prototype of the infrastructure based on Cloud computing to support the innovation and needs of healthcare applications [65]. The scope of the infrastructure is to have:

- Enabling platform: Which is an essential element to support the other components of the system.
- Technology platform for diagnostics: Which is aimed at the development of advanced sensors for real-time direct detection of clinical parameters.
- Semantics platform and documentary: In order to facilitate data exchange and heterogeneous information, based on open and integrated tools and technologies that will ensure full inter-operability between platforms and services.

As for the project's objective with respect to applications, the goal is the implementation of the EHR database that is able to provide an overall, unified vision of the health conditions of the citizens. The EHR also aims at the integration and the connection of collaborative environments, where different parties can collaborate in order to improve the health of patients [66].

2) Smart Health in Saensuk, Thailand:

Saensuk Smart City, a project by the Saensuk Municipality in Thailand in collaboration with Dell, Intel and the IoT City Innovation Center (ICIC), was launched based on multiple proofs-of-concept that can be extended to other smart applications. The first phase of the project is the implementation of a smart healthcare system to improve the quality of care towards Saensuk's elderly population. Around 15% of Saensuk's residents are ageing citizens, most of whom are living in nursing facilities or alone at home during the day with minimal care [67]. Launched in January 2016, the project targeted over 140 households with elderly members. The elderly patients are monitored in order to gain insights on how to efficiently manage the nursing resources and healthcare services.

In this project, elderly patients will wear a small bluetooth-enabled smart device. The smart device is used to monitor and collect data regarding movements, walking distance and sleep patterns. These data are used to detect unusual activities such as falling or activating a panic button, in which case healthcare practitioners as well as the family members are informed of the situation at hand.

Dell has implemented intelligent Intel-based gateway systems to aggregate and analyze the large amounts of health data generated daily by the smart devices. Relevant data and insights are sent to the municipal nursing headquarters cloud system, where city-wide updates can be displayed in real-time.

With access to patients' medical history and real-time data, local medical practitioners can identify specific emergencies and perform the best medical response needed for urgent cases. This led to resolving the challenge of limited human resource while meeting the demands for requested health support more swiftly and efficiently in case of emergencies [67].

IV. Data Acquisition

In smart city applications, the first step in the data's journey through the application is its collection by the different technologies deployed throughout the city. In order for smart cities to be able to manage the data and accommodate the citizens' needs, some aspects need to be considered. These aspects are data standards, data quality and data use.

Data standards are necessary in order for similar data to be treated in the same manner. Data quality refers to how much the acquired data is useful for the applications and Data use mainly focuses on specifying the range of applications for which the acquired data is useful. Due to the vast amount of heterogeneous data acquired by the different devices in smart cities, the cities need to combine different standards and different technologies into a unified framework to simplify data acquisition.

In the following sections, we start with an overview of the different technologies for data acquisition and survey the literature considering these technologies in the context of smart cities. We then conclude with future insights pertaining to data acquisition technologies in smart cities.

A. Data Acquisition Technologies

In this section, an overview of the different technologies for data acquisition is given. These technologies include Sensor Networks, MANETs, Unmanned Aerial Vehicles (UAVs), Vehicular Ad hoc Networks (VANETs), Internet of Things, Social Networks, 5G and Device-to Device (D2D) communication. We also provide a survey of the literature considering these technologies in the context of smart cities.

1) Sensor Networks

Sensor networks are used by a vast number of applications (*e.g.*, environment monitoring, waste management, health monitoring, smart grids, etc.), making it a key technology for collecting data in smart cities. Current cities are already deploying a wide range of sensors (*e.g.*, motion sensors, cameras, sensors for collecting environmental parameters, etc.). The main challenge for sensor networks is not the deployment of a large number of sensors around the city, but rather on how to provide proper semantics for the heterogeneous data used in different smart city applications. Since the literature is rich with studies that consider sensor networks in smart cities, we limit the survey to those works related to the use cases mentioned in Section III.

a) Sensor Networks for Smart Street Lights

The main sensors used in smart street light are motion sensors and brightness sensors. Data regarding pedestrians' movement, vehicles' movement and the amount of ambient light in the surrounding environment are collected through these sensors. These data are then used to determine when to turn a street light on or off. The authors in [37] and [68] use motion sensors to detect surrounding movements to turn a street light on or off, while the authors in [69]–[72] propose the deployment of WSN for smart street light to minimize the energy consumption. Abinaya et al. [73] turn on the lights ahead of a moving vehicle and turn off the lights behind it to reduce energy consumption. The vehicle's movement is detected through piezoelectric sensors.

b) Sensor Networks for Smart Traffic Management

The use of different types of sensors has been proposed in the literature for smart traffic management. Cheung et al. [74] propose the use of wireless magnetic sensors as an alternative for inductive loops for the purpose of traffic surveillance. Wireless sensor networks have been used in [75] for traffic routing and over speeding detection, in [76]–[78] for parking applications, in [79], [80] for an intelligent traffic signal control system, in [81] for road safety applications and in [82] for monitoring vehicles' behavior to name a few.

c) Sensor Networks for Virtual Power Plants

Moghe et al. [83] proposes the use of smart stick-on sensors for smart grid monitoring. Stick-on sensors are low-cost, self-powered universal sensors that can monitor different parameters of the smart grid. Moghe et al. [84] propose the use of voltage sensors for utility network asset management. Chang et al. [85] proposes the use of energy-harvesting wireless sensors for smart grid monitoring. Erol-Kantarci and Mouftah [86] propose an in-home energy management application for demand-supply balancing, where the communication between the consumer and the controller utilizes wireless sensor networks. Barbato et al. [87] monitor the energy consumption of household appliances through wireless power meter sensors. Gungor et al. [88] discuss the challenges and opportunities of using wireless sensor networks in smart grid applications.

d) Sensor Networks for Smart Emergency Systems

In smart emergency applications, sensors are used to collect data from the surrounding environment. These data are then sent for processing in order to deduce an emergency situation. Bruckner et al. [89] goal is to establish communication paths between sensors for surveillance applications. Sathishkumar and Rajini [90] propose the integration of sensor networks and GSM to detect trespassers. Systems integrating WSN and cameras are proposed in [91] and [92] for human identification and tracking.

e) Sensor Networks for Smart Health

Lee and Chung [93] design a shirt equipped with Body Area Sensor network for monitoring purposes. Virone et al. [94] use body sensor network for monitoring vital signs and uses WSN for monitoring the environment (*e.g.*, temperature, light, etc.). Otto et al. [95] propose a system architecture based on WSNs for ubiquitous health monitoring. The authors in [96]–[98] discuss the challenges and potentials of using WSNs for healthcare applications. Liao et al. [99] propose a flexible wireless body area sensor model to maintain quality of service in terms of fast transmissions and energy efficiency. Furthermore, Arifuzzaman et al. [100] propose the use of a chemical sensor to detect infections around biomedical implants.

2) Mobile Ad hoc Networks (MANETs)

MANETs are infrastructure-less networks consisting of mobile devices, which communicate with each other wirelessly [138]. The main challenge is to maintain required information for proper routing. Jabbar et al. [101] evaluate different routing protocols for MANETs

TABLE V: DATA ACQUISITION CHALLENGES IN SMART CITIES

Technology	Advantages	Limitations and Challenges	References
Sensor Networks	• Scalability • Easy Deployment in Harsh Environments • Relatively Cheap	• High Concurrent Network Access • Limited Coverage • High Real-Time Transmission • Semantic Representation and Processing • Standardization	[37], [68]–[100]
MANETs	• Infrastructure-less • Fault Tolerance • Scalability	• Non-Uniform Node Distribution • Use of Multiple Communication Technologies	[101]–[104]
VANETs	• Sufficient Computational Resources • Enhanced Traffic Safety	• Dynamic Topology • Bandwidth Limitation and QoS • Signal Fading and Fast Movement of Nodes • Security and Privacy	[105]–[109]
IoT	• Daily Tasks Automation • Relatively Cheap • Tracking Capabilities	• Standardization • Data Analysis and Fusion • Scalability	[110]–[114]
UAVs	• Easy Deployment in Harsh Environments • Lower Risk for Human Operators • Relatively Cheap	• Coverage Issues • Battery Recharging	[115]–[121]
Social Networks	• Citizens' Empowerment • Worldwide Connectivity	• Noisy Data • Data Literacy • Privacy Issues	[122]–[126]
Crowdsourcing	• Citizens' Empowerment • Relatively Cheap • Collective Intelligence	• System Integrity and Confidentiality • User Integrity and Trustworthiness	[127]–[134]
5G	• Large Bandwidth • High Speed	• Standardization	[135], [136]
D2D	• Enhance Spectral Efficiency • Energy Efficiency	• Interference Management	[137]

for VoIP, HTTP and FTP applications in the context of smart cities. Bellavista et al. [102] and Cardone et al. [103] propose the integration of MANETs and WSNs urban data acquisition. To maintain data security and privacy in smart cities, Didolkar and Zama [104] propose an architecture based on MANETs and IoT.

3) Vehicular Ad hoc Networks (VANETs)

VANETs are a type of MANETs that are extensively studied in the context of smart mobility and intelligent transportation systems. VANETs facilitate V2V and V2I communications. Since VANETs are a special type of MANETs, the problems that plague MANETs also influence the data acquisition process in VANETs. Different types of applications can utilize the data collected in VANETs to provide various services for users [105]. These applications can be categorized into safety and infotainment applications. Safety applications are used to improve road safety, such as forward collision warning, while infotainment applications are geared towards comfort and entertainment for vehicle passengers, such as traffic and weather information.

The nature of VANETs and its application requirements (*i.e.*, strict latency for safety applications) add to the challenge of data acquisition in VANETs. Data acquisition problems are further exacerbated by the use of different types of technologies [105].

4) Internet of Things (IoT)

IoT is the next step in the evolution of the Internet, which leverages ubiquitous connectivity to empower inter-networking and communication between physical devices. The devices can be smart home appliances, weather and temperature sensors, vehicles or buildings. IoT's architecture can be divided into three domains: Sensing, Network and Application [139]. The Sensing domain enables IoT devices to interact with each other and collect data from the physical world. The Network domain utilizes standard technologies to collect data from sensing domain devices and transfer them to remote locations for further processing. The Application domain is responsible for the final processing of the collected data and providing services. Key data acquisition technologies of IoT include sensors and embedded systems. Since IoT gathers data from many different types of sensors across different types of devices, it presents many challenges. These challenges are briefly presented in Table V.

5) Unmanned Aerial Vehicles (UAVs)

UAVs can be used by smart cities to collect data from regions where it is difficult to deploy other technologies for data collection. Challenges for deploying UAVs include ensuring coverage and battery recharging. DAloia et al. [115] use images captured by UAVs for empty parking space detection. Mohammed et al. [116] discuss the challenges and the potential of using UAVs in smart cities highlighting the city of Dubai [117]. Ermacora et al. ([118] and [119]) develop a cloud-robotic service using UAVs for emergency management operations in smart cities. Witayangkurn et al. [120] propose a system that integrates UAVs and sensors to develop real-time monitoring systems. Xie et al. [121] develop a long distance communication system using UAVs for smart city applications such as emergency response.

6) Social Networks

Smart cities can use information posted by citizens on social media such as Facebook and Twitter as a source of data. Posted status can be a great source of feedback for different aspects of smart city services. Psomakelis et al. [122] and Aisopos et al. [123] propose an architecture for the retrieval and analysis of big datasets stemming from social networking sites and IoT devices for use in smart city applications. Samaras et al. [124] also propose an architecture that aggregates social networks and sensors in support of smart city services. Chifor et al. [125] propose a security architecture based on IoT and social networks that enables adaptive sensing as a service. Clarke and Steele [126] propose the use of fitness data posted by users on social network for smart healthcare and urban planning applications.

7) Crowdsourcing

Cities can adopt crowdsourcing techniques and applications such as Waze [140] to encourage the citizens to play a vital role in providing data or services to other citizens. This way, citizens can submit their input (*i.e.,* opinion on a service or an answer to a problem), which helps in achieving the goal of a smart city. Crowdsourcing has been used in some smart cities to achieve the goal of an "open government" such as the city of Louisville, USA. The latter joined Waze's Connected Citizens Program [43] where information about the current traffic state are being shared with Louisville Metro Government. This way, the congestion hotspots can be identified and the collected data can be leveraged to provide better road experience for the drivers.

Different works have targeted the use of crowdsourcing in smart cities. Cilliers and Flowerday [127] investigate the main factors that must be incorporated in crowdsourcing to address the security concerns (confidentiality, integrity and availability) of the citizens. Pouryazdan et al. [128] take an opposite point of view by evaluating an anchor-based voting system to identify the integrity and trustworthiness of the users, where an anchor is a fully-trusted user. Chowdhury et al. [129] review the use of crowdsourcing in different smart city applications such as education, healthcare and environment, and the incentive models used to encourage the citizens to participate in the decision-making process in smart cities. Schuurman et al. [130] investigate the advantages and disadvantages of using crowdsourcing for the generation and selection of ideas for ICT innovation. Cen et al. [131] take a theoretical approach of task recommendation for workers participating in mobile crowdsourcing, where the problem is formulated as a stochastic integer linear program to maximize the expected total utility of all workers. Through a study survey, Breetzke and Flowerday [132] conclude that using an Interactive Voice Response system in smart city crowdsourcing is beneficial. Cardone et al. [133] propose a crowdsourcing architecture along with an Android-based platform to manage the crowdsourcing process. Mirri et al. [134] present a case study of using crowdsourcing to provide better routes to citizens with disabilities.

8) 5G

Due to the increasing number of mobile devices in cities, 5G is expected to play a vital role in the development of smart city applications. The development of 5G is based on the use of new Radio Access Technologies, use of higher frequencies and antenna improvements [141]. Orsino et al. [135] study the integration of 5G, IoT and D2D for data acquisition in smart cities. Beard [136] identifies the challenges faced by the use of 4G and 5G in smart cities.

9) Device-to-Device (D2D)

D2D refers to radio communication technology where devices can exchange data directly without traversing through base stations or access points. Infrastructure-less services can greatly benefit from D2D communications. A possible scenario would be to provide safety communications in case of infrastructure damage. Furthermore, D2D promises to provide peer-to-peer (P2P) and location-based services [142]. D2D is specified by 3GPP in LTE Release 12 [143] and can use both licensed and unlicensed spectrum.

B. Insights and Research Challenges

In the previous subsection, we have discussed the different data acquisition technologies that can be used in smart cities along with the specific challenges and limitations faced by each technology. However, overcoming these limitations independently is not enough for the realization of a smart city. In the following, we discuss the challenges that smart cities need to address when considering data acquisition technologies and draw insights towards the realization of the smart city.

1) Coordination and Management

Due to the different methods for collecting data in smart cities, it is critical to have a clear coordination among the different technologies and the agencies managing those technologies. This stems from the smart cities' desire to be governmentally smart [3]. Having a clear view of the coordination, collaboration and management of data acquisition technologies will contribute to smarter decisions that will enhance the citizens' quality of life.

For example, when considering tracking applications (*i.e.,* tracking of a suspecting vehicle), different technologies can be combined for better tracking. Visual sensors (*i.e.,* cameras) are usually used for tracking purposes. In areas where cameras are not deployed, VANETs and 5G can be used to provide a continuous monitoring of the target vehicle. Without a proper coordination among the agencies responsible for the different technologies and the law enforcement department, the targeted vehicle may be lost, which leads to public safety concerns.

2) Ensuring Data Quality and Integrity

Due to the large volume of data generated by smart city applications, the standards and technologies for ensuring data quality and integrity should be revisited. The new technologies should be able to scale well in the face of explosive growth in data. Technologies should also be able to identify "good" data as fast as possible.

This challenge is more pronounced in smart city applications that generate large volume of data, such as smart traffic management and smart grid. In smart grid, for example, large volume of data is being collected from different customers. These data contain useful information such as usage patterns and failure indications. These data are used by the power grid operators to optimize their performance, quickly fix any power failure and lower the overall power consumption of the city. However, if data quality and integrity are not ensured, the collected data may be compromised and the power grid operators may take the wrong decisions.

Another example is smart traffic management, where ensuring the data quality and integrity can help in optimizing the traffic flows within the city (*e.g.,* when to turn traffic lights red or green at intersections, suggest alternative routes in case of detours), providing better road experience for the citizens (*e.g.,* less VMT), and scheduling road maintenance when the traffic is low.

Since social networks and crowdsourcing can be used as a way for collecting data, the citizens should engage in ensuring the quality and integrity of the data they share, as this will help in improving the citizens' quality of life. This will also encourage the citizens to participate in the smart city vision of having smart people [3]. Smart traffic management can benefit from the participation of citizens' in both collecting data and ensuring data quality and integrity. Drivers can report traffic jam locations (*e.g.,* due to a road block or an accident) or suggest alternative routes, so that other drivers can be well informed about traffic situations down the road.

3) Cloud vs. Fog Computing

Depending on the smart city applications, the agencies managing the different data acquisition technologies should decide whether to send the data to the cloud to be processed or should the data be processed locally. In other terms, the agencies should choose between cloud computing and fog computing. The decision is affected by the nature of the smart city applications, the time restrictions required by the applications and the processing capabilities of the devices constituting the fog. For example, in smart street lighting, processing data to decide when to turn on the street lights ahead of a vehicle and when to turn off the lights behind it can be done locally. On the other hand, processing data collected for smart grid applications containing usage patterns are better off being processed at the cloud.

4) Energy Efficiency

As one of smart city goals is to be environmentally smart [3], the data acquisition tools, techniques and standards need to be revisited in light of lower power consumption. Data acquisition tools (*i.e.,* UAVs, VANETs) need to reduce their carbon footprint. This can be realized by making these tools more energy-efficient, or by incorporating renewable energy sources, where the stored energy can be used at later times.

For example, body area sensors used to monitor patients' vitals need to be extremely energy efficient, as it is desirable for these sensors to work for a prolonged period of times without frequently changing batteries. Another example is weather monitoring, where the different sensors distributed throughout the city need to be energy-efficient. These sensors can benefit from renewable energy sources to reduce their carbon footprint.

The data acquisition techniques should also be refined to be energy-efficient. For example, optimizing sensors' locations, transmitting methods and perhaps scheduling can further lower their power consumption. Using new techniques such as RF and Visible Light Communication (VLC) backscattering, which are starting to show promise in terms of energy efficiency [144]–[146], can also help in lowering the power consumption.

V. Data Processing

In this section, we survey data processing, the second phase of the data's journey through the smart city applications. We begin by discussing techniques for discovering patterns in the collected data, which will identify the potential uses for the data, followed by discussing techniques for data presentation to bring data to life.

A. Knowledge Discovery

One important challenge faced by a data-centric smart city is the pattern and knowledge discovery from the large amount of heterogeneous data collected by different data acquisition approaches as discussed in Section IV. Different knowledge discovery technologies can be used in the context of smart cities to address the above-mentioned challenge. In the following subsections, we discuss the role of machine learning, Deep learning and Real-time Analytics in the context of smart cities for knowledge discovery.

1) Machine Learning

Machine learning is a type of artificial intelligence (AI) where computers are given the ability to learn without being explicitly programmed [147]. A formal definition of machine learning provided by Tom M. Mitchell is "A computer program is said to learn from experience E, with respect to some class of tasks T, and performance measure P if its performance at tasks in T, as measured by P, improves with experience E" [148]. The goal of machine learning is the development of self-taught computer programs that adapt to new data. Machine learning algorithms are used to infer patterns in the data in order for the program to adjust its actions accordingly. In this subsection, we briefly discuss machine learning algorithms and platforms and delineate the use of machine learning in smart cities.

Generally, machine learning is classified into reinforcement learning, supervised and unsupervised learning. Reinforcement learning algorithms are defined by a quintuple, the set of states (including a beginning and final states), actions, transitions, policies and rewards. Each transition, from a state-action pair to another either earns a rewards or a penalty. The objective is to chose transitions from the beginning to the final state that maximize the rewards in the long-term [149].

Supervised and unsupervised machine learning depend on the presence or absence of training data, respectively. In supervised learning, the algorithm is given an example of the input data and the corresponding label (*i.e.*, desired output). The algorithm then infers patterns from these labeled training data, which are later applied to new data sets. On the other hand, in unsupervised learning, the data is not labeled and the algorithm has to discover the hidden patterns within the data.

One of the main challenges in machine learning is to find appropriate data sets from massive urban data for training purposes and to meet the specific needs of the applications. The urban dynamic measuring research (*i.e.,* measuring how the movement of people, objects and data change in a city) often requires that the urban data set should cover as many urban dynamic features as possible. At the same time, the data needs to be as uniform as possible to meet the applications' needs. Data set requests create significant challenges for the collection, management and mining of urban data. Solving the problem of data set selection and data combination is a key challenge for smart city applications.

a) Machine Learning Algorithms

Machine learning algorithms can be further classified into different types of algorithms based on their algorithmic perspective. Some of these types include Clustering, Instance Based and Decision Trees. Clustering is a type of unsupervised machine learning. The clustering methods aim at grouping the data that share mutual properties based on the structure of the data, for example, k-means and k-medians algorithms. Instance Based is a type of supervised machine learning, which requires training data. In instance-based learning, the algorithm makes decisions about new data by comparing it to training data, using a similarity metric. Through this comparison the algorithm can make a prediction and the find the best match for the new data. Examples of instance-based supervised machine learning algorithms are k-Nearest Neighbor and Self-Organizing Map. Decision Trees are a type of supervised machine learning usually used for classification and regression problems. Decision tree methods build a tree structure for decision-making based on real values. When a new data is introduced to the decision tree, it traverses the tree until a decision is reached. Advantages of this method are its speed and accuracy (under the assumption of accurate training data sets). Examples include Classification and Regression Trees. More on machine learning algorithms can be found in [150]–[152] A taxonomy of the types of machine learning algorithms is summarized in Figure 11.

Machine learning has been extensively studied in the literature and many surveys discuss machine learning from different perspectives. For example, Zhu [154] provides a survey on semi-supervised machine learning, Caruana and Niculescu-Mizil [155] provide an empirical study for supervised algorithms where a variety of performance criteria are used to evaluate the learning algorithms. Buczak and Guven [156] focus on surveying machine learning use in support for intrusion detection. Other works on machine learning algorithms include

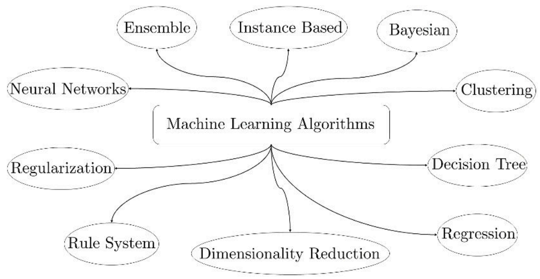


Fig. 11: Taxonomy of machine learning algorithms [153].

[150], [157]–[159]

b) Machine Learning Platforms

In this section, we provide a comparison between five machine learning platforms: Amazon ML, Microsoft Azure ML, Google Prediction API, BigML and IBM Watson machine learning.

Amazon ML [160] is a relatively new service provided by Amazon to obtain predictions for applications using simple Application Programming Interfaces (APIs), without the need of implementing custom generation code or managing infrastructure. Amazon ML provides visualization and wizards to build the machine learning models. Although Amazon ML provides scalable and high throughput models, it suffers from the limited functionality in terms of importing data (through Amazon AWS only) and data preparation (provides basic data cleaning only) and does not allow an extension of the built-in algorithms or a creation of new ones.

Microsoft Azure ML [161] is a cloud predictive analytics service that quickly creates and deploys predictive models as analytics solutions. Azure ML provides a workflow and a visual editor for users to create their own models, supports different types of data sources (CSV, SQL data base, etc.), provides advanced data cleaning functionalities and gives provision to extend built-in algorithms.

Google Prediction API [162] provides a RESTful API to build machine learning models. The users are responsible for managing their data (*i.e.* cleaning and transformation) before submitting it as training data to the API. Google Prediction API is suitable for small scale models but it does not allow for extension of built-in algorithms or creation of new ones.

BigML [163] offers cloud-based and on-premise machine learning services, distributed systems and data visualization. BigML has pioneered the machine learning as a Service (MLAAS) wave of innovation through its consumable, programmable and scalable software platform. It streamlines the creation and deployment of smart applications powered by the state-of-the-art predictive models. Data can be uploaded through a web interface or through a RESTful API. These data are used for training the models and generating predictions. BigML provides evaluations for the models through performance metrics or results comparisons.

IBM Watson [164] is a Question Answering (QA) computing system aiming at providing the best answer to a question posed by users through the use of different natural language processing and machine learning algorithms. Watson supports different types of questions from different data sources and provides advanced data cleaning functionality. It returns the best answer after comparing the results of different algorithms.

Table VI provides a comparison of the above-mentioned machine learning platforms. From this table, we note that due to the differences in the properties of the platforms, they are suitable for different smart city applications. For example, Smart grid applications can greatly benefit from the ability of the platform to create/extend the algorithms, to perform advanced data cleaning and transformation and to support different data sources, in which case Azure ML, BigML and IBM Watson are good candidates for processing smart grid data.

c) Machine Learning and Smart Cities

Machine learning can be used in smart city projects to extract useful data for assessing the way the city is working [165]. An example of the use of machine learning in smart city projects has been demonstrated in the smart power grid project of New York city [166]. Here, the machine learning algorithms are used for transforming historical electrical grid data into models that aim to predict the risk of failures for components and systems. These models can then be used directly by power companies to assist with prioritization of maintenance and repair works.

Other examples of applying machine learning algorithms in smart city projects include traffic flow optimization [167] to predict the best route for a user with a particular destination. Ertugrul and Kaya [168] estimate the energy efficiency of the buildings for the purpose of smart city planning. Parvez et al. [169] uses machine learning algorithms for the purpose of securing the metering infrastructure of smart grids. The above-mentioned works apply machine learning algorithms on data stored in the cloud. Raising network congestion issues, Valerio et al. [170] proposes a distributed machine learning approach that processes the data where it is collected (*i.e.*, at the sensors).

As for data acquisition techniques that make use of machine learning, several works have considered the use of machine learning in WSNs in order to solve network associated problem, such as energy-aware communication [171]–[175], optimal deployment and localization [176]–[179], resource allocation and task scheduling

TABLE VI: COMPARISON OF MACHINE LEARNING PLATFORMS

		Amazon ML [160]	Azure ML [161]	Google API [162]	BigML [163]	IBM Watson [164]
Support for Different Data Sources			✓		✓	✓
Data Cleaning and Transformation Capabilities		Basic	Advanced	Basic	Advanced	Advanced
Support for Different Algorithms		Limited	✓	✓	✓	✓
Allows Extension/Creation of Algorithms			✓		✓	✓
Algorithm Evaluation Using Performance Metrics		✓	✓		✓	
Algorithm Evaluation Using Results Comparison			✓	✓	✓	✓
Support for Parameter Tuning		Limited	✓	Limited	✓	✓
Potential Smart City Applications	Smart Street Light	✓				✓
	Smart Traffic Management	✓		✓		✓
	Smart Power Grid		✓		✓	✓
	Smart Emergency System	✓				
	Smart Health	✓				✓

[180]–[182], information processing [183], [184], target tracking [185], [186] and target identification [187], [188].

In MANETs, machine learning has been used to achieve different objectives. These objectives range from location prediction [189], [190], adaptive scheduling and offloading [191], data dissemination [192], intrusion detection and identification of malicious nodes [193], [194] and routing protocols [195]. Similarly, in VANETs, machine learning algorithms have been used for packet prioritization [196]–[198], packet routing and prediction of link breakage [199], [200], location and shock wave prediction [201], misbehaviour detection [202], [203], development of safety applications [204] and detection of traffic accidents [205].

machine learning in UAVs has been incorporated into image processing for altitude estimation [206], swing-free trajectory planning for cargo delivery [207]–[209], intelligent control of UAVs [210], information processing for disaster response [211] and velocity prediction [212].

Lastly, the interaction between machine learning and IoT raises many challenges. The main challenge of incorporating machine learning approach with IoT data analytics is to process large data sets to find meaningful domain-specific insights. For example, in case of smart grid utility domain, it is important for utilities to gain a strong understanding of electricity usage for the city and neighborhoods to assess further needs, load balancing and load shedding [213]. Different ideas have been proposed that combine machine learning algorithms with IoT technology. Zhang et al. [214] propose a semantic framework that integrates the IoT with machine learning for smart cities. The proposed framework retrieves and models urban data for certain kinds of IoT applications based on semantic and machine learning technologies. Vijai and Sivakumar [215] discuss the use of machine learning algorithms and IoT devices for a water management system in India. Rathore et al. [216] proposes a combined IoT-based system for smart city development and urban planning using Big Data analytics.

machine learning has also been used in data dissemination technologies, such as Publish and Subscribe services. QoS-enabled publish/subscribe middleware provides the infrastructure needed to disseminate data predictably, reliably and scalably in distributed real-time and embedded systems. For systems operating in changing environment, adapting in a timely manner with accuracy is of great importance. Hoffert et al. [217] combines multiple machine learning approaches with publish/subscribe middleware to address the above-mentioned challenge. Katakis et al. [218] propose web-based news reader that incorporates a machine learning framework for dynamic content personalization. Other works such as [219] and [220] use machine learning approaches to filter data for dissemination.

The machine learning algorithms in the above-mentioned works can be categorized as supervised or unsupervised. In the context of smart cities, providing a properly labeled training data set for supervised learning algorithms from the large volume of heterogeneous data is a major challenge. While in unsupervised learning, which does not require a training data set, working through these heterogeneous data can be time consuming. Therefore, semi-supervised learning, which strikes a balance between these two categories, can be a viable option when designing machine learning algorithms for smart cities.

2) Deep Learning

In this section, we start by providing discussions regarding deep learning algorithms and platforms, then we survey the use of deep learning in smart cities. Although deep learning is part of machine learning, we dedicate a separate section to deep learning due to the big interest in this area, both from academia and industry.

a) Deep Learning Algorithms

Deep learning is a set of algorithms in machine learning with the goal of modelling high-level data

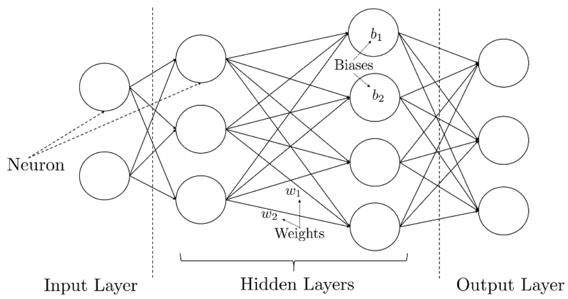


Fig. 12: Example of a Neural Network.

abstractions using linear and non-linear transformations [221], [222]. Neural networks are the core of deep learning techniques. A neural network consists of a set of nodes (neurons) connected together by edges, where biases are associated with neuron and weights are associated with edges. An example of a neural network is illustrated in Figure 12, where b_1 and b_2 represent the bias values of the corresponding neurons and w_1 and w_2 represent the weights of the corresponding edges. A neural network's main function is to perform progressively complex operations on received data and then use the output to solve a problem. Neural networks are used for different applications such as character recognition and image compression.

Neural networks are highly structured with layers. The first layer is the input layer, the final layer is the output layer and all layers in between are referred to as hidden layers. Deep learning discovers sophisticated structure in large data sets by using algorithms to suggest how a machine should adapt its internal parameters (*i.e.*, weights and biases) from one layer to another for data representation.

For analyzing simple patterns in data, basic classification techniques such as Support Vector Machines (SVM) are suitable. As the patterns get complicated, neural networks outperform other methods. However, neural networks also suffer from scalability. As the patterns grow in complexity, the number of nodes (neurons) in each layer also grows exponentially with the number of possible patterns in the data. In such cases, the training becomes more expensive (in terms of time and space complexities) and the accuracy starts to suffer. Typically, to overcome this challenge, deep networks are employed. They are able to break the complex patterns into a series of simpler patterns, which are then combined to analyze the data. There are different models for deep learning. In the following, we briefly discuss two of the most important deep learning models: Restricted Boltzmann Machines (RBM) and Long Short Term Memory (LSTM).

Restricted Boltzmann Machines (RBM): In this unsupervised method the patterns in data are found automatically by reconstructing the input. An RBM network has two layers: the first layer is known as the visible layer and the second is called the hidden layer. Each node in the visible layer is connected to every node in the hidden layer. The training of an RBM involves iterating through three steps until a desirable level of accuracy is achieved. The first step is called the *forward pass*, where every input is associated with weight and bias and the result is passed to the hidden layer. Depending on the result, neurons in the hidden layer may or may not be activated. The second step is called the *backward pass*, where each activation is associated with weight and bias, and the result is passed back to the visible layer for reconstruction. In the third step, the original input and the reconstructed input are compared by the visible layer. If the desired level of accuracy is achieved, the training stage terminates and the network is ready to work on new data. Otherwise, the weights and biases are adjusted and the three steps are repeated again.

Long Short Term Memory (LSTM): The main motivation behind the use of LSTM is to deal with the problems of *vanishing* and *exploding gradients*. Vanishing gradient can cause the deep learning algorithm to either learn at a very slow pace or stop learning altogether, while exploding gradients can cause the learning algorithm to diverge. LSTM allows a neuron cell to read, write, or erase the current state of the cell via gates. These gates perform action based on the received signal. During the learning process, these gates learn when to pass, block or delete the incoming data. More on LSTM can be found in [223] and [224].

b) Deep Learning Platforms

In this section, we provide a brief description and a comparison of four widely used deep learning frameworks. These frameworks are: Theano, TensorFlow, Caffe and Torch.

Theano [225] is a free Python symbolic manipulation library under a BSD license, aiming to improve execution and development times for machine learning algorithms. It has specifically been utilized for the gradient-based methods such as deep learning that require repeated computation of the tensor-based mathematical expressions. Such mathematical expressions can be rapidly coded in Theano using a high-level description language, similar to a functional language, that can be compiled and executed on either a CPU or a GPU.

TensorFlow [226] is a C++ based deep learning framework along with Python APIs. TensorFlow uses data flow graphs for performing numerical computations and has a flexible architecture that supports multiple backends, CPU or GPU on desktop, server or mobile platforms.

Caffe [227] is a deep learning tool developed by the Berkeley Vision and Learning Center. It separates

TABLE VII: COMPARISON OF DEEP LEARNING PLATFORMS

	Theano [225]	**TensorFlow [226]**	**Caffe [227]**	**Torch [228]**
Base Language	Python	Python/C++	C++	Lua
Programming Paradigm	Declarative Programming	Declarative Programming	Imperative Programming	Imperative Programming
Distributed Execution		✓		

the definition of the network architecture from actual implementation allowing to conveniently and quickly explore different architectures and layers on either CPU or GPU. Caffe is developed in C++ and has command line, Python and Matlab interfaces for training and deployment purposes.

Torch [228] is a framework built using Lua that supports deep learning algorithms. Its goal is to provide a flexible environment to design and train learning machines. Torch has strong CUDA and CPU backends and contains well-developed, mature machine learning and optimization packages. Although the use of Lua allows for rapid prototyping and quick execution, its limited API and libraries make industrial deployment harder compared to a Python based library.

These frameworks are summarized in Table VII. From this table, we note that for smart city applications that require processing of large volume of data, TensorFlow may be a good candidate due to its distributed execution.

c) Deep Learning and Smart Cities

Deep learning methods have been used for different applications in smart cities. For example, Han and Sohn [229] use Deep Belief Networks to divide Seoul's metropolitan area into homogeneous zones based on the travel patterns of the residents. Wu et al. [230] discuss the application of deep learning for smart water management networks. Alsheikh et al. [231] use deep learning and a framework over Apache Spark for mobile big data analytics.

Dedinec et al. [232] use a Deep Belief Network for electricity load forecasting in the city of Macedonia. The network consists of multiple layers of restricted Boltzmann machines, where unsupervised training is augmented by a supervised back-propagation training for fine tuning. The work considers the Mean Absolute Percentage Error (MAPE) as a performance metric. In comparison to other schemes, the proposed network is able to reduce the MAPE by around 9% for a 24-hour prediction, while reducing the MAPE for daily forecasting by 21%.

He et al. [233] propose a Recurrent Neural Network (RNN) for real-time optimization of pricing in smart grids. Through non-smooth analysis and differential inclusion, the proposed network can converge to an optimal solution. Aryal and Dutta [234] propose a framework that is based on deep learning for urban object detection from high-resolution images, with the objective of minimizing issues of accessing big data and increasing the efficiency of monitoring and planning.

In the field of smart traffic, Tian and Pan [235] propose the use of RNN for traffic flow prediction. The proposed network is able to accurately capture the randomness of the traffic flow. Through the use of memory blocks, it can store longer historical data, which offers better performance in terms of prediction accuracy and helps overcome back-propagated error decay issues. In order to find fastest routes, Niu et al. [236] combine a deep learning approach for processing spatial and temporal GPS traces with a dynamic weighted classifier that assigns traffic condition vector for each road segment. These vectors are used to find the fastest routes based on the current traffic condition.

Liang et al. [237] combine recurrent neural networks with geographical spatial data processing and parallel streaming analytical programming for crowd density prediction in metro areas. Through the use of Caller Detail Record (CDR) of the mobile users, the proposed scheme is able to predict the number of passengers entering a station and the number of passengers waiting on the platform, among other metrics related to crowd sensing.

Table VIII provides a summary of the literature incorporating machine learning and deep learning into different aspects of smart city projects.

3) Real-Time Analytics

Real-time analytics refers to the processing of data within a certain deadline from when they enter the system. There are different applications in which large amounts of data generated in external environments are pushed to servers for real-time processing. These applications include sensor-based monitoring, web traffic processing and network monitoring. In this section, we provide a discussion on real-time analytics algorithms and platforms and survey the use of real-time analytics in smart cities.

a) Real-Time Analytics Algorithms

In this section, we review three algorithms used for real-time analytics: Bloom filter, Hyperloglog and Minhash.

Bloom Filter [243] is a probabilistic algorithm that is used to determine whether an element is in a set or not. The algorithm uses an array of M bits (initially set to

TABLE VIII: SUMMARY OF MACHINE LEARNING AND DEEP LEARNING IN SMART CITIES

Category	Ref.	Algorithm's Type	Objective	Performance Metrics	Computing Platform	Potential Integration with other Technologies	Potential Smart Projects					Advantages	Limitations
							Smart Street Light	Smart Traffic	Power Grid	Emergency System	Smart Health		
Machine Learning	Rudin et al. [166]	Ranking / Classification	Failure Ranking and Prediction	Mean Time Between Failures	Cloud Computing	IoT, PLC			•			Suitable for Prioritization	Large Volume of Training Data
	Ouerhani et al. [238]	Decision Tree	System Implementation	-	Cloud Computing	IoT, WiFi	•					Simple Interpretation	Data Overfitting
	Krishnan et al. [167]	Decision Trees	Traffic Flow Optimization	Travel Time	Cloud Computing	IoT, LiFi		•				Simple Interpretation	Data Overfitting
	Kaya et al. [168]	Extreme Learning Machine	Energy Efficiency Estimation	MSE, MAE, MRE, MAPE	Cloud Computing	IoT			•			Less Training Error	Data Overfitting
	Parvez et al. [169]	Instance Based	Securing Data from Power Meters	MSE	Fog Computing	IoT, PLC, WiFi			•			Adaptability to New Data	Memory Intensive
	Valerio et al. [170]	Classification	Reducing Network Overhead through Distributed Machine Learning	Prediction Loss, Accuracy Gain	Fog Computing	IoT				•		Distributed Implementation	Large Volume of Training Data
	Garcia et al. [239]	SVM	Anomaly Detection	True Positive Rate	Cloud Computing	WSN, IoT		•		•		High Accuracy	Standardization
	Fleury et al. [240]	SVM	Activity Classification	Classification Accuracy	Fog Computing	Sensor Networks					•	High Accuracy	Standardization
	Longstaff et al. [241]	Classification	Improving Classifier's Accuracy	Accuracy	Fog Computing	Mobile Phones					•	Improved Accuracy	Large Volume of Training Data
Deep Learning	Dedinec et al. [232]	Deep Belief Network	Electricity Load Forecasting	MAPE	Cloud / Fog Computing	IoT			•			Highly Customizable	Memory Intensive
	He et al. [233]	Recurrent Neural Networks	Real-Time Electricity Pricing	Optimal Real-Time Price	Cloud Computing	IoT			•			Suitable for Time Series Analysis	Memory Intensive
	Aryal et al. [234]	Deep Neural Networks	Object Recognition	Classification Accuracy	Cloud Computing	WSN, UAVs		•		•		High Accuracy	Choosing the Right Topology
	Tian et al. [235]	Recurrent Neural Networks	Traffic Load Prediction	MAPE, RMSE	Fog Computing	VANET		•				Suitable for Time Series Analysis	Memory Intensive
	Niu et al. [236]	Restricted Boltzmann Machine	Finding Fastest Driving Routes	Accuracy / Travel Time	Fog Computing	VANET		•				No Need for Labeled Data	Time Consuming for Training
	Liang et al. [237]	Recurrent Neural Networks	Population Density Prediction	MAPE	Cloud Computing	4G/5G		•				Suitable for Time Series Analysis	Memory Intensive
	Fang et al. [242]	Deep Belief Network	Human Activity Recognition	Accuracy	Fog Computing	Sensor Networks					•	Highly Customizable	Memory Intensive

zeros) and K hash functions, where typically $K < M$. Elements are fed to the hash functions to produce K array positions per element and these positions are set to 1 in the array of M bits. To determine if an element is included in a set or not, the filter will apply the hash functions to the element and check the array positions returned by the hash functions. If any of those positions is set to 0, then the element is definitely not in the set. Otherwise, the element is probably in the set. Due to the nature of the algorithm, false positives are possible, but false negatives are not.

Hyperloglog [244] is an algorithm used to count the distinct elements in a set. The algorithm applies a hash function to every element in the set to produce a new set with the same cardinality as the original set with uniformly distributed random numbers. This new set, along with the observation that the maximum number of leading zeros in the binary representation of the elements can be used to estimate the cardinality of the set, are used to produce an estimate of the number of distinct elements in the original set.

Minhash [245] is used to estimate the similarity of two sets A and B using the concept of Jaccard Similarity [246]. The algorithm applies K hash functions to each set. Considering one hash function at a time, the algorithm determines the elements from both sets that resulted in the minimum value of the hash functions (*i.e.*, $\{x|x \in A \ \& \ x = argmin(h(A))\}, \{y|y \in B \ \& \ y = argmin(h(B))\}$). The probability that these two elements are equal (*i.e.*, $Pr[x = y]$) is the Jaccard similarity index [247]. Each hash function will produce a result that is either 0 or 1. Averaging over the K hash functions produces an estimate of the similarity of the two sets.

b) Real-Time Analytics Platforms

Due to the timeliness constraint imposed on data for real-time analytics, the data cannot be processed using traditional centralized solutions. To overcome this problem, Distributed Stream Processing Frameworks (DSPF) have emerged to promote such large-scale data analytics in real-time. Examples of such frameworks are Apache Storm [248] and Apache Spark [249].

Streaming applications are connected to heterogeneous stream sources, where the sources feed their streaming data to the applications for real-time analytics. Since an individual source can be active or inactive at any point in time and can use multiple communication protocols, a middleware that understands these protocols is required to act as a gateway between the source and the streaming applications. The gateway usually has low complexity since it does not involve any complicated processing or buffering. The streaming data is then buffered in message queues and routed to the proper destinations for analysis. The queues acts as data source to the streaming applications, while matching the streaming data sources and the applications. The architecture of stream analysis is shown in Figure 13.

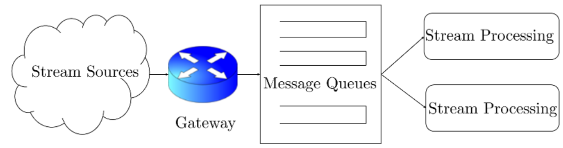


Fig. 13: Streaming analysis architecture.

Message brokers are used to manage the message queues in streaming applications. The brokers' purpose is to match the message generation and consumption rates and alleviate temporal differences issues. Moreover, the brokers act as a filter for routing messages to the appropriate streaming applications. Table IX summarizes the differences between three of the widely used message brokers: Kafka [250], RabbitMQ [251] and Mosquitto [252].

In stream processing, a graph is created consisting of processing nodes connected by streams of events acting as edges. The goal of DSPFs is the creation of these graphs by providing the required infrastructure and APIs and the execution of these graphs with continuous message streaming. Depending on the DSPF used, the graphs and their components are handled differently. For example, Apache Storm allows the users to create their own processing graph and submit to the processing application, while Apache Spark does not provide such provision. Table X provides a comparison between different DSPFs.

c) Real-Time Analytics and Smart Cities

Integration of real-time analytics in smart cities has only been viewed as a building block of a system architecture in the recent literature [254]–[256]. However, the literature does not delve into the challenges faced by real-time analytics for smart cities. These challenges include the heterogeneous nature of stream sources, the different protocols used for communication and data interpretation and the large amount of data produced in a smart city environment.

Different smart cities have been applying real-time analytics in their projects. For example, Swisscom, a telecommunication company in Switzerland, created a data analytics platform capable of delivering detailed analysis at a nationwide scale, which could be sold to urban planners for key use cases. The volume of data, the requirement for real-time computation and the associated performance requirements led the company to Apache Spark at the big data processing layer [257]. The platform also needed to match the stringent quality of service expectations, such as high availability, reliability and resilience under peak usage. This platform is used

TABLE IX: COMPARISON OF KAFKA, RABBITMQ AND MOSQUITTO FOR STREAM ANALYTICS

	Kafka [250]	RabbitMQ [251]	Mosquitto [252]
Underlying Message Protocol	Binary	AMQP	MQTT
Throughput (events per second)	100k+	20k+	60k+
Scalability	✓	✓	
Fault Tolerant	✓	✓	
Rich Routing Capabilities		✓	

TABLE X: COMPARISON OF DIFFERENT DSPFS

	Apache Storm [248]	Apache Spark [249]	Neptune [253]
Message Abstraction	Tuple	Resilient Distributed Dataset (RDD)	Stream Packet
Primary Implementation Language	Java	Java/Scala	Java
Graph Creation by User	✓		✓
Data Serialization	Kryo	RDD	Java Objects
Task Scheduler	Nimbus	Mesos, Yarn	Granules
Flow Control		✓	✓
Fault Recovery	✓	✓	
Message Processing Guarantees	At least once	Exactly once	Not available

to analyze mobile users' data to enrich urban planning across the country, which could support a wide range of use cases where comprehensive and real-time data on urban population unlocks huge opportunities, including accurate population density mapping.

B. Data Presentation

Data presentation is closely associated with the end users of a smart city. It is a way to represent the data and services for end users in a friendly and easy manner [258]–[260]. Data presentation allows the interaction between the users and the data by simplifying how users view the data. This is done by connecting the data generated in real life to data storage and management systems in cyber world and converting the data residing in storage systems into living entities. Current work on data presentation is mainly focused on Geographic Information Systems (GIS) visualization. For example, translating New York City taxi trip data into urban visualization [261] and supporting traffic incident analysis [262].

Similar to other technologies, the main challenge faced by data presentation is that the data generated by smart city applications are voluminous. Therefore, the innovation and development of new techniques, frameworks and user-friendly representations are key to addressing the needs of smart cities and incorporating data presentation into smart city applications.

Following the evolution of data in information systems is one of the strong aspects of data presentation. This leads to a better management of the urban data in smart cities. To this end, the smart city architectures proposed by [254], [263] are based on data presentation core functionalities. Mei et al. [264] propose a surveillance video data structuring method with data visualization techniques. Data presentation technology has shown its technical advantage in many fields of data management. Reconstructing data organization using data presentation techniques and realizing smartness from the structure of data will be important trends of the futuristic data-centric smart city.

C. Insights and Research Challenges

After discussing the different data processing technologies and identifying the limitations faced by each technology, we turn our attention to the collective challenges faced by the different data processing technologies that smart cities need to address.

1) Processing Heterogeneous Data

The main challenge smart cities face in processing the collected data stems from the vast volume of available data and its heterogeneous nature. Thus, it is critical for the different data processing platforms to be able to process different data semantics and to scale well in the face of the increasing amount of data. These challenges become more pronounced when the data need to be processed in real-time.

For example, when there is a public event in the city, such as a sport's event or a musical concert, smart traffic management may have to process large volumes of data from different sources with different semantics. Data is collected from sensors deployed on the streets reporting traffic flows, from people using social networks or crowdsourcing applications (*i.e.,* Waze) to express their road experience and from 5G technologies that track the mobile phones' locations. The ability to process such heterogeneous data will help the smart traffic management system to provide a better road experience for the users.

2) Moving Toward Semi-Supervised Learning

As for machine learning and deep learning techniques, the dependence on the availability of labeled data for supervised learning is a major challenge. Real-life data are mostly unlabeled and it is costly to label such large volume of data. Moreover, it is necessary to identify the proper performance metric and the proper training data set for unsupervised learning, as selecting an unrepresentative training data set will lead to performance degradation. Therefore, there is a need to move toward "semi-supervised" learning, which strikes a balance between supervised and unsupervised learning and can benefit from both labeled and unlabeled data.

For example, in the public event scenario mentioned above (*i.e.,* a sport's event or a musical concert), data collected from the different sources (*i.e.,* sensors, social networks, 5G) contain both labeled and unlabeled data. The smart traffic management system in charge of regulating the traffic within the city can benefit from semi-supervised learning techniques to process the data and discover hidden patterns. In this scenario, the traffic management system should select a learning technique and a processing platform that are scalable and able to process the large volumes of generated data.

3) Spatial and Temporal Dependencies

Another challenge for processing data for smart city applications is that the data processing platforms need to be aware of the dependencies of some data on the time and location these data were collected, as ignoring such dependencies might lead to catastrophic decisions especially in safety-critical situations and disasters.

For example, in smart emergency systems, the dependence of data on time and location is critical. The data processing platforms need to identify new data from old ones in order for the law enforcement agencies to be updated with the latest information. Moreover, the platforms need to be aware of the locations at which the data were collected and identify which data is more relevant to accurately report the location of the incident under investigation. When the processing platforms are able to identify such dependencies, the law enforcement agencies can quickly respond to safety-critical situations.

4) Deployment of an Information Management System

Ensuring data quality and the interpretation of meaningful results are challenges faced by any data processing platform. However, these challenges become more pronounced when big data is considered. To ensure the data quality, the processing platform needs to check that the data is "good" before processing it. This means that an information management system should be deployed to address this issue. Although data acquisition technologies need to ensure data quality as well, they are able to do so to some extent due to the limited processing capabilities. Therefore, data quality should be ensured at all levels of data management in smart cities as shown in our holistic view in Figure 2.

As for interpreting meaningful results, data presentation techniques should present large volumes of results such that the decision-making agencies can interpret the results in the best way possible. This can be realized by grouping "similar" results under some form of hierarchy for effective data presentation. For example, in smart city planning applications, results interpreted in meaningless ways can affect the decisions made by the city authorities and result in dissatisfaction among the citizens.

VI. Data Dissemination

The last step in the journey of the data through a smart city application is to disseminate the data to the interested end users. Facilitating data dissemination between different parties is key to smart city realization [265]. Due to the existence of different kinds of end users (*e.g.*, citizens, companies, government agencies, etc.) requiring different levels of quality of service, the need arises for a smart city to deploy different protocols for data dissemination. In this section, we survey the recent literature and discuss the different data dissemination techniques and the challenges they face in the context of smart city applications.

A. Data Dissemination Methods

Data can be disseminated to end users using one of the following methods:

- Direct Access: In this method, the data resides in a database that can either be accessed openly or by authenticated users. Users interested in a piece of data issue requests indicating their interest and receive a response containing the data. Challenges faced by this method are mainly the same challenges faced by databases, ranging from validating authenticated users, to performing fast queries on the voluminous data of smart cities, to ensuring the correctness of the results, to security concerns especially for open access databases. Smart city applications that require the data to be stored in a database, such as smart health (where patient records are stored in a database) and city planning (where records of the city's infrastructure are stored in a database) can take full advantage of this method.

- Push method: Where a piece of data is pushed to the end users without being requested by the users. This method is usually suitable for conveying notifications regarding future events (*e.g.*, electricity outage, road closures, etc.), or delivering critical messages in case of emergencies. The most important challenge faced by this method is the timely delivery of data, especially in case of emergencies.
- Publish/Subscribe services: This is a messaging system where data senders (publishers) publish their data without knowing the exact identity of the receivers (subscribers) and subscribers receive data based on their expressed interest. To implement this service, a middleware called a message broker is required, such as Kafka, RabbitMQ, or Mosquitto. Which message broker to use depends on the smart city application under consideration, as shown in Table IX. The main challenge of using publish/subscribe services is to ensure the stability of the message queues and the delivery of messages in the face of the large amount of data in smart cities.
- Opportunistic Routing: Due to the highly dynamic topology and the wireless nodes being oblivious to their surroundings, the sender and the receiver may not be aware of each other. Opportunistic routing aims at delivering data in such topologies, where the routing decisions are made dynamically after the data is received by intermediate nodes. Although this may cause message flooding, it can be solved through the use of acknowledgement packets as suggested in [266].

B. Data Dissemination in Smart City Applications

To this date, there are limited efforts that address data dissemination in the context of smart cities. Although there are few works that have considered this aspect, most of the literature targets the data acquisition and processing in smart cities as discussed in Sections IV and V.

To summarize the current literature, Palma and Vegni [267] evaluate the use of a broadcasting system for VANETs, where the topology is changing dynamically according to traffic patterns. Bonola et al. [268] provide experimental evaluation on using taxis as relaying nodes for collecting and disseminating data from/to different devices in the city of Rome. Le et al. [269] propose a routing algorithm to disseminate data in topologies consisting of heterogeneous nodes. Reina et al. [270] propose a multi-objective optimization for data dissemination in Delay Tolerant Networks (DTN). Gorrieri [271] proposes multihop routing in support of IoT applications. Wu et al. [272] present a framework for Urban Sensing applications using UAVs to collect, process and disseminate the data. Morelli et al. [273] propose a mathematical model to predict recurring patterns in mobile movements to facilitate opportunistic routing to disseminate data for smart city applications. All of these works use opportunistic routing for data dissemination.

The works in [274]–[276] propose architectures of middlewares in which the data dissemination is based on a Publish/Subscribe service using Kafka, OpenSplice and Google Pub/Sub platform, respectively. De Alvarenga et al. [277] propose an architecture based on a push server model for data dissemination in smart cities. TRIMARC, a traffic response and accident management deployed in Louisville, USA [278] pushes road closure schedules using APIs to different departments. Rusu and Vert [279] propose a notification system called City Alerts, where data is stored in a database that is accessible through a web interface.

Taking a different approach to data dissemination, Lauriault's goal in [280] is to help make a decision about the data that should be disseminated through a decision making tree. Tian et al. [281] present a Traffic Adaptive data Dissemination (TrAD) protocol for VANETs. The performance of two data dissemination protocols for VANETs, DV-CAST and Edge Aware Epidemic Protocol (EAEP), are evaluated by Islam and Palit [282]. Olaru et al. [283] identifies three categories, under which requirements needed by any data dissemination infrastructure falls; context-awareness and integration, scale and dependability, and users' privacy. Bessis and Dobre [284] provide a taxonomy and analysis of data dissemination techniques in the context of IoT. Lupi et al. [285] evaluate a broadcast protocol for data dissemination in VANETs. A survey for data dissemination in VANETs is presented by Chen et al. [286]. Hahner et al. [287] proposes a protocol for data dissemination in MANETs. A policy for regulating data dissemination is in effect in the city of Dubai [288].

Table XI summarizes the challenges faced by these data dissemination techniques.

C. Insights and Research Challenges

In this section, we discuss the challenges faced by the data dissemination technologies when used collectively by smart cities. We also draw some insights toward realizing smart cities.

1) Scalability

As with data acquisition and data processing, the challenges faced by data dissemination technologies stem from the large volume of data to be delivered to different smart city applications and users that require different semantics and data representation. Therefore, data dissemination technologies must be able to scale well and be able to deliver data with different semantics.

TABLE XI: DATA DISSEMINATION CHALLENGES IN SMART CITIES

Technology	Advantages	Limitations and Challenges	References
Direct Access	• Data Consistency • Reduced Data Redundancy • Enhanced Data Security	• Scalability	[279]
Push Notifications	• Real-Time Communication • Wide Reach to End Users • User Retention	• Platform Dependency • Scalability • Routing Issues	[277], [278]
Pub/Sub	• Loose Coupling between Publishers and Subscribers • Enhanced Response Time	• Inflexibility of the Data Structure. • Scalability for Large Number of Users.	[274]–[276]
Opportunistic Routing	• Infrastructure-less • Increased Reliability • Increased Transmission Range	• Potential Lack of End-to-End Path • High Delay • Message Loss • Next Hop Decision	[267]–[273]

For example, continuing with the scenarios mentioned in Section V-C (*i.e.,* a sport's event or a musical concert), reporting information back to the citizens should be in different semantics (*i.e.,* information reported through social networks have different semantics than those reported through crowdsourcing or 5G). Moreover, the traffic management system needs to deliver data to a large group of people. Therefore, the technologies used to disseminate the data need to scale well.

2) Distributed Data Access

For technologies that require direct access to a database, challenges such as users' authentication, performing fast queries and security threats become more pronounced. City management systems should provide a distributed way to handle the massive amount of accesses and to quickly respond to requested queries. For example, in smart healthcare, accessing health records of patients must be authenticated. Only the patient's doctors and nurses should be able to access these records. Moreover, since there are large number of records, the doctors or the nursing staff should be able to quickly access the desired records and fast queries should be performed.

3) Federations of Message Brokers

For Publish/Subscribe services, there is a need to design management algorithms for clusters and federations of message brokers in order for these brokers to operate at city-scale. Without such algorithms, individual brokers are unable to handle the massive load that can be generated at the city-scale.

For example, smart city parking applications that can benefit from Publish/Subscribe services may need to report the location of empty spaces to drivers who are interested in such applications. These applications need to choose Publish/Subscribe services that are able to disseminate the location of empty parking spaces to large number of drivers (especially in crowded areas and rush hours).

4) Citizens Dynamism

Since the citizens in the city are highly dynamic by changing locations quickly, technologies such as opportunistic routing should focus on addressing the issues of energy efficiency and intermittent connections. These issues become more explicit in the context of smart cities and the new technologies should be able to quickly decide how to disseminate the data in light of low power consumption. For example, Road Side Units (RSU) use opportunistic routing to communicate with the vehicles on the road. These units should be designed with energy efficiency in mind, as well as allowing data storage until a connection with a vehicle or another RSU can be established.

VII. Data Security and Privacy

Smart cities are born from convergence of its citizens, infrastructure and ICT in order to improve resource management, as defined in Section I. This convergence offers many benefits, but it also poses many security and privacy challenges if not implemented adequately. Although security threats and challenges are an inherent part of any ICT system [289]–[292], its impact level amplifies many folds in case of smart cities where symbiosis of physical infrastructure and ICT becomes a reality. A hacked email account might cause problems to a single individual, but if a Smart Grid (SG) is hacked, it can paralyze a city or even an entire state [293]. One manifestation of such a threat was Stuxnet worm [294]. The worm is believed to have been designed to target the Iranian nuclear program, infecting industrial Supervisory Control and Data Acquisition (SCADA) system. Based on the reports, before its discovery by the Iranians, the

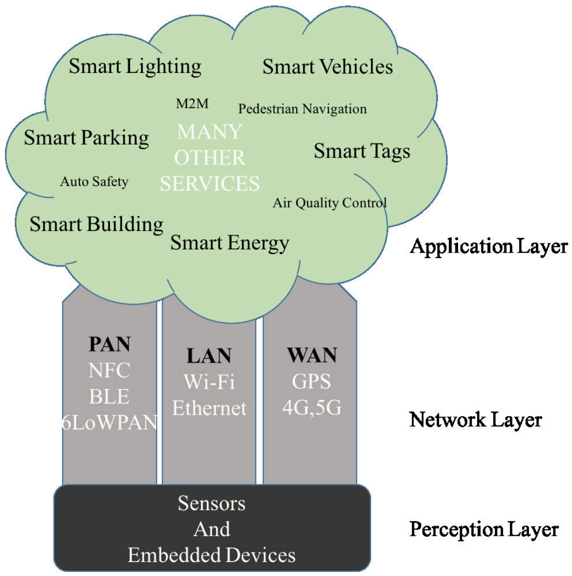


Fig. 14: Smart city and IoT.

worm had rendered more than 30% of the centrifuges at the Natanz Uranium enrichment facility useless.

Analyzing security and privacy challenges in smart cities are difficult due to complexity of systems and involvement of numerous partakers. Technological, socio-economical and governmental factors all affect security and privacy [12]. In this study, the focus is solely on technological challenges of possible future. Even-though the focus is only on technological challenges, not all technological challenges will be covered due to the diversity and big number of technologies that can be used in smart cities. Therefore, we mainly focus on challenges and issues that are unique to smart cities; such as Smart Mobility (SM), Smart Grids and to some extent IoT.

In the following, we discuss unique security and privacy challenges in smart cities and some of its components and possible solutions. Furthermore, we outline the future trends in security and privacy of smart cities.

A. Challenges and Threats

Smart cities usher in a new era of Internet and communication, and with it, comes a new set of cyber security threats. In smart cities, billions of devices will be gathering, storing and processing data ubiquitously using hardware embedded in the environment. The heterogeneity of technologies in smart cities makes security and privacy a multi-dimensional problem, for which traditional solutions might not work.

There are several aspects of the smart city ecosystem that makes it vulnerable to security and privacy threats which are uncommon in traditional cyber-networks. One such vulnerable aspect is its heterogeneous nature. Attacks on smart cities might emerge from the integration of different technologies that are prone to incompatibility issues and in some instances are not built with security in mind.

Another vulnerable aspect is the physically distributed nature of smart city networks, which might incorporate huge numbers of small devices and sensors, introduces new security and privacy threats. Physically distributed networks make it hard to provide physical security and increases attack surface. Likewise, usage of cheap, proprietary devices and sensors heralds new security and privacy threats. For instance, burglars can use camera footage, motion sensor data, microphones embedded within smart TVs, log of lights and thermostat to figure out when a house is not occupied [295]. Such security and privacy threats are further escalated by usage of small and cheap IoT devices that may not have the capabilities to support cryptographic solutions necessary to countermeasure common security and privacy threats. In the following, we review security and privacy threats and challenges of three essential smart city components.

1) Smart Grids (SG)

Electric grids have evolved a great deal since conception of the first grid by Thomas Edison in Lower Manhattan. Nevertheless, despite all developments the classical grid has remained a one-way flow grid that has several short comings [296]–[298] and is not suitable for today's society. Furthermore, classical grids suffer from over generation due to their inability to match the generation to the demand. Considering that it is hard for distributors to precisely predict peak demand, they have to over generate energy in order to sustain demands during peak hours, which results in environment pollution and contributes to global warming where fossil fuels are used. Likewise, classical grids do not have the capability to help inform consumers about their energy usage, which could help consumers plan usage accordingly, thus improving efficiency. In pursuance of overcoming aforementioned shortcomings, a framework for next generation of electric power systems, called SGs, was proposed in [299]. SGs create two-way communication infrastructure that supports new applications, such as Advanced Metering Infrastructure, Demand Response, Distribution Grid Management, and wide area situation awareness [300]. Although SGs allow us to use the grid much more efficiently, the added two-way communication systems would be more susceptible to cyber attacks.

In addition to common security and privacy challenges, which are listed in Table XII, SGs also introduce unique security and privacy challenges that needs to be addressed. One such challenge stems from the use of legacy devices and protocols in SGs. For instance, SCADA protocols that are extensively used in Industrial Control Systems (ICS), which SGs are part of, were designed over twenty years ago for isolated environments and for good performance but with no security in mind [301]. Integration of such legacy systems into smart cities pose huge security challenges. Authors of [302] asserts to have found more than $60,000$ vulnerable SCADA systems on the Internet. Likewise, distributed nature of SGs introduces new security and privacy challenges. SGs are distributed across several hundred square kilometers with several substations that each can act as entry to point to the network. Physical security for such a distributed systems is very challenging [303]. Additionally, some of the legacy devices used in power grids does not support cryptographic solutions and are virtually impossible to patch or update [304] which introduces a new set of challenges to security and privacy in SGs.

There are several different solutions proposed in literature to the aforementioned challenges. Passive and active intrusion detection systems have been proposed [302], [304]–[306]. Intrusion detection systems although efficient in classic computer networks, still have limitations in ICS that needs to be addressed [304]. The authors of [307] proposes using a *Shadow Security Unit* that is capable of transparently intercepting communication channels and process I/O lines to monitor system security. Such a solutions is cheap and non-intrusive. Fingerprinting devices in order to monitor ICS security have been proposed by [303]. Fingerprinting is suitable for SGs since the networks are distributed and maintaining physical security is very difficult [303].

2) Smart Mobility

SM is the application of ICT solutions to resolve the mobility issues (*e.g.*, pollution, accidents, traffic congestion) that the citizens face. These issues have both social (*e.g.*, each year more than 1.2 million lives are lost due to road accidents world wide [308]) and economical (*e.g.*, road congestion in the U.S. costs $37.5 billion each year [309]) consequences.

Despite all the advantages, SM and ITS are not without challenges. The consequences of security flaws in SM systems can be life threatening. For example, imagine a malicious party that makes a fast moving vehicle on the highway to brake hard in order to avoid collision with an imaginary vehicle in front of it; this can be life threatening if there are other vehicles behind the targeted vehicle. In its National ITS Architecture (NITSA) [310], the Department of Transporation specified 22 subsystems for ITS and SM that cover all communication aspects of V2V and V2I systems and their security objective and requirements.

To realize the SM, it is necessary to integrate a wide range of systems and technologies [311], [312] together. Securing such a heterogeneous system is an arduous task. To better identify potential security threats and evaluate security performance of a system, security objectives and requirements of the system need to be identified. In ITS, exchanged data should not be subjected to intentional or unintentional modifications. Otherwise, it will be possible for malicious users to take advantage of the system (*e.g.*, *sybil attack*) [313] resulting in serious consequences (*e.g.*, falsifying certificates makes the identification of malicious vehicles difficult in case of disputes). Denial of Service (DoS) and DDoS attacks are the most serious threats against the availability of services. ITS users rely on services provided by the system, and the absence of such services can have dire consequences (*e.g.*, flooding or jamming attacks, preventing or delaying receipt of Basic Safety Messages (BSM) by vehicles on a highway, can prove to be fatal).

Attacks on integrity of ITS system include data tampering attacks (*e.g.*, man-in-the-middle attacks or replay attacks), unauthorized use/access attacks (*e.g.*, masquerading), and broadcast tampering attacks [312], [314], [315]. ITS service availability is important because users rely on offered services to make decisions (*e.g.*, pedestrians being alerted of approaching vehicle). Preventing or delaying the dissemination of messages by a malicious attacker can lead to fatal consequences. Attacks on availability need not be complex; simple attacks such as jamming [316] can prevent or delay the delivery of messages in wireless networks that ITS relies on. Attacks on availability include jamming, flooding, DoS, DDoS and Sybil attacks [312], [314], [315], [317], [318].

Although some of the applications in ITS do not require confidentiality (*e.g.*, BSM in VANETs [319]), it is of utmost importance for other applications (*e.g.*, Electronic Toll Collection). Attacks on confidentiality can range from simple wiretapping and eavesdropping to brute force and man-in-the-middle attacks.

Countermeasures to security threats in ITS are as wide ranged as the attacks themselves. Each of the security threats have to be dealt in its own right. While some of the attacks can be prevented (*e.g.*, using certified and disposable certificates to prevent cryptographic replication attacks [312]), others can only be mitigated using different techniques (*e.g.*, jamming attack mitigation [320]). Table XII contains a list of security threats and their most common countermeasures

3) Smart Homes

Smart Homes is another component of smart cities that will pose huge security and privacy threats. Home appliances are becoming smarter each day and soon citizens would be able to control all aspects of their homes both locally and remotely via smart home systems. Google Home and Amazon Echo are two of the latest gadgets that allows its owners to control some part of their homes. Smart TVs equipped with microphone and cameras, security cameras with motion sensors, smart thermostats, smart lights (*e.g.,* Philips Hue Lights), smart fridges, smart door locks, smart utility meters and smart shutters are already present in many homes. Although such systems are valuable and can help us better manage our homes, their security and privacy aspects are not well studied. Additionally, many of such devices are being produced by manufacturers with no security and privacy in mind. Authors of [321] have studied Samsung owned *SmartThings* programming framework and Samsung's *SmartApps* market and claim that 55% of the smart applications in the store are over-privileged. These applications can access functionalities that they have no use and thus can be easily exploited by malicious entities.

Based on documents published by *WikiLeaks*, Central Intelligence Agency (CIA) already has the capability and tools to hack any smart appliance currently present in our homes [322]. Such report was no surprise given CIA's resources, but these attacks are not all that difficult given how un-secure the devices are as demonstrated by [321]; who were able to change door lock codes and induce fake alarms among other activities. Such reports are alarming and dangerous as society is moving towards smart homes at a very fast pace.

Likewise, malicious users can benefit greatly from gathering data from personal devices in used in homes. For instance, data gathered can be used for user profiling and tracking or for launching other types of attacks [323]. The most striking difference between traditional computer security and privacy attacks and smart home attacks are the number of different ways malicious users can gain access. Burglars can determine where and when to rob based on security camera feeds, motion sensors, energy usage patterns and can gain access to target homes by exploiting smart lock weaknesses [295]. Such attacks can not only cause financial harms but are also serious threats to privacy.

To counter smart home attacks better hardware standard needs to be introduced so that sensors and devices are not vulnerable to common security and privacy attacks. Furthermore, home appliance manufactures have to improve security of their softwares. Devices should be able to be remotely and easily updated and new software patches installed.

B. Insights and Research Challenges

We discussed common security and privacy threats in smart cities and their countermeasures. In this part we highlight security and privacy research challenges that can affect the realization of smart cities. Furthermore, we highlight critical insights into novel solutions that have the potential to solve security and privacy issues of smart cities.

1) IoT Security and Privacy

One of the first challenges that smart cities face is providing security and privacy using IoT systems. IoT is an essential part of a smart city infrastructure and applications. IoT systems rely on low-power devices with limited computational power embedded in environments that communicate via different wireless technologies. This paradigm poses numerous security and privacy challenges that need to be addressed. Use of sensors and devices with limited computational power, which rely on weak cryptography algorithms, pose serious threats to data security and integrity. In addition, existence of sensors with or without limited computing power to perform basic cryptographic operations limit the length of cryptographic keys; which in turn can jeopardize both confidentiality and integrity of data [346]. Moreover, dense deployment of IoT devices and sensors carry the risk of physical security breaches. Adversaries might be able to install malware on devices and compromise data integrity.

One powerful tool to counter the aforementioned security and privacy challenges is Trusted Platform Module (TPM) standard [347]. The TPM, as specified by the Trusted Computing Group, is a dedicated hardware module for cryptographic processing operations. It is usually deployed as a co-processor and is used for cryptographic random number generation, secure boot, attestation and data sealing. TPM saves a hash of desired state of platform in a secure area, and each time the system boots, it checks the current state of the system against the desired state hash. If any changes were detected, it prevents the system from booting. TPM along with the BIOS system create a *root-of-trust*. Using TPM can greatly increase the systems' integrity and confidentiality. TPM is a viable solution for devices with hardware that can support such operations. Network overlays is a viable solution to protect security and privacy in networks with sensors and devices that have limited or no cryptographic capabilities. The overlay network provides security and privacy by isolating the network in question from attackers.

Likewise, maintaining user privacy in IoT and smart cities is a much harder challenge than traditional systems due to the ubiquitous data gathering sensors embedded in the environment. Personal data gathered by sensors can be indefinitely retained by servers, which can threaten users' privacy. Moreover, since all activities in smart cities are performed using ICT, it becomes difficult for users to hide their presence and activities. For example, automatic toll collection will be offered in smart cities under smart mobility services. But they will require users to pay toll fees via authenticated means. In such

TABLE XII: SECURITY THREATS AND COUNTERMEASURES [312], [314], [315], [320], [324]–[327], [327]–[343]

Attack	Description and Countermeasure(s)
Data alteration and modification	Malicious users can break integrity of exchanged data by altering, deleting or fabricating its content. Public Key Infrastructure (PKI) can be used to counter such attacks.
Masquerade attack	In masquerading attacks, malicious entities duplicate valid identities to achieve their goals. Identity certificates issued by trusted authorities (PKI) are used to identify entities. To ensure that compromised certificates are not used, certificate revocation lists mechanism can be utilized to prevent such attacks.
Replay attack	In replay attacks, malicious entities repeatedly send valid data gathered maliciously to gain access to the system. To counter replay attacks, a system can keep a cache of exchanged messages and compare new message with previously received messages.
Man-in-the-middle attack	In this type of attack, the attacker intercepts the communication between two entities, while the entities think they have direct communication. Preventing such attacks is possible via cryptographic solutions.
Sybil attack	Sybil attacks are impersonation attacks. They can be simply prevented by explicitly binding an identity to participating entities in a system. PKI-based identities (signatures) can be used for assigning identities. It is also possible to detect such attacks via cryptographic solutions.
GPS spoofing	Attackers can make ITS entities that use GPS for positioning (*i.e.*, vehicles) believe that they are in a different position than they originally are [344]. Such actions can lead to accidents. Furthermore, GPS is also used to synchronize system time, and if GPS is spoofed, then the system will also become susceptible to replay attacks. To counter GPS Spoofing, implementing plausibility rules, such as using location and signal strength of satellite to detect any malicious and abrupt changes can be used. Technical countermeasures include using military Precise Positioning System (PPS) signals instead of civic Standard Positioning System (SPS) signals.
Broadcast and Transaction Tampering	Broadcast tampering is the injection of false data into the system by malicious users using broadcast messages. In transaction tampering, the malicious user could tamper transmitted data or create an alternate reply to unsuspecting users. Using authentication and digital certificates can prevent both of these attacks. Even if malicious users gain access via valid certificate, the problem can be solved by using CRL.
Eavesdropping and Traffic Analysis	Both of these attacks target users' privacy. Encryption and cryptographic solutions are strong enough and can counter these attacks.
DoS	Jamming is a physical layer attack, usually conducted by transmitting noise signals to prevent the transfer of legitimate traffic. Different techniques exist to mitigate jamming attacks. Spamming is difficult to stop due to its infrastructure-less nature. Flooding attacks try to make the system unavailable by generating more data than the system can handle.
Malware	It can be any attack that involves malicious software, such as Trojan horses, viruses and worms. The software can infect the infrastructure or any other part of ITS. Malware attacks can be prevented by signing the software, using anti-virus software and keeping software up-to-date.
Brute Force	In brute force attacks, attacker uses all possible combinations of keys to gain unauthorized access to the system or the data. National Institute of Standard and Technology, in its guidelines for computer security, recommends using strong cryptography algorithms to deter and prevent brute force attacks. Authors of [345] provide a comprehensive analysis of current cryptography algorithms and their susceptibility to brute-force attacks.
Timing attack	Timing attacks are a significant challenge in networks where time-critical applications exist. Safety applications, such as forward collision warning applications, are delay-sensitive and susceptible to such attacks. Timing attacks can be prevented by using time-stamps and signing the packets with an algorithm, such as Elliptic Curve Digital Signature Algorithm (EDCA).
Conflict Collision	Conflict collision occurs at the perception layer of IoT when multiple Radio Frequency Identification (RFID) tags try to transmit data simultaneously, and RFID reader might not be able to read data properly. To resolve this issue, RFID anti-collision techniques can be used.
Node Security	To ensure security and privacy in IoT sensors, nodes have to not only trust each other but also trust the base stations and the core-network. Trust management techniques can be used to ensure trustworthiness of nodes and communication.
Security Attacks on devices with limited computational and storage resources	WSN is an integral part of IoT network, which is an essential part of smart cities. There are many different attacks that target these devices. The key to countering such attacks are lightweight cryptographic solutions, such as TinySA.
Routing attacks	WSN is susceptible to routing attacks, such as sinkhole attacks and selective forwarding. These attacks can be mitigated using secure routing protocols.

a scenario, users' data saved in the system can later be accessed and/or compromised by an attacker.

Blockchain [348] can be used to solve privacy issues in the mentioned scenarios and has the potential to address all the privacy concerns in smart cities. This is a peer-to-peer distributed open database that first became famous as the ledger technology used to keep track of exchanged cryptocurrency, *Bitcoins* [349]. Blockchain's distributed database can be used to record any type of transaction securely and anonymously. The major benefit of Blockchain is its un-hackable nature. In order to compromise the system, attackers have to hack 51% of the nodes in the network, which is essentially impractical. In the mentioned toll collection scenario mentioned above, Blockchains can be used so the user can pay the toll collection system using some form of digital currency securely while maintaining his/her privacy. This need not be the only usecase. Blockchain can be used in smart cities to establish relations between service providers and users using smart contracts without involvement of third-parties and re-negotiations. For instance, a service provider could lend goods to users and keep track of the goods via Blockchain. Users could automatically pay lenders via Blockchain connected to their bank accounts. Such a smart contract would allow fast transactions while maintaining privacy.

2) Machine Learning Security

Another future research challenge in smart cities is securing machine learning vulnerabilities in adversarial environments, which is referred to as *Adversarial Machine Learning* field. Intrusion Detection Systems (IDSs) are one of the technologies that rely extensively on machine learning systems to keep networks safe from complex attacks (*e.g.,* man-in-the-middle attacks, wiretapping attacks, malware and viruses). For IDSs to perform efficiently, their machine learning algorithms are trained on datasets that are called adversarial samples. They are past known patterns and behaviors of attackers. For instance, in order to mark emails correctly as spam, the spam detection software relies on a set of keywords in past spam emails. As machine learning algorithms mature, adversarial attacks also get sophisticated in order to evade detection. Adversaries know that machine learning algorithms require training, so they often devise targeted attacks that aim to poison the training data that can render the algorithm useless. In addition, some adversaries focus on crafting input data that resembles normal input in order to escape detection. Although solutions to some of the security vulnerabilities in adversarial machine learning have been devised [350], [351], current solutions do not completely eliminate all vulnerabilities and more research is required to find viable solutions.

In this section, we reviewed security and privacy objectives, requirements and threats in smart cities and some countermeasures. Furthermore, we highlighted solutions that can be leveraged to solve security and privacy issues in smart cities.

VIII. Networking and Computing Technologies

The data lifecycle needs to be supported by different networking and computing technologies. As the ubiquitous devices and systems generate abundant data that is often underutilized. The data they generate should be reused and distributed across different application domains, devices and systems. For instance, municipality, private and public organizations can utilize various embedded systems and infrastructure, such as traffic monitoring cameras, smart buildings, smart power grids and government clouds [352] to monitor, process, coordinate and control various activities.

These activities and tasks can be broadly classified into safety, efficiency and infotainment services and applications. Safety services and applications can range from pedestrian and passenger safety in the ITS, to disease prevention and control of outbreak of epidemics through smart healthcare systems employed in the smart city. Efficiency services and applications include the ever famous on-the-go connectivity, smart parking assistance and traffic monitoring of the smart city to improve productivity of the workforce and residents. The infotainment services and applications that will benefit significantly from a smart city will include personalized and context aware advertisements about items on sale, TV shows to watch, trending tweets, and breaking news highlights.

At one end of the smart city spectrum, we have a wide range of smart devices and systems that are already embedded in the ambient environment. The smart devices can vary tremendously in their purpose. They can be sensors embedded in wearable devices, such as clothes, watches and glasses. Alternatively, the sensors could be embedded in the environment for actuation and automation, and in control systems in homes and offices, such as occupancy based lighting control, programmable temperature controlling systems and water consumption control in bathrooms. There are also ambient sensors embedded in the on-board units in vehicles for collision avoidance and vehicle maintenance. These embedded smart devices and actuation, automation and control systems in the environment and the latent network elements, such as, routers and switches, are all integrated into the IoT that enables smart cities [353].

On the opposite end of the spectrum, we have the high performance, scalable and reliable datacenters of the cloud. It is envisaged that many of the smart city applications and services will be hosted in the Cloud. Therefore, smart city residents and service providers can rely on cloud services to host, build and/or deploy their smart city services and applications.

However, the disparity in communication protocols, proprietary vendor-specific software and intrinsic hardware differences inhibit the realization of smart cities. Recent advances in virtualization and softwarization of various transportation and network layer functionalities can overcome some of these challenges. Key enabling technologies for softwarization include Network Functions Virtualization (NFV), Software-Defined Networking (SDN) and Cloud computing [354]. They enable integration of smart devices and systems and facilitate data management in smart cities. The softwarization of network functions and communication, using NFV and SDN, respectively, can offer all the L2-L7 applications and services for data management and exchange in an IoT for smart cities [355]. In the following subsections, we will briefly discuss the enabling technologies, evaluate them against well motivated IoT requirements for the smart city and discuss future insights and open research challenges.

A. Cloud computing

Traditionally, service providers predict demand for their applications and services and allocate the necessary resources accordingly. Though accurate prediction models [356], [357] can estimate the popularity of services, service providers may still not provision resources adequately to cater to sudden and unexpected surges in demand. For example, in a city hosting a spectacular sports event, the audience experience deterioration in performance of wireless devices with unacceptable latency and unavailability of cellular and social media services due to the sheer number of people and their sharing of voluminous, high-resolution content, such as videos.

Similarly, disruption in cellular communication was witnessed in the disaster of 9/11 in New York City. Such variations in demand are unpredictable and directly result in performance degradation and monitory loss for service providers. The elasticity required by service providers to meet the fluctuating end-user demands can be easily achieved by cloud computing. The cloud offers seemingly infinite resources, namely network, compute and storage that are leased by service providers. The elasticity of the cloud enables service providers to dynamically provision resources to meet sudden surges or troughs in demand.

The cloud consists of hardware and software in large-scale datacenters, with hundreds and thousands of machines spread across the globe. Primarily, it offers three services, namely, Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [358]. The services differ in the level of access to the cloud infrastructure. In SaaS, users can access applications running in the cloud via web interfaces, whereas in PaaS the users can implement their own applications using tools (*e.g.*, libraries, programming languages) and services in the cloud. In IaaS, users can provision resources, such as compute and storage, to deploy arbitrary applications, services and software components in the cloud.

The cloud computing paradigm enables cloud infrastructure providers to offer cloud resources as services in a pay-as-you-go cost model with QoS guarantees. QoS with respect to availability and response time is increasingly becoming the de facto clause in Service Layer Agreements (SLAs), which guarantees service uptime and response time for service consumers.

Cloud computing offers smart city service providers with dynamic resource provisioning, primarily through virtualization. The virtual resources can include computation, storage and communication, which can be dynamically allocated and deallocated in datacenters across different geographic regions to meet demands. The datacenters can belong to the same cloud infrastructure provider or they can be across clouds. Currently, cloud computing has matured to the point where it is widely accepted and adopted for its scalability and reliability [359] in hosting services and applications. However, it is important to note that not all applications and services will be hosted or migrated far into the traditional cloud, since various applications and services will be brought closer to the end-user using converged edges [360] in smart cities.

The converged edges will build on cloud computing concepts to offer a dynamic resource pool for hosting cloud like applications and services that have strict latency requirements. Examples include smart city applications and services that are used by first response teams for immediate coordination of safety procedures, applications that require large-scale processing of highly localized data [360], and Peer-to-Peer Video-on-Demand and safety applications for ITS [361], [362]. Smart city services that appear as SaaS include road safety applications for pedestrians and vehicles [363], taxi service applications in mobile clouds [364], and cloud-based Smart City Operating System [365]. Other services include Smart City Platforms [366] and Smart City as a Service (SCaaS) [367] for PaaS and IaaS.

B. Software-Defined Networking

Traditional telecommunication networks consist of tightly coupled data and control planes implemented in hardware and software. SDN enables softwarization of networks by decoupling the control and data planes. The hardware generally includes data forwarding devices, such as routers and switches, while the control plane is implemented in software as a logically centralized controller. The controllers and forwarding hardware in the data plane communicate via non-proprietary and secure communication protocol. OpenFlow [368] has become the de facto standard protocol for communication between the software controllers and the data plane.

OpenFlow conveniently exposes the typical network elements and functions of hardware to the controller for programmability of the data plane [369]. In essence, any hardware device can be updated with a firmware to be OpenFlow compliant [369], which dramatically decreases capital expenditure (CAPEX) and reduces time to deploy a software-defined network for smart cities.

Figure 15 illustrates the high-level SDN concept using SDN controllers and OpenFlow enabled network devices. An OpenFlow enabled network device maintains flow tables that record generic routing information, such as packet identification, source IP address, destination IP address, ingress and egress ports. The OpenFlow controller manages the flow tables that represent the data forwarding rules in the data plane. An OpenFlow controller includes a Network Operating System (NOS) that interacts with the southbound OpenFlow API. There are various OpenFlow controllers, such as NOX/POX [370], Floodlight [371], McNettle [372], and NetCore [373], which allow external applications to create and update high-level network policies that are implemented in the data plane [369].

In this way, SDN offers extreme flexibility and high programmability. The programmability of the data plane by the controller enables cost-effective and dynamic network configuration in support of smart cities. SDN is being proposed to control IoT for smart cities, by extending connectivity to homes using SDN for capacity sharing [374], securing routing in smart cities [353] and mobility management within various clouds [375], [376].

C. Network Functions Virtualization

Traditionally, telecommunication companies deploy specialized network hardware to perform specific network functions (NFs). Network functions provide network level services, such as deep packet inspection (DPI), firewall, and network address translation (NAT). The network traffic passes through multiple network functions in a specific order, known as a Service Function Chain (SFC). For example, an SFC can consist of a firewall, followed by an IDS, and then DPI. Therefore, an SFC requires a fixed sequence of these middleboxes that process different flows. Myriad SFCs exist in a network infrastructure to offer various network layer services. Therefore, SFCs must be orchestrated to optimally and efficiently utilize the network hardware.

There is significant capital and operational expenditure (CAPEX/OPEX) to deploy, maintain and update traditional networks (*i.e.*, their hardware and software), which requires specialized maintenance personnel. These costs rise further, as the requirements for future Internet applications change and grow to meet extremely large network traffic and rich applications requiring intensive processing and communication. NFV cost-effectively decouples network hardware and network functions, as illustrated in Figure 16.

The NFs are software running on virtualized resources on top of Commercial-off-the-Shelf (COTS) hardware. A NFV management and orchestration (MANO) software is used for creating, configuring, managing and monitoring the Virtual Network Functions (VNFs) and the Network Functions Virtualization Infrastructure (NFVI). NFV does not require specialized personnel or proprietary hardware and enables faster maintenance, update and deployment of new and novel network functions. Currently, NFV has been successfully applied to typical network layer functions and is being extended to provide end-to-end services envisioned for smart cities, such as multimedia content delivery by virtualizing application level functions (e.g., video compression, transcoding and mixing) [377].

NFV shows great potential to facilitate faster deployment of IoT for smart cities through IoT-Clouds [378] and SDN-based NFV to develop a PaaS for IoT [379]. OpenNF [380] is a converged control plane for VNFs extending SDN in the network forwarding plane to steer network traffic through VNF instances. Stratos [381] is a VNF orchestrator that manages VNFs in a cloud using traffic engineering and employs horizontal scaling techniques, so that VNFs can be instantiated and/or removed. Traffic engineering techniques for managing VNFs in a SDN-based network include for example steering network traffic through an existing sequence of VNFs by using middleboxes that modify packet headers and alter traffic signatures [382], [383].

SDN, NFV and Cloud computing can enable the design, development and realization of smart cities. Essentially, smart city is a seamless integration of personal, residential, commercial, municipal, private and public devices, equipment, buildings and systems for various safety, efficiency and convenience services for its citizens. At a high level, a smart city can be organized into three tiers [355], as illustrated in Figure 17.

The first tier consists of myriad heterogeneous devices connected to each other through a wireless (*i.e.*, WiFi, cellular 4G/5G) and/or wired (*i.e.*, Ethernet, optical) access network, converged edges [360] and cloud services and applications. The converged edges on the second tier bring the cloud resources, such as compute and storage, closer to the end-users. They can include Metropolitan Area Network (MAN) edge points [355], edge nodes [255], [378], including cloudlets and fog nodes,

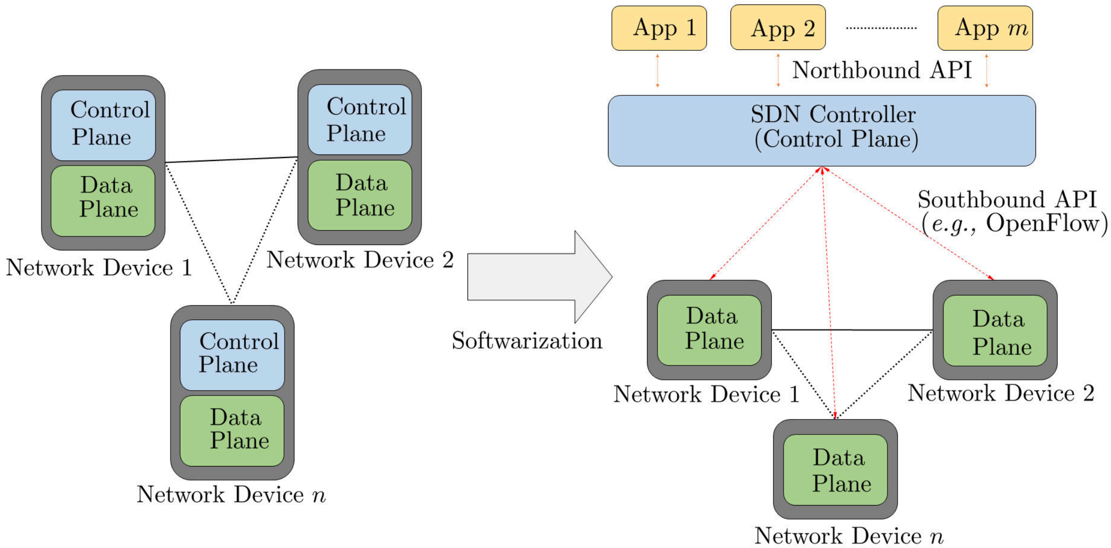


Fig. 15: High-level view of softwarization from traditional to Software-Defined Networking.

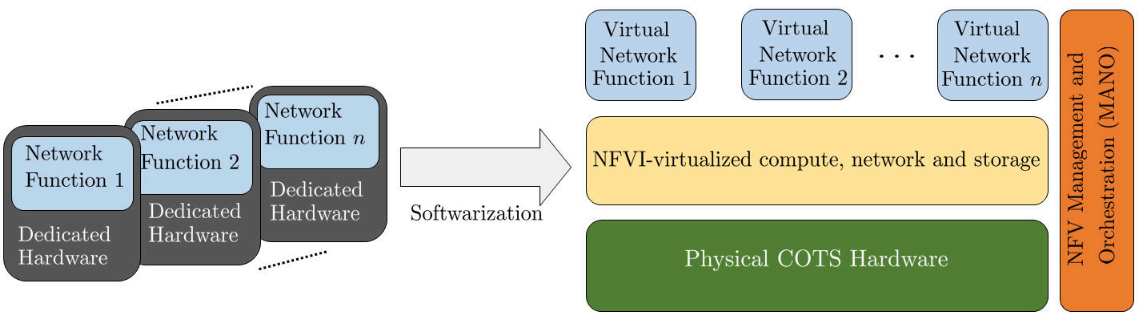


Fig. 16: High-level view of softwarization from traditional network functions to virtual network functions.

NFV/SDN based edges [384] or at telecommunication service providers [360]. They facilitate communication and information processing for low latency applications and highly localized and voluminous data processing applications, such as safety applications in ITS [362]. The third tier consists of the cloud that is interconnected by a backbone infrastructure, which can be softwarized and virtualized for various L2-L7 functions.

D. Smart City Requirements and Evaluation

In this section, we derive some of the essentials for networking in a smart city and evaluate the enabling technologies against these requirements. As illustrated in Figure 17, there are heterogeneous devices that will be connected via access networks to converged edges and traditional large scale cloud datacenters leveraging softwarization and virtualization technologies. Apart from this softwarized and hierarchical IoT for smart cities, we identify fundamental network requirements for smart cities from the literature. After a thorough review of the smart city literature [3], [4], [8], [10]–[12], [18], we deduce and present a list of fundamental networking and computing requirements for smart cities. These include heterogeneity, interoperability, QoS, configurability, management and privacy and security, as presented in Table XIII. We evaluate the enabling technologies (*i.e.*, cloud, SDN and NFV) as they are currently implemented for meeting the fundamental network requirements for smart cities.

Smart city enabling technologies must be able to meet the heterogeneity [355] and interoperability [379] requirements. The heterogeneity and interoperability in smart cities span various domains, beginning from end-user devices and network elements hardware disparity, to vendor specific proprietary software, to disparate communication protocols. Open standards must be designed for seamless integration of devices and systems, irrespective of the vendor or hardware. These standards must include overcoming heterogeneity in network access technologies and communication protocols. They must

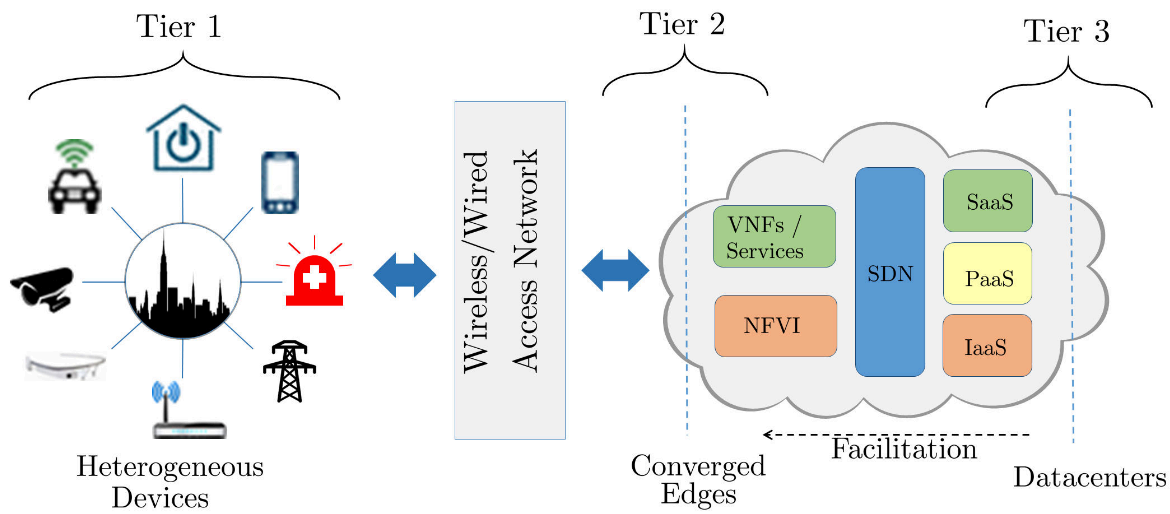


Fig. 17: Smart city facilitated by cloud, SDN and NFV.

TABLE XIII: EVALUATION OF ENABLING TECHNOLOGIES FOR MEETING THE NETWORKING AND COMPUTING REQUIREMENTS FOR SMART CITIES

Smart City Requirements		**Supported by**		
		SDN	**NFV**	**Cloud**
Heterogeneity and Interoperability	Communication Protocols	✗	✗	✗
	Network Appliances	✓	✓	✗
	End-user Devices	✗	✗	✗
QoS	Reliability	✗	✗	High
	Scalability	✗	✗	High
	Latency	High	Low	High
	Throughput	High	High	High
	Differentiated Service	✓	✓	✗
Configurability and Management		✓	✓	✓
Privacy and Security		✗	✗	✗

also enable backward compatibility with older devices and systems.

Due to the inherent techniques employed for softwarization and virtualization in SDN and NFV, they can overcome the heterogeneity in network elements and vendor specific hardware and software. For example, the design of OpenFlow enables any hardware to become OpenFlow compliant with a firmware [369]. This significantly reduces CAPEX and reduces deployment of new and costly infrastructure to facilitate Smart Cities.

Though SDN and NFV technologies do not currently enable integration of disparate communication protocols and access technologies, there are efforts underway to design, implement and experiment with a SDN based network for the integration of wired (*e.g.*, Ethernet and optical) and 802.11 wireless networks [385], and the integration of wireless 802.11 with next generation 4G/5G mobile devices [386]. On the other hand, there are SDN based solutions for delivering on-demand video and multimedia across all wireless devices using Internet Protocol (IP) Multimedia Subsystem (IMS) [387]. SDN can further extend the convergence of wired and cellular access to IMS with increased QoS, resource utilization and management [388]–[390].

The scalable and reliable [359] cloud offers high resolution data processing and storage. However, it does not overcome heterogeneity at the level of devices, network appliances or communication protocols. Each cloud provider has proprietary interfaces and development environments [359], [391], [392], which are used by service providers to build and deploy services in the cloud. This further complicates a converged solution for smart cities as service providers find it impossible to seamlessly migrate their services within and across cloud infrastructures [359]. Furthermore, the heterogeneity of datacenters and the dynamically changing demand pose unique challenges for resource provisioning in the cloud [393].

Softwarization of network and end-to-end functions can circumvent an additional layer of networking, that is, the MAN, which are deemed necessary for smart cities [355]. For example, VNFs can bypass MANs and significantly reduce CAPEX and complexity of smart cities. As MANs not only require specialized hardware but also add latency to performance of services and applications. SDN and NFV offer L2-L7 services without degradation in the QoS.

There are various QoS metrics that are typically used in evaluating network performance, such as latency, throughput, scalability, and reliability. Latency metrics can include end-to-end delay, round-trip time (RTT), jitter, reliability, availability, and packet-loss. The smart city applications and services range from mundane to extraordinary and their QoS requirements vary tremendously. Therefore, it is essential to minimize response time and end-to-end delay, and maximize throughput and reliability [379]. In fact, proponents of IoT and 5G networks instigate the need to achieve "zero-latency" communication [355] for all future Internet applications and services using effective routing [379] and converged edges [360].

As SDN decouples data and control planes and controllers update flows in the data plane, the load on the data plane burdens the controllers, decreases throughput, and increases latency of the controllers [394]. Therefore, it is essential for QoS, with respect to reliability and scalability, to efficiently deploy and maintain multiple, distributed controllers [394]. The placement of controllers and assignment of switches to controllers is often referred to as controller placement problem [395]. The controller placement technique must dynamically provision the distributed controllers [394], [395] and strategically assign switches to controllers for load balancing [394]. Controller placement strategies must minimize latency, overhead [396], cost of resource provisioning and controller placement for a scalable network infrastructure. Due to these limitations, there is currently high latency in setting up the data forwarding rules, and is often considered the major limitation in SDN scalability [397].

On the other hand, centralized and distributed controllers have been designed to meet enterprise level throughput requirements [397]. Though distributed controllers on a centralized cluster can achieve higher throughput, physically distributed controllers achieve higher resiliency [397]. Reliability in SDN based networks for smart cities must ensure availability of switches and controllers in the data and control planes, respectively [398]. To ensure availability, fault detection, prevention and recovery techniques must be employed to seamlessly recover so that switches and controllers are always reliable in the underlying communication infrastructure [398].

There are various challenges in achieving high reliability in SDN-based networks since the fault tolerance must be achieved in data and control planes. The switches in the data plane can be made intelligent to be able to perform fault detection and recovery, or the controller can detect the faults and repair the data forwarding rules to recover from these faults [398]. However, there is a limitation in the reliability offered in current SDN-based networks [397] that prevents its applicability as a pillar in networking infrastructure; it requires critical analysis of the proposed solutions, such as accounting for overhead and latency for fault recovery [398] in data and control planes.

The underlying smart city infrastructure must be capable of supporting millions of devices and systems, often mobile and intermittent. Therefore, scalability [379] is a crucial requirement for Smart Cities. SDN are not scalable for the magnitude of routes and flows required for smart city [399]. This can be overcome by employing the fundamental concept of scheduling in WSNs for monitoring, activity and packet transmission [339], [399]. On the other hand, distributed SDN controllers [400] not only increase availability and scalability of the underlying network, they can also dynamically change the load on the network links, which requires continuous monitoring for selecting optimal number of controllers and their placement in the network [395] to achieve load balancing [401], and to minimize delay and overhead due to reconfiguration between control and data forwarding planes [395], [400], [401].

Furthermore, SDN technology can be extended to include flexibility in the data plane. Therefore, a dual routing scheme can be implemented [402], such that the data plane can choose data forwarding paths to dynamically adjust to changing traffic on the network links. SDN scalability can be improved via distributed controllers and a controller placement strategy that minimizes overhead [396], and cost of resource provisioning.

Smart city network traffic is generated by mundane and critical lifesaving applications and services. Therefore, it is necessary to offer differentiated service [403], which prioritizes traffic that is generated from a small but imperative and integral set of applications and services. These applications and services pertain to emergency, first response teams initiated by police, fire and paramedic departments and emergency municipality services, or other pedestrians and vehicle safety applications in ITS [403].

VNFs performance capacity is less than their physical counterparts [404]. However, high performance VNFs that achieve the same performance of NFs hosted on specialized hardware have been implemented [405]. Nonetheless, scalability in NFV is still limited and challenging. Some of these include optimizing the mapping of SFCs to VNFs [406], [407] and increasing the capacity of virtual machines on commodity hardware using clustering [408]. It is also necessary to scrutinize dynamic allocation of resources for vertical and horizontal scaling, to increase the capacity of a virtual machine (VM) or to instantiate new VMs to spawns new VNFs, respectively. Often, this scalability is programmed in the VNF management module. It plays a critical role in minimizing the cost of VNF deployment and placement, energy consumption and communication overhead of deploying and changing placement of VNF(s) [409], [410].

However, NFV requires critical consideration for design and implementation of QoS, with respect to reliability. Current NFs on specialized hardware in telecommunication offer five-nines (99.999%) reliability [404], whereas current VNFs achieve only three-nines reliability in simulation [411]. To this end, distributed VNFs [412] and microservices [255], [413] are being scrutinized to improve scalability of NFV for large-scale deployments in support of smart cities. Cloud-based services and applications for smart cities have high scalability, reliability and throughput [359], but suffer in latency [360] for those applications that require real-time solutions [13].

Configurability and infrastructure management [379] is critical to dynamically configure and reconfigure the network in face of intermittent and faulty nodes. Various smart and often mobile devices and systems can not only arbitrarily join and leave the smart city network but may frequently move, potentially at high speeds within the smart city. Therefore, mobility management in smart city infrastructure becomes essential and can be achieved by employing IP mobility management practices to SDN [414], or novel mobility management solutions using SDN [375]. SDN controllers can be programmed to increase their configurability and management [13], [397].

These management protocols monitor mobile nodes to facilitate continuous connectivity by configuring and reconfiguring the SDN nodes in the smart city network. NFV can ease the deployment and management of smart city networks with respect to planned and routine maintenance [404] and improves the utilization of resources by reducing over-provisioning of resources [404]. However, orchestration of VNFs in the NFVI in a smart city is complicated as VNFs also have to meet requirements for reliability and low latency. Therefore, there is a trade-off between increased reliability and low maintenance overhead.

Privacy and Security [353] are essential to encourage the widespread integration of various smart devices and systems into an IoT for smart cities. Therefore, it is essential to guarantee privacy of end-users and security of data and information of private and public systems, such as smart power grids and intelligent road infrastructure. Currently, SDN, NFV and cloud suffer from security and privacy issues [353], [376], [415]–[417]. It is a challenge to ensure security for Smart City applications and users. However, there are proposals of using black networks and registries [353] as fundamental building blocks for secure smart cities.

SDN can enable a more secure smart city infrastructure with the introduction of trusted SDN controllers [353] that have a global view of the network and can route packets efficiently. The SDN controllers can route smart city data packets through black networks [418] that preserve privacy of payload and meta-data to deter a wide range of security attacks. The data forwarding rules can include routing and scheduling traffic flows based on availability of nodes [353] to accommodate for unpredictability of nodes that abruptly join, move and leave the smart city network.

Therefore, there are various advantages of SDN, NFV and cloud due to programmability and virtualization, such as ease in dynamic adaptation of network functions and data forwarding rules, the increased utilization of resources and utility like computing resources available throughout a large scale network. Furthermore, SDN and NFV overcome vendor lock-in in cloud infrastructure [359], vendor specific devices and protocols for network elements and communication [403]. Smart cities require modeling techniques, architectures and algorithms that support virtualization and multiple heterogeneous services to be hosted on a single platform [393], [408].

The smart city models must achieve a high level of security and resilience to faults and threats. Furthermore, these technologies cost effectively facilitate the transformation of the traditional home and business to virtualized home and business. They reduce hardware devices, specialized maintenance and support, and CAPEX and OPEX [355]. It is important to note that, as businesses migrate to the cloud, smart city models reduce CAPEX but increase OPEX [419]. Therefore, in smart cities, there is a need to find solutions for reducing OPEX costs.

Testbeds and frameworks are vital to the realization of smart cities for simulation and experimentation. Table XIV presents some testbeds and frameworks for simulation and experimentation [379], [382], [420]–[422] for the enabling technologies. Some of the frameworks have been designed for experimentation and simulation of smart city applications, services and deployment, while others are experimentation and simulation frameworks for some of the enabling technologies and are not smart city specific. Smart city specific testbeds and frameworks must support large scale deployment, in the order of millions of heterogeneous devices and connections over diverse communication protocols. Nevertheless, these testbeds and frameworks allow preliminary study of SDN, NFV and cloud, including various

TABLE XIV: FRAMEWORKS USING SDN, NFV, CLOUD COMPUTING AND THEIR APPLICABILITY FOR SMART CITY EXPERIMENTATION

Framework / Testbed	Technology			Applicable to Smart Cities
	SDN	NFV	Cloud	
ADRENALINE [421]		•	•	
CityFlow [420]	•			•
SELFNET [384]	•	•	•	
TRESCIMO [379]		•		•
CloudSimNFV [422]		•	•	

aspects in programming, virtualization, cloud services and dynamic resource provisioning at L2-L7 layers.

E. Insights and Research Challenges

We have discussed the essential networking and computing technologies for smart cities. Inherently, the softwarization and virtualization used by the enabling technologies greatly reduce CAPEX and OPEX, overcome vendor lock-in and are a step towards integration of heterogeneous devices. However, there are various open research challenges, limiting the realization of smart cities. We discussed many of these open research challenges while evaluating the enabling technologies in the previous subsection. Here, we take a step back and highlight critical insights and present open research challenges from a broader perspective that will dramatically increase the feasibility and realization of smart city infrastructure, applications and services.

1) Integration of Softwarization with 5G

A critical and fundamental open research challenge remains to integrate the Long Term Evolution (LTE) of next generation cellular systems (*i.e.*, 5G) into the IoT ecosystem. The most fundamental benefit to IoT is the promised ultra-low latency of 5G networks. This will require a seamless integration of 5G enabled devices with the smart devices and systems in the softwarized IoT ecosystem. Therefore, it remains an open problem to evaluate performance of existing softwarization technologies, such as SDN and NFV, for 5G cellular systems [423]. It is envisaged that 5G devices will be integrated in the IoT ecosystems as gateways to sensor networks that offer low latency and high performance. Thus, it is evident that the softwarized and virtualized IoT infrastructure will have to be integrated with 5G. In order to achieve this, there are various challenges, such as dynamic cell configuration, load balancing, resource management, and spectrum and transmission power assignment to involved cells. A fundamental problem is the assignment of the best interconnections between pure 5G devices and 5G enabled IoT devices, to offer differentiated QoS. This will require activation of the appropriate transceivers that will be involved in the handling of a particular situation to offer differentiated QoS.

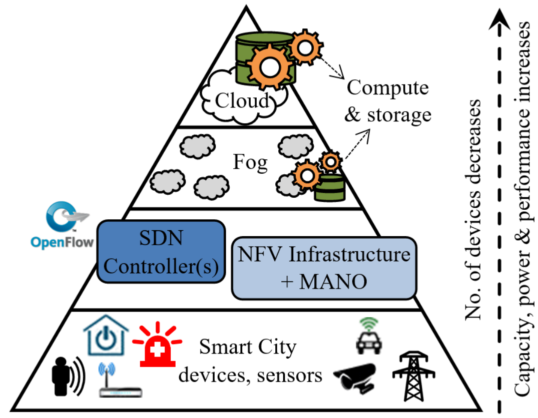


Fig. 18: IoT pyramid for a smart city.

2) Fog Computing

Smart city infrastructure, applications and services will need to bring cloud-like resources and computing closer to the end-users. Primarily, this will significantly reduce the latency and the unnecessary traffic to the cloud. Fog computing achieves this with fog nodes, that are generally much smaller than cloud nodes, but more powerful than the smart devices and systems at the extreme end of the IoT spectrum. Fog nodes offer low latency and high performance for processing and aggregating localized data. Therefore, an IoT fog that spans across access, aggregation and core layers in the network domain and the "things" of the IoT, will greatly improve feasibility of smart cities.

Figure 18 illustrates the envisaged pyramid for an IoT of a smart city. The voluminous data generated by the IoT in the smart city will leverage the low-latency and higher performance of the IoT Fog for integration, data management and analytics necessary for smart cities. The IoT fog will leverage virtualization, software-defined control and flexible configuration of integrated 5G technology with mobile edge cloud and cloud computing to provide an agile infrastructure. This will achieve greater connectivity, with lower latency for smart city applications.

Therefore, leveraging softwarization and fog computing will enable an agile infrastructure that will increase connectivity, reliability and productivity of the IoT for smart cities.

IX. Conclusion

The "smartness" of a city is in essence a measure of convergence. It is imperative to achieve convergence of the disparate devices and systems with a unified framework for managing data through its lifecycle. The ultimate goal is to improve citizens' quality of life, reduce cost of living and attain a sustainable environment. To this end, we review various use cases and deployments of smart city infrastructure, application and services and highlight the lessons learnt.

Realizing a smart city requires maturity of critical components, such as, privacy and security, service discovery, edge computing, dynamic resource provisioning, and configuration and management of the underlying IoT enabling the smart city. In this survey, we extensively discussed data management techniques for data acquisition, processing and dissemination. Data acquisition techniques are still pending standards to enable interoperability, consistency and reusability across heterogeneous devices, systems, applications and services. Data processing techniques are employed to aggregate data, deduce patterns for data generation and information access and perform data analytics for streamlining the smart city. Data dissemination techniques offer prioritized and differentiated access to data and information based on the type of user, that is residential, commercial, industrial, governmental, etc.

We thoroughly discuss softwarization and virtualization of networking, with Cloud Computing, Software-Defined Networking and Network Functions Virtualization to provide freedom of deploying network functions on commercial-off-the-shelf hardware rather than proprietary hardware, agility in deployment, configurability and maintenance and lower capital expenditure costs. Throughout the survey, we identify limitations and present research challenges for data management, data security and privacy, and networking and computing technologies that enable smart cities.

In conclusion, the lack of a standard definition of a smart city eventually results in various shortcomings in many facets of a smart city. Amongst many things, there is lack of architecture, framework and standards for data management, networking and computing technologies, experimentation and simulation frameworks and facilities that impede the large-scale deployment of smart cities. The research challenges illustrate that there are various emerging areas in smart cities that can greatly benefit from an open, interdisciplinary, holistic approach for designing integrated solutions for enabling smart cities.

X. Acronyms

The acronyms used throughout the survey and their definitions are listed in Table XV.

References

[1] United Nations, "World's population increasingly urban with more than half living in urban areas," 2014, (Accessed on December 2016). [Online]. Available: http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

[2] D. Evans, "The internet of things: how the next evolution of the internet is changing everything," 2011. [Online]. Available: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, "A global perspective of smart cities: A survey," in *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, July 2013, pp. 439–444.

[4] V. Fernandez-Anez, *Stakeholders Approach to Smart Cities: A Survey on Smart City Definitions*. Cham: Springer International Publishing, 2016, pp. 157–167. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-39595-1_16

[5] E. M. Biggs, E. Bruce, B. Boruff, J. M. Duncan, J. Horsley, N. Pauli, K. McNeill, A. Neef, F. Van Ogtrop, J. Curnow *et al.*, "Sustainable development and the water–energy–food nexus: A perspective on livelihoods," *Environmental Science & Policy*, vol. 54, pp. 389–397, 2015.

[6] Scott Hilton, "Summary of friday october 21 attack," 2016, (Accessed on January 2017). [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[7] ETSI, "ETSI - smart cities," 2016, (Accessed on December 2016). [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/smart-cities

[8] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah, and P. Siano, "IoT-based smart cities: a survey," 2016, (Accessed on December 2016). [Online]. Available: https://www.researchgate.net/profile/Aurelio_Tommasetti/publication/301790173_IoT-based_Smart_Cities_a_Survey/links/572cc90108aee02297597c99.pdf

[9] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Data collection and wireless communication in internet of things (iot) using economic analysis and pricing models: A survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 4, pp. 2546–2590, Fourthquarter 2016.

[10] W. M. da Silva, A. Alvaro, G. H. Tomas, R. A. Afonso, K. L. Dias, and V. C. Garcia, "Smart cities software architectures: a survey," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 2013, pp. 1722–1727.

[11] D. El Baz and J. Bourgeois, "Smart cities in europe and the alma logistics project," *ZTE Communications*, vol. 13, no. 4, 2015.

[12] S. Ijaz, M. A. Shah, A. Khan, and M. Ahmed, "Smart cities: A survey on security concerns," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 2, pp. 612–625, 2016.

[13] R. Petrolo, V. Loscrì, and N. Mitton, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms," *Trans. Emerging Telecommunications Technologies*, vol. 28, 2017.

[14] C. Perera, Y. Qin, J. C. Estrella, S. Reiff-Marganiec, and A. V. Vasilakos, "Fog computing for sustainable smart cities: A survey," *arXiv preprint arXiv:1703.07079*, 2017.

[15] W. Shuai, P. Maillé, and A. Pelov, "Charging electric vehicles in the smart city: A survey of economy-driven approaches," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2089–2106, 2016.

[16] L. Wang and D. Sng, "Deep learning algorithms with applications to video analytics for a smart city: A survey," *arXiv preprint arXiv:1512.03131*, 2015.

[17] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, 2016.

[18] S. Djahel, R. Doolan, G.-M. Muntean, and J. Murphy, "A communications-oriented perspective on traffic management systems for smart cities: challenges and innovative approaches," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 125–151, 2015.

TABLE XV: ACRONYMS USED IN THE SURVEY AND THEIR DEFINITIONS

Acronym	Definition		Acronym	Definition		Acronym	Definition
AI	Artificial Intelligence		ICIC	IoT City Innovation Center		RBM	Restricted Boltzmann Machines
ANPR	Automatic Number Plate Reading Cameras		ICS	Industrial Control Systems		RDD	Resilient Distributed Dataset
API	Application Programming Interface		ICT	Information Communication Technology		RFID	Radio Frequency Identification
ATSC	Advanced Solid State Traffic Controllers		IDS	Intrusion Detection System		RSU	Road Side Unit
BSM	Basic Safety Messages		IMS	Internet Multimedia Subsystems		RTC	Real-Time Clock
CAPEX	Capital Expenditure		IoT	Internet of Things		RTT	Round Trip Time
CCTV	Closed Circuit Television Cameras		IP	Internet Protocol		SaaS	Software as a Service
CDR	Caller Detail Record		ITS	Intelligent Transportation System		SCaaS	Smart City as a Service
CHP	Combined Heating and Power Plants		LED	Light Emitting Diodes		SCADA	Supervisory Control and Data Acquisition
CIA	Central Intelligence Agency		LSTM	Long Short Term Memory		SDN	Software-Defined Networking
COTS	Commercial off the Shelf		LTE	Long Term Evolution		SFC	Service Function Chain
D2D	Device to Device		MAN	Metropolitan Area Network		SG	Smart Grid
DALI	Digital Addressable Lighting Interface		MANETs	Mobile Ad hoc Networks		SLA	Service Layer Agreement
DDoS	Distributed Denial of Service		MANO	NFV Management and Orchestration		SM	Smart Mobility
DER	Distributed Energy Resources		MAPE	Mean Absolute Percentage Error		SPS	Standard Positioning System
DG	Distributed Generation		MLAAS	Machine Learning As A Service		SVM	Support Vector Machines
DNP	Distributed Network Protocol		NAT	Network Address Translation		TMC	Traffic Management Center
DoIT	Department of Innovation and Technology		NF	Network Function		TMS	Traffic Management Systems
DoS	Denial of Service		NFV	Network Functions Virtualization		TPM	Trusted Platform Module
DPI	Deep Packet Inspection		NFVI	NFV Infrastructure		TrAD	Traffic Adaptive Data Dissemination
DSPF	Distributed Stream Processing Framework		NOS	Network Operating Systems		UAV	Unmanned Aerial Vehicle
DTN	Delay Tolerant Networks		OCPP	Open Charge Point Protocol		V2I	Vehicle to Infrastructure
EAEP	Edge Aware Epidemic Protocol		P2P	Peer to Peer		V2V	Vehicle to Vehicle
EDCA	Elliptic Curve Digital Signature Algorithm		PaaS	Platform as a Service		VANETs	Vehicular Ad hoc Networks
EHR	Electronic Health Record		PKI	Public Key Infrastructure		VLC	Visible Light Communication
EMS	Energy Management Systems		PLC	Power Line Communication		VM	Virtual Machine
ESS	Energy Storage Systems		PPS	Precise Positioning System		VMT	Vehicle Miles Traveled
FEW	Food, Energy, Water		PV	Photo-Voltic		VNF	Virtual Network Function
GIS	Geographic Information Systems		QA	Questions Answering		VPP	Virtual Power Plant
HE	HAMBURG ENERGIE		QoS	Quality of Service		WSN	Wireless Sensor Networks
IaaS	Infrastructure as a Service						

[19] Taiwan Sourcing Service Provider. (2015) Green ideas technology introduces blind-spot-free smart lighting control system. (Accessed October 2016). [Online]. Available: http://www.cens.com/cens/html/en/news/news_inner_48111.html

[20] P. C. Veena, P. Tharakan, H. Haridas, K. Ramya, R. Joju, and T. S. Jyothis, "Smart street light system based on image processing," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, March 2016, pp. 1–5.

[21] M. H. Sheu, L. H. Chang, S. C. Hsia, and C. C. Sun, "Intelligent system design for variable color temperature led street light," in *2016 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, May 2016, pp. 1–2.

[22] A. Jain and C. Nagarajan, "Efficient control algorithm for a smart solar street light," in *9th International Conference on Next Generation Mobile Applications, Services and Technologies*. IEEE, 2015, pp. 376–381.

[23] F. J. Bellido-Outeiriño, F. J. Quiles-Latorre, C. D. Moreno-Moreno, J. M. Flores-Arias, I. Moreno-García, and M. Ortiz-López, "Streetlight control system based on wireless communication over dali protocol," *Sensors*, vol. 16, no. 5, p. 597, 2016.

[24] J. Crowther, C. Herzig, and G. Feller, "The time is right for connected public lighting within smart cities," *Philips and Cisco Internet Business Solutions Group(IBSG)*, 2012, (Accessed on September 2016).

[25] Y. Helmy, "Smart + connected communities solutions for a smart city," Cisco, 2014, (Accessed on September 2016). [Online]. Available: https://www.cisco.com/web/offer/emear/38586/images/Presentations/P15.pdf

[26] Silver Spring Networks, "White paper: The business case for smart street lights," 2013, (Accessed on September 2016). [Online]. Available: http://www.silverspringnet.com/wp-content/uploads/SilverSpring-Whitepaper-Smart-Street-Light-Bizcase.pdf

[27] F. Leccese, "Remote-control system of high efficiency and intelligent street lighting using a zigbee network of devices and sensors," *IEEE transactions on power delivery*, vol. 28, no. 1, pp. 21–28, 2013.

[28] R. Caponetto, G. Dongola, L. Fortuna, N. Riscica, and D. Zufacchi, "Power consumption reduction in a remote controlled street lighting system," in *2008 International Symposium on Power Electronics, Electrical Drives, Automation and Motion*, June 2008, pp. 428–433.

[29] G. W. Denardin, C. H. Barriquello, A. Campos, and R. N. do Prado, "An intelligent system for street lighting monitoring and control," in *2009 Brazilian Power Electronics Conference*, pp. 274–278.

[30] C. Iordache, S. Gavat, C. Mada, D. Stanciu, and C. Holban, "Streetlight monitoring and control system Part I: System structure," in *2008 IEEE International Conference on Automation, Quality and Testing, Robotics*, vol. 3, May, pp. 183–186.

[31] K. Rajput, G. Khatav, M. Pujari, and P. Yadav, "Intelligent street lighting system using gsm," *International Journal of Engineering Science Invention*, vol. 2, no. 3, pp. 60–69, 2013.

[32] A. Lavric, V. Popa, I. Finis, and D. Simion, "The design and implementation of an energy efficient street lighting monitoring and control system," *Przeglad Elektrotechniczny*, no. 11, pp. 312–316, 2012.

[33] S. Cho and V. Dhingra, "Street lighting control based on lonworks power line communication," in *2008 IEEE International Symposium on Power Line Communications and Its Applications*, April, pp. 396–398.

[34] J. Liu, C. Feng, X. Suo, and A. Yun, "Street lamp control system based on power carrier wave," in *2008 International Symposium on Intelligent Information Technology Application Workshops*, Dec, pp. 184–188.

[35] A. Bruno, F. Di Franco, and G. Rasconà, "Smart street lighting," *EE Times*, 2012, (Accessed on December 2016). [Online]. Available: http://www.eetimes.com/design/smartenergy-design/4375167/Smart-street-lighting

[36] C. Badgaiyan and P. Sehgal, "Smart street lighting system," *International Journal of Science and Research*, vol. 4, no. 7, 2015.

[37] Y. Fujii, N. Yoshiura, A. Takita, and N. Ohta, "Smart street light system with energy saving function based on the sensor network," in *Proceedings of the Fourth International Conference on Future Energy Systems*, ser. e-Energy '13, New York, NY, USA, 2013, pp. 271–272. [Online]. Available: http://doi.acm.org/10.1145/2487166.2487202

[38] Cisco, "Amsterdam uses IoE-driven capabilities to cut energy usage, improve electric grids reliability, and more," 2014, (Accessed on September 2016). [Online]. Available: http://internetofeverything.cisco.com/sites/default/files/pdfs/Amsterdam_Jurisdiction_Profile__051214REV.pdf

[39] San Jose City Hall, "Innovative LED streetlight replacement RFP, url = http://www.sanjoseca.gov/LEDrfp, note = (Accessed on September 2016)."

[40] IBM, "IBMs smarter cities challenge: Boston report," 2012, (Accessed on December 2016). [Online]. Available: https://smartercitieschallenge.org/assets/cities/boston-united-states/documents/boston-united-states-full-report-2012.pdf

[41] New York Department of Transportation. (2012) Press release number 12-25. (Accessed on September 2016). [Online]. Available: http://www.nyc.gov/html/dot/html/pr2012/pr12_25.shtml

[42] Waze, "Join the connected citizens free data exchange program from Waze!" (Accessed on April 2017). [Online]. Available: https://www.waze.com/ccp

[43] E. Blayney, "Louisville leverages crowdsourcing for civic good," 2016, (Accessed on April 2017). [Online]. Available: http://datasmart.ash.harvard.edu/news/article/louisville-leverages-crowdsourcing-for-civic-good-919

[44] A. Zurborg, "Unlocking customer value: The virtual power plant," *US Department of Energy*, 2010.

[45] M. M. Othman, Y. Hegazy, and A. Y. Abdelaziz, "A review of virtual power plant definitions, components, framework and optimization," *International Electrical Engineering Journal*, vol. 6, no. 9, pp. 2010–2024, 2015.

[46] Bosch, "Virtual power plant manager activated-grid and energy trading optimized," 2015, (Accessed on September 2016). [Online]. Available: https://www.bosch-si.com/media/en/bosch_software_innovations/documents/brochure/energy_4/virtual_power_plant_energy.pdf

[47] O. C. Alliance, "Open charge point protocol 1.6," (Accessed on September 2016). [Online]. Available: http://www.openchargealliance.org/protocols/ocpp/ocpp-16/

[48] P. P. Vuthi, P. Lorenzen, H. Schaefers, S. Raths, S. Krengel, J. Sudeikat, and M. Thomsen, "Smart power hamburg: A virtual power plant for hamburg," in *Proceedings of International ETG Congress; Die Energiewende-Blueprints for the new energy age*. VDE, 2015, pp. 1–8.

[49] R. Van Brakel and P. De Hert, "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Technology-led policing*, vol. 20, p. 165, 2011.

[50] K. Finch and O. Tene, "Welcome to the metropticon: Protecting privacy in a hyperconnected town," *Fordham Urb. LJ*, vol. 41, p. 1581, 2013.

[51] Honeywell, "Bhubaneswar's smart safety city surveillance project powered by honeywell technologies," (Accessed on September 2016). [Online]. Available: http://www.honeywell.com/newsroom/news/2015/05/bhubaneswars-smart-safety-city-surveillance-project-powered-by-honeywell-technologies

[52] G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, "A survey on ambient intelligence in healthcare," *Proceedings of the IEEE*, vol. 101, no. 12, pp. 2470–2494, 2013.

[53] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, 2016.

[54] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile networks and applications*, vol. 16, no. 2, pp. 171–193, 2011.

[55] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[56] E. J. Pauwels, A. A. Salah, and R. Tavenard, "Sensor networks for ambient intelligence," in *IEEE 9th Workshop on Multimedia Signal Processing*, 2007, pp. 13–16.

[57] T. He, S.-H. G. Chan, and C.-F. Wong, "Homemesh: a low-cost indoor wireless mesh for home networking," *IEEE Communications Magazine*, vol. 46, no. 12, pp. 79–85, 2008.

[58] G. Singla, D. J. Cook, and M. Schmitter-Edgecombe, "Recognizing independent and joint activities among multiple residents in smart environments," *Journal of ambient intelligence and humanized computing*, vol. 1, no. 1, pp. 57–63, 2010.

[59] L. Chen, J. Hoey, C. D. Nugent, D. J. Cook, and Z. Yu, "Sensor-based activity recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 42, no. 6, pp. 790–808, 2012.

[60] P. Rashidi and D. J. Cook, "Keeping the resident in the loop: adapting the smart home to the user," *IEEE Transactions on systems, man, and cybernetics-part A: systems and humans*, vol. 39, no. 5, pp. 949–959, 2009.

[61] E. O. Heierman and D. J. Cook, "Improving home automation by discovering regularly occurring device usage patterns," in *Third IEEE International Conference on Data Mining*, pp. 537–540.

[62] A. C. Tran, S. Marsland, J. Dietrich, H. W. Guesgen, and P. Lyons, "Use cases for abnormal behaviour detection in smart homes," in *International Conference on Smart Homes and Health Telematics*. Springer, 2010, pp. 144–151.

[63] E. Turban, "Implementing decision support systems: a survey," in *1996 IEEE International Conference on Systems, Man and Cybernetics. Information Intelligence and Systems (Cat. No.96CH35929)*, vol. 4, pp. 2540–2545 vol.4.

[64] Boston Children's Hospital and Harvard Medical School, "Smart, an app platform for healthcare," (Accessed October 2016). [Online]. Available: http://smarthealthit.org/

[65] National Operational Programme for Research and Competitiveness Convergence, "Smart health 2.0, infrastructure scope," (Accessed on October 2016). [Online]. Available: http://www.smarthealth2.com/eng/?page=infrastructural

[66] ——, "Smart health 2.0, application scope," (Accessed on October 2016). [Online]. Available: http://www.smarthealth2.com/eng/?page=application

[67] Enterprise Innovation, "Saensuk smart city launches smart healthcare pilot," 2016, (Accessed on October 2016). [Online]. Available: http://www.enterpriseinnovation.net/article/saensuk-smart-city-launches-smart-healthcare-pilot-1759874204

[68] N. Yoshiura, Y. Fujii, and N. Ohta, "Smart street light system looking like usual street lights based on sensor networks," in *13th IEEE International Symposium on Communications and Information Technologies*, 2013, pp. 633–637.

[69] M. Popa and A. Marcu, "A solution for street lighting in smart cities," *Carpathian Journal of Electronic and Computer Engineering*, vol. 5, p. 91, 2012.

[70] S. P. Lau, G. V. Merrett, A. S. Weddell, and N. M. White, "A traffic-aware street lighting scheme for smart cities using autonomous networked sensors," *Computers & Electrical Engineering*, vol. 45, pp. 192–207, 2015.

[71] J. Chunguo, W. Yan, S. Wenyi, and S. Xin, "Design of street light pole controller based on WSN," in *10th IEEE International Conference on Electronic Measurement & Instruments*, vol. 3, 2011, pp. 147–150.

[72] C.-l. Fan and Y. Guo, "The application of a zigbee based wireless sensor network in the LED street lamp control system," in *IEEE International Conference on Image Analysis and Signal Processing*, 2011, pp. 501–504.

[73] R. Abinaya, V. Varsha, and K. Hariharan, "An intelligent street light system based on piezoelectric sensor networks," *Indian Journal of Science and Technology*, vol. 9, no. 43, 2016.

[74] S. Y. Cheung, S. C. Ergen, and P. Varaiya, "Traffic surveillance with wireless magnetic sensors," in *Proceedings of the 12th ITS world congress*, vol. 1917, 2005, pp. 173–181.

[75] R. K. Megalingam, V. Mohan, P. Leons, R. Shooja, and A. M., "Smart traffic controller using wireless sensor network for dynamic traffic routing and over speed detection," in *2011 IEEE Global Humanitarian Technology Conference*, pp. 528–533.

[76] S. Lee, D. Yoon, and A. Ghosh, "Intelligent parking lot application using wireless sensor networks," in *2008 International Symposium on Collaborative Technologies and Systems*, May 2008, pp. 48–57.

[77] V. W. s. Tang, Y. Zheng, and J. Cao, "An intelligent car park management system based on wireless sensor networks," in *2006 First International Symposium on Pervasive Computing and Applications*, pp. 65–70.

[78] J. Chinrungrueng, U. Sunantachaikul, and S. Triamlumlerd, "Smart parking: An application of optical wireless sensor network," in *IEEE International Symposium on Applications and the Internet Workshops*, 2007, pp. 66–66.

[79] F. A. Al-Nasser and H. Rowaihy, "Simulation of dynamic traffic control system based on wireless sensor network," in *2011 IEEE Symposium on Computers Informatics*, pp. 40–45.

[80] M. Tubaishat, Y. Shang, and H. Shi, "Adaptive traffic light control with wireless sensor networks," in *Proceedings of IEEE consumer communications and networking conference*, 2007, pp. 187–191.

[81] A. Pascale, M. Nicoli, F. Deflorio, B. Dalla Chiara, and U. Spagnolini, "Wireless sensor networks for traffic management and road safety," *IET Intelligent Transport Systems*, vol. 6, no. 1, pp. 67–77, 2012.

[82] M. Karpiriski, A. Senart, and V. Cahill, "Sensor networks for smart roads," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06)*, 2006, pp. 5–pp.

[83] R. Moghe, F. C. Lambert, and D. Divan, "Smart stick-on sensors for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 241–252, 2012.

[84] R. Moghe, A. R. Iyer, F. C. Lambert, and D. M. Divan, "A low-cost wireless voltage sensor for monitoring mv/hv utility assets," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 2002–2009, 2014.

[85] K.-S. Chang, S.-M. Kang, K.-J. Park, S.-H. Shin, H.-S. Kim, and H.-S. Kim, "Electric field energy harvesting powered wireless sensors for smart grid," *Journal of Electrical Engineering and Technology*, vol. 7, no. 1, pp. 75–80, 2012.

[86] M. Erol-Kantarci and H. T. Mouftah, "Wireless sensor networks for cost-efficient residential energy management in the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 314–325, 2011.

[87] A. Barbato, A. Capone, M. Rodolfi, and D. Tagliaferri, "Forecasting the usage of household appliances through power meter sensors for demand management in the smart grid," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 404–409.

[88] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE transactions on industrial electronics*, vol. 57, no. 10, pp. 3557–3564, 2010.

[89] D. Bruckner, G. Zucker, J. Simo, W. Herzner, and S. Mahlknecht, "Semantic neighborhood sensor network for smart surveillance applications," in *Proceedings of the 3rd International Conference from Scientific Computing to Computational Engineering*, 2008.

[90] M. Sathishkumar and S. Rajini, "Smart surveillance system using PIR sensor network and GSM," *International Journal of Advnced Research in Computer Engineering & Technology*, vol. 4, no. 1, 2015.

[91] W. T. Chen, P. Y. Chen, W. S. Lee, and C. F. Huang, "Design and implementation of a real time video surveillance system with wireless sensor networks," in *2008 IEEE Vehicular Technology Conference (VTC)*, pp. 218–222.

[92] S. Saha and S. Neogy, "A case study on smart surveillance

application system using WSN and IP webcam," in *2014 Applications and Innovations in Mobile Computing (AIMoC)*, pp. 36–41.

[93] Y.-D. Lee and W.-Y. Chung, "Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring," *Sensors and Actuators B: Chemical*, vol. 140, no. 2, pp. 390–395, 2009.

[94] G. Virone, A. Wood, L. Selavo, Q. Cao, L. Fang, T. Doan, Z. He, and J. Stankovic, "An advanced wireless sensor network for health monitoring," in *Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2)*, 2006, pp. 2–4.

[95] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *Journal of mobile multimedia*, vol. 1, no. 4, pp. 307–326, 2006.

[96] A. Darwish and A. E. Hassanien, "Wearable and implantable wireless sensor network solutions for healthcare monitoring," *Sensors*, vol. 11, no. 6, pp. 5561–5595, 2011.

[97] J. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Lin, S. Son, R. Stoleru, and A. Wood, "Wireless sensor networks for in-home healthcare: Potential and challenges," in *High confidence medical device software and systems (HCMDSS) workshop*, 2005, pp. 2–3.

[98] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2688–2710, 2010.

[99] Y. Liao, M. S. Leeson, and M. D. Higgins, "Flexible quality of service model for wireless body area sensor networks," *Healthcare technology letters*, vol. 3, no. 1, pp. 12–15, 2016.

[100] M. Arifuzzaman, C. Behrend, J. DesJardins, and J. N. Anker, "A smart polymer hydrogel as a chemical sensor on biomedical implant," 2016, (Accessed on December 2016). [Online]. Available: http://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1005&context=cars

[101] W. A. Jabbar, M. Ismail, and R. Nordin, "On the performance of the current MANET routing protocols for VoIP, HTTP, and FTP applications," *Journal of Computer Networks and Communications*, vol. 2014, 2014.

[102] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, "Convergence of manet and wsn in IoT urban scenarios," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3558–3567, 2013.

[103] G. Cardone, P. Bellavista, A. Corradi, and L. Foschini, "Effective collaborative monitoring in smart cities: Converging MANET and WSN for fast data collection," in *Proceedings of ITU Kaleidoscope 2011: The Fully Networked Human? - Innovations for Future Networks and Services (K-2011)*, Dec 2011, pp. 1–8.

[104] A. Didolkar and F. Zama, "SMARTIE: A security solution for a smart city using internet of things - architecture reference model," *International Journal of Advance Research and Innovative Ideas in Education*, vol. 2, no. 4, 2016.

[105] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 2014.

[106] P. Ranjan and K. K. Ahirwar, "Comparative study of vanet and manet routing protocols," in *Proc. of the International Conference on Advanced Computing and Communication Technologies*, 2011.

[107] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 536–551, Feb 2013.

[108] O. Trullols-Cruces, M. Fiore, and J. Barcelo-Ordinas, "Cooperative download in vehicular environments," *IEEE Transactions on Mobile Computing*, vol. 11, no. 4, pp. 663–678, April 2012.

[109] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[110] M. Stolpe, "The internet of things: Opportunities and challenges for distributed data analysis," *SIGKDD Explorations Newsletter*, vol. 18, no. 1, pp. 15–34, 2016.

[111] V. Gazis, C. G. Cordero, E. Vasilomanolakis, P. Kikiras, and A. Wiesmaier, *Security Perspectives for Collaborative Data Acquisition in the Internet of Things*, 2014, pp. 271–282.

[112] R. Van Kranenburg and A. Bassi, "IoT challenges," *Communications in Mobile Computing*, vol. 1, no. 1, p. 1, 2012.

[113] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349–359, Aug 2014.

[114] H.-D. Ma, "Internet of things: Objectives and scientific challenges," *Journal of Computer science and Technology*, vol. 26, no. 6, pp. 919–924, 2011.

[115] M. DAloia, M. Rizzi, R. Russo, M. Notarnicola, and L. Pellicani, "A marker-based image processing method for detecting available parking slots from UAVs," in *International Conference on Image Analysis and Processing*. Springer, 2015, pp. 275–281.

[116] F. Mohammed, A. Idries, N. Mohamed, J. Al-Jaroodi, and I. Jawhar, "UAVs for smart cities: Opportunities and challenges," in *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, May 2014, pp. 267–273.

[117] ——, "Opportunities and challenges of using UAVs for Dubai smart city," in *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)*, March 2014, pp. 1–4.

[118] G. Ermacora, S. Rosa, and A. Toma, "Fly4smartcity: A cloud robotics service for smart city applications," *Journal of Ambient Intelligence and Smart Environments*, vol. 8, no. 3, pp. 347–358, 2016.

[119] G. Ermacora, A. Toma, S. Rosa, B. Bona, M. Chiaberge, M. Silvagni, M. Gaspardone, and R. Antonini, "A cloud based service for management and planning of autonomous UAV missions in smart city scenarios," in *International Workshop on Modelling and Simulation for Autonomous Systems*. Springer, 2014, pp. 20–26.

[120] A. Witayangkurn, M. Nagai, K. Honda, M. Dailey, and R. Shibasaki, "Real-time monitoring system using unmanned aerial vehicle integrated with sensor observation service," in *Conference on Unmanned Aerial Vehicle in Geomatics*, 2011.

[121] J. Xie, F. AI-Emrani, Y. Gu, Y. Wan, and S. Fu, "UAV-carried long distance Wi-Fi communication infrastructure," in *AIAA Infotech@ Aerospace*, 2016, p. 0747.

[122] E. Psomakelis, F. Aisopos, A. Litke, K. Tserpes, M. Kardara, and P. M. Campo, "Big IoT and social networking data for smart cities: Algorithmic improvements on big data analysis in the context of radical city applications," *arXiv preprint arXiv:1607.00509*, 2016.

[123] F. Aisopos, A. Litke, M. Kardara, K. Tserpes, P. M. Campo, and T. Varvarigou, "Social network services for innovative smart cities: the radical platform approach," *Journal of Smart Cities*, vol. 2, no. 1, 2016.

[124] C. Samaras, A. Vakali, M. Giatsoglou, D. Chatzakou, and L. Angelis, "Requirements and architecture design principles for a smart city experiment with sensor and social networks integration," in *Proceedings of the 17th Panhellenic Conference on Informatics*. ACM, 2013, pp. 327–334.

[125] B.-C. Chifor, I. Bica, and V.-V. Patriciu, "Sensing service architecture for smart cities using social network platforms," *Soft Computing*, pp. 1–10, 2016.

[126] A. Clarke and R. Steele, "How personal fitness data can be re-used by smart cities," in *2011 Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Dec 2011, pp. 395–400.

[127] L. Cilliers and S. Flowerday, "Information security in a public safety, participatory crowdsourcing smart city project," in *World*

Congress on Internet Security (WorldCIS-2014), Dec 2014, pp. 36–41.

[128] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, "Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing," *IEEE Access*, vol. 4, pp. 529–541, 2016.

[129] S. N. Chowdhury, S. Dhawan, and A. Agnihotri, "Crowdsourcing for smart cities," in *2016 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*, May 2016, pp. 360–365.

[130] D. Schuurman, B. Baccarne, L. De Marez, and P. Mechant, "Smart ideas for smart cities: Investigating crowdsourcing for generating and selecting ideas for ict innovation in a city context," *Journal of theoretical and applied electronic commerce research*, vol. 7, no. 3, pp. 49–62, 2012.

[131] C. Cen, S.-F. Cheng, H. C. Lau, and A. Misra, "Towards city-scale mobile crowdsourcing: Task recommendations under trajectory uncertainties," 2015.

[132] T. Breetzke and S. V. Flowerday, "The usability of IVRs for smart city crowdsourcing in developing cities," *The Electronic Journal of Information Systems in Developing Countries*, vol. 73, 2016.

[133] G. Cardone, L. Foschini, P. Bellavista, A. Corradi, C. Borcea, M. Talasila, and R. Curtmola, "Fostering participaction in smart cities: a geo-social crowdsensing platform," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 112–119, 2013.

[134] S. Mirri, C. Prandi, P. Salomoni, F. Callegati, and A. Campi, "On combining crowdsourcing, sensing and open data for an accessible smart city," in *2014 Eighth International Conference on Next Generation Mobile Apps, Services and Technologies*, Sept 2014, pp. 294–299.

[135] A. Orsino, G. Araniti, L. Militano, J. Alonso-Zarate, A. Molinaro, and A. Iera, "Energy efficient IoT data collection in smart cities exploiting D2D communications," *Sensors*, vol. 16, no. 6, p. 836, 2016.

[136] C. Beard, "High reliability 4G and 5G cellular wireless services for smart cities," 2015, (Accessed on December 2016). [Online]. Available: http://sce2.umkc.edu/csee/beardc/Beard_2015_Smart_Cities_Final.pdf

[137] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5g cellular networks: challenges, solutions, and future directions," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, 2014.

[138] C. K. Toh, *Ad hoc mobile wireless networks: protocols and systems*. Pearson Education, 2001.

[139] H. Chen, X. Jia, and H. Li, "A brief introduction to IoT gateway," in *IET International Conference on Communication Technology and Application*, 2011, pp. 610–613.

[140] Waze, "Get the best route, every day, with realtime help from other drivers." (Accessed on April 2017). [Online]. Available: https://www.waze.com/

[141] Global mobile Suppliers Association, "The road to 5G: Drivers, applications, requirements and technical development," 2015, (Accessed on December 2016). [Online]. Available: http://www.huawei.com/minisite/5g/img/GSA_the_Road_to_5G.pdf

[142] X. Lin, J. G. Andrews, A. Ghosh, and R. Ratasuk, "An overview of 3gpp device-to-device proximity services," *IEEE Communications Magazine*, vol. 52, no. 4, pp. 40–48, 2014.

[143] "Release 12." [Online]. Available: http://www.3gpp.org/specifications/releases/68-release-12

[144] P. Hu, P. Zhang, and D. Ganesan, "Laissez-faire: Fully asymmetric backscatter communication," in *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, 2015, pp. 255–267.

[145] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013.

[146] S. Shao, A. Khreishah, and H. Elgala, "Pixelated vlc-backscattering for self-charging indoor IoT devices," *IEEE Photonics Technology Letters*, 2016.

[147] Wikipedia, "Machine learning," (Accessed on October 2016). [Online]. Available: https://en.wikipedia.org/wiki/Machine_learning

[148] T. M. Mitchell, *Machine learning*. McGraw-Hill, 1997.

[149] R. S. Sutton and A. G. Barto, *Introduction to reinforcement learning*. MIT Press Cambridge, 1998, vol. 135.

[150] F. Sebastiani, "Machine learning in automated text categorization," *ACM computing surveys (CSUR)*, vol. 34, no. 1, pp. 1–47, 2002.

[151] S. B. Kotsiantis, I. Zaharakis, and P. Pintelas, "Supervised machine learning: A review of classification techniques," 2007.

[152] L. P. Kaelbling, M. L. Littman, and A. W. Moore, "Reinforcement learning: A survey," *Journal of artificial intelligence research*, vol. 4, pp. 237–285, 1996.

[153] J. Brownlee, "A tour of machine learning algorithms," 2013, (Accessed on September 2016). [Online]. Available: http://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/

[154] X. Zhu, "Semi-supervised learning literature survey," 2005, (Accessed on October 2016). [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.9681&rep=rep1&type=pdf

[155] R. Caruana and A. Niculescu-Mizil, "An empirical comparison of supervised learning algorithms," in *Proceedings of the 23rd international conference on Machine learning*. ACM, 2006, pp. 161–168.

[156] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2015.

[157] D. W. Aha, D. Kibler, and M. K. Albert, "Instance-based learning algorithms," *Machine learning*, vol. 6, no. 1, pp. 37–66, 1991.

[158] A. P. Bradley, "The use of the area under the roc curve in the evaluation of machine learning algorithms," *Pattern recognition*, vol. 30, no. 7, pp. 1145–1159, 1997.

[159] T. G. Dietterich, "Ensemble methods in machine learning," in *International workshop on multiple classifier systems*. Springer, 2000, pp. 1–15.

[160] Amazon, "Amazon machine learning," (Accessed on October 2016). [Online]. Available: https://aws.amazon.com/machine-learning/

[161] Microsoft, "Introduction to machine learning in the cloud," (Accessed on October 2016). [Online]. Available: https://docs.microsoft.com/en-us/azure/machine-learning/machine-learning-what-is-machine-learning

[162] Google, "Prediction api," (Accessed on October 2016). [Online]. Available: https://cloud.google.com/prediction/

[163] BigML, "BigML API documentation," (Accessed on October 2016). [Online]. Available: https://bigml.com/api

[164] D. Ferrucci, E. Brown, J. Chu-Carroll, J. Fan, D. Gondek, A. A. Kalyanpur, A. Lally, J. W. Murdock, E. Nyberg, J. Prager *et al.*, "Building watson: An overview of the deepQA project," *AI magazine*, vol. 31, no. 3, pp. 59–79, 2010.

[165] M. Batty, K. W. Axhausen, F. Giannotti, A. Pozdnoukhov, A. Bazzani, M. Wachowicz, G. Ouzounis, and Y. Portugali, "Smart cities of the future," *The European Physical Journal Special Topics*, vol. 214, no. 1, pp. 481–518, 2012.

[166] C. Rudin, D. Waltz, R. N. Anderson, A. Boulanger, A. Salleb-Aouissi, M. Chow, H. Dutta, P. N. Gross, B. Huang, S. Ierome *et al.*, "Machine learning for the new york city power grid," *IEEE transactions on pattern analysis and machine intelligence*, vol. 34, no. 2, pp. 328–345, 2012.

[167] S. Krishnan and T. Balasubramanian, "Traffic flow optimization and vehicle safety in smart cities," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 5, 2016.

[168] . F. Ertugrul and Y. Kaya, "Smart city planning by estimating energy efficiency of buildings by extreme learning machine," in *2016 4th International Istanbul Smart Grid Congress and Fair (ICSG)*, April 2016, pp. 1–5.

[169] I. Parvez, A. I. Sarwat, L. Wei, and A. Sundararajan, "Securing metering infrastructure of smart grid: A machine learning and localization based key management approach," *Energies*, vol. 9, no. 9, p. 691, 2016.

[170] L. Valerio, A. Passarella, and M. Conti, "Hypothesis transfer learning for efficient data computing in smart cities environments," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, May 2016, pp. 1–8.

[171] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00, New York, NY, USA, 2000, pp. 56–67. [Online]. Available: http://doi.acm.org/10.1145/345910.345920

[172] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, Jan 2000, pp. 10 pp. vol.2–.

[173] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE personal communications*, vol. 7, no. 5, pp. 16–27, 2000.

[174] C. Chien, I. Elgorriaga, and C. McConaghy, "Low-power direct-sequence spread-spectrum modem architecture for distributed wireless sensor networks," in *International Symposium on Low Power Electronics and Design*, 2001, pp. 251–254.

[175] A. Sinha and A. Chandrakasan, "Dynamic power management in wireless sensor networks," *IEEE Design & Test of Computers*, vol. 18, no. 2, pp. 62–74, 2001.

[176] H. Shu and Q. Liang, "Fuzzy optimization for distributed sensor deployment," in *IEEE Wireless Communications and Networking Conference*, vol. 3, March 2005, pp. 1903–1908 Vol. 3.

[177] A. Krause, C. Guestrin, A. Gupta, and J. Kleinberg, "Near-optimal sensor placements: Maximizing information while minimizing communication cost," in *Proceedings of the 5th International Conference on Information Processing in Sensor Networks*, ser. IPSN '06. New York, NY, USA: ACM, 2006, pp. 2–10. [Online]. Available: http://doi.acm.org/10.1145/1127777.1127782

[178] A. G. Dharne, J. Lee, and S. Jayasuriya, "Using fuzzy logic for localization in mobile sensor networks: simulations and experiments," in *2006 American Control Conference*, June 2006, pp. 6 pp.–.

[179] V. Tam, K. y. Cheng, and K. s. Lui, "A descend-based evolutionary approach to enhance position estimation in wireless sensor networks," in *2006 18th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'06)*, Nov 2006, pp. 568–574.

[180] W. van Norden, J. de Jong, F. Bolderheij, and L. Rothkrantz, "Intelligent task scheduling in sensor networks," in *2005 7th International Conference on Information Fusion*, vol. 2, July, pp. 8 pp.–.

[181] M. C. Foo, H. B. Lim, Y. Zeng, V. T. Lam, R. Teo, and G. W. Ng, "Impact of distributed resource allocation in sensor networks," in *2005 International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Dec, pp. 69–74.

[182] H. B. Lim, M. C. Foo, Y. Zeng *et al.*, "An adaptive distributed resource allocation scheme for sensor networks," in *International Conference on Mobile Ad-Hoc and Sensor Networks*. Springer, 2006, pp. 770–781.

[183] A. Kulakov and D. Davcev, "Intelligent data acquisition and processing using wavelet neural-networks," in *2005 IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Sept 2005, pp. 491–494.

[184] ——, "Distributed data processing in wireless sensor networks based on artificial neural-networks algorithms," in *10th IEEE Symposium on Computers and Communications (ISCC'05)*, June, pp. 353–358.

[185] Z. J. Yu, S. L. Dong, J. M. Wei, T. Xing, and H. T. Liu, "Neural network aided unscented kalman filter for maneuvering target tracking in distributed acoustic sensor networks," in *Computing: Theory and Applications, 2007. ICCTA '07. International Conference on*, March 2007, pp. 245–249.

[186] J. Lim, J. Lee, S. Hong, and P. Park, "Algorithm for detection with localization of multi-targets in wireless acoustic sensor networks," in *2006 18th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'06)*, Nov 2006, pp. 547–554.

[187] G. Mazarakis and J. Avaritsiotis, "Lightweight time encoded signal processing for vehicle recognition in sensor networks," in *2006 Ph.D. Research in Microelectronics and Electronics*, 2006, pp. 497–500.

[188] J. H. Hong, N. J. Kim, E. J. Cha, and T. S. Lee, "Classification technique of human motion context based on wireless sensor network," in *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, Jan 2005, pp. 5201–5202.

[189] F. Cadger, K. Curran, J. Santos, and S. Moffett, "Manet location prediction using machine learning algorithms," in *International Conference on Wired/Wireless Internet Communications*. Springer, 2012, pp. 174–185.

[190] L. Ghouti, T. R. Sheltami, and K. S. Alutaibi, "Mobility prediction in mobile ad hoc networks using extreme learning machines," *Procedia Computer Science*, vol. 19, pp. 305–312, 2013.

[191] H. Eom, P. S. Juste, R. Figueiredo, O. Tickoo, R. Illikkal, and R. Iyer, "Machine learning-based runtime scheduler for mobile offloading framework," in *2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing*, Dec 2013, pp. 17–25.

[192] B. Xu, O. Wolfson, and C. Naiman, "Machine learning in disruption-tolerant manets," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 4, no. 4, p. 23, 2009.

[193] R. Akbani, T. Korkmaz, and G. Raju, "Emltrust: an enhanced machine learning based reputation system for manets," *Ad Hoc Networks*, vol. 10, no. 3, pp. 435–457, 2012.

[194] M. Patel and S. Sharma, "Detection of malicious attack in manet a behavioral approach," in *2013 3rd IEEE International Advance Computing Conference (IACC)*, Feb 2013, pp. 388–393.

[195] B. Russell, M. L. Littman, and W. Trappe, "Integrating machine learning in ad hoc routing: A wireless adaptive routing protocol," *International Journal of Communication Systems*, vol. 24, no. 7, pp. 950–966, 2011.

[196] P. Szczurek, B. Xu, J. Lin, and O. Wolfson, "Machine learning approach to report prioritization with an application to travel time dissemination," in *Proceedings of the Second International Workshop on Computational Transportation Science*, ser. IWCTS '09, New York, NY, USA, 2009, pp. 31–36. [Online]. Available: http://doi.acm.org/10.1145/1645373.1645379

[197] T. Zhong, B. Xu, P. Szczurek, and O. Wolfson, "Trafficinfo: An algorithm for vanet dissemination of real-time traffic information," in *5th World congress on Intelligent Transport Systems*. Citeseer, 2008.

[198] P. Szczurek, B. Xu, O. Wolfson, J. Lin, and N. Rishe, "Prioritizing travel time reports in peer-to-peer traffic dissemination," in *2010 7th International Symposium on Communication Systems, Networks Digital Signal Processing (CSNDSP 2010)*, July 2010, pp. 454–458.

[199] C.-J. Huang, Y.-T. Chuang, Y.-J. Chen, Y.-C. Luo, and D.-X. Yang, "Constructing alternative routes for VANET using machine learning techniques," in *international Conference on Advanced Information Technologies*, 2007.

[200] M. Slavik and I. Mahgoub, "Applying machine learning to the design of multi-hop broadcast protocols for VANET," in *2011 7th International Wireless Communications and Mobile Computing Conference*, July 2011, pp. 1742–1747.

[201] J. Kim, "Modeling vehicular traffic shock wave with machine learning approaches," 2016, (Accessed on November 2016). [Online]. Available: http://escholarship.org/uc/item/9vd6v7h7

[202] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in

VANET," in *International Conference on Advances in Computing and Communications*. Springer, 2011, pp. 644–653.

[203] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (dmn) in vehicular ad-hoc networks," *Procedia Computer Science*, vol. 46, pp. 965–972, 2015.

[204] P. Szczurek, B. Xu, O. Wolfson, and J. Lin, "A methodology for the development of novel vanet safety applications," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, 2012, pp. 119–122.

[205] N. Dogru and A. Subasi, "Traffic accident detection by using machine learning methods," in *Third International Symposium on Sustainable Development (ISSD12)*, 2012, p. 467.

[206] A. Cherian, J. Andersh, V. Morellas, N. Papanikolopoulos, and B. Mettler, "Autonomous altitude estimation of a UAV using a single onboard camera," in *2009 IEEE/RSJ International Conference on Intelligent Robots and Systems*, Oct 2009, pp. 3900–3905.

[207] A. Faust, I. Palunko, P. Cruz, R. Fierro, and L. Tapia, "Learning swing-free trajectories for UAVs with a suspended load," in *2013 IEEE International Conference on Robotics and Automation*, May 2013, pp. 4902–4909.

[208] C. De Crousaz, F. Farshidian, and J. Buchli, "Aggressive optimal control for agile flight with a slung load," in *IROS Workshop on Machine Learning in Planning and Control of Robot Motion*. Citeseer, 2014.

[209] A. Faust, I. Palunko, P. Cruz, R. Fierro, and L. Tapia, "Automated aerial suspended cargo delivery through reinforcement learning," *Artificial Intelligence*, 2014.

[210] E. L. Hayes, "Machine learning for intelligent control: Application of reinforcement learning techniques to the development of flight control systems for miniature uav rotorcraft," *Master Thesis, University of Canterbury. Department of Mechanical Engineering*, 2013.

[211] F. Ofli, P. Meier, M. Imran, C. Castillo, D. Tuia, N. Rey, J. Briant, P. Millet, F. Reinhard, M. Parkan *et al.*, "Combining human computing and machine learning to make sense of big (aerial) data for disaster response," *Big Data*, vol. 4, no. 1, pp. 47–59, 2016.

[212] R. Wang, D. Zou, L. Pei, P. Liu, and C. Xu, "Velocity prediction for multi-rotor UAVs based on machine learning," in *China Satellite Navigation Conference Proceedings: Volume II*. Springer, 2016, pp. 487–500.

[213] K. Nahrstedt, D. Lopresti, B. Zorn, A. W. Drobnis, B. Mynatt, S. Patel, and H. V. Wright, "Smart communities internet of things," *arXiv preprint arXiv:1604.02028*, 2016.

[214] N. Zhang, H. Chen, X. Chen, and J. Chen, "Semantic framework of internet of things for smart cities: Case studies," *Sensors*, vol. 16, no. 9, p. 1501, 2016.

[215] P. Vijai and P. B. Sivakumar, "Design of IoT systems and analytics in the context of smart city initiatives in india," *Procedia Computer Science*, vol. 92, pp. 583–588, 2016.

[216] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the internet of things using big data analytics," *Computer Networks*, vol. 101, pp. 63–80, 2016.

[217] J. Hoffert, D. Mack, and D. Schmidt, "Integrating machine learning techniques to adapt protocols for qos-enabled distributed real-time and embedded publish/subscribe middleware," *Network Protocols and Algorithms*, vol. 2, no. 3, pp. 37–69, 2010.

[218] I. Katakis, G. Tsoumakas, E. Banos, N. Bassiliades, and I. Vlahavas, "An adaptive personalized news dissemination system," *Journal of Intelligent Information Systems*, vol. 32, no. 2, pp. 191–212, 2009.

[219] G. Amati and F. Crestani, "Probabilistic learning for selective dissemination of information," *Information processing & management*, vol. 35, no. 5, pp. 633–654, 1999.

[220] M. Altınel and M. J. Franklin, "Efficient filtering of xml documents for selective dissemination of information," in *Proc. of the 26th Intl Conference on Very Large Data Bases (VLDB), Cairo, Egypt*, 2000.

[221] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[222] Y. Bengio, A. Courville, and P. Vincent, "Representation learning: A review and new perspectives," *IEEE transactions on pattern analysis and machine intelligence*, vol. 35, no. 8, pp. 1798–1828, 2013.

[223] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: Continual prediction with lstm," *Neural computation*, vol. 12, no. 10, pp. 2451–2471, 2000.

[224] M. Tan, C. d. Santos, B. Xiang, and B. Zhou, "Lstm-based deep learning models for non-factoid answer selection," *arXiv preprint arXiv:1511.04108*, 2015.

[225] F. Bastien, P. Lamblin, R. Pascanu, J. Bergstra, I. Goodfellow, A. Bergeron, N. Bouchard, D. Warde-Farley, and Y. Bengio, "Theano: new features and speed improvements," *arXiv preprint arXiv:1211.5590*, 2012.

[226] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin *et al.*, "Tensorflow: Large-scale machine learning on heterogeneous distributed systems," *arXiv preprint arXiv:1603.04467*, 2016.

[227] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, "Caffe: Convolutional architecture for fast feature embedding," in *Proceedings of the 22nd ACM international conference on Multimedia*, 2014, pp. 675–678.

[228] R. Collobert, K. Kavukcuoglu, and C. Farabet, "Torch7: A matlab-like environment for machine learning," in *BigLearn, NIPS Workshop*, no. EPFL-CONF-192376, 2011.

[229] G. Han and K. Sohn, "Clustering the seoul metropolitan area by travel patterns based on a deep belief network," in *2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC)*, March 2016, pp. 1–6.

[230] Z. Y. Wu, M. El-Maghraby, and S. Pathak, "Applications of deep learning for smart water networks," *Procedia Engineering*, vol. 119, pp. 479–485, 2015.

[231] M. A. Alsheikh, D. Niyato, S. Lin, H.-P. Tan, and Z. Han, "Mobile big data analytics using deep learning and apache spark," *IEEE Network*, vol. 30, no. 3, pp. 22–29, 2016.

[232] A. Dedinec, S. Filiposka, A. Dedinec, and L. Kocarev, "Deep belief network based electricity load forecasting: An analysis of macedonian case," *Energy*, vol. 115, pp. 1688–1700, 2016.

[233] X. He, T. Huang, C. Li, H. Che, and Z. Dong, "A recurrent neural network for optimal real-time price in smart grid," *Neurocomputing*, vol. 149, pp. 608–612, 2015.

[234] J. Aryal and R. Dutta, "Smart city and geospatiality: Hobart deeply learned," in *2015 31st IEEE International Conference on Data Engineering Workshops*, April 2015, pp. 108–109.

[235] Y. Tian and L. Pan, "Predicting short-term traffic flow by long short-term memory recurrent neural network," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, Dec 2015, pp. 153–158.

[236] X. Niu, Y. Zhu, Q. Cao, X. Zhang, W. Xie, and K. Zheng, "An online-traffic-prediction based route finding mechanism for smart city," *International Journal of Distributed Sensor Networks*, vol. 2015, p. 18, 2015.

[237] V. C. Liang, R. T. B. Ma, W. S. Ng, L. Wang, M. Winslett, H. Wu, S. Ying, and Z. Zhang, "Mercury: Metro density prediction with recurrent neural network on streaming CDR data," in *2016 IEEE 32nd International Conference on Data Engineering (ICDE)*, May 2016, pp. 1374–1377.

[238] N. Ouerhani, N. Pazos, M. Aeberli, J. Senn, and S. Gobron, "Dynamic street light management," (Accessed on November 2016). [Online]. Available: http://www.stephane-gobron.net/Core/Publications/Papers/2015_HCC15.pdf

[239] V. Garcia-Font, C. Garrigues, and H. Rifà-Pous, "A comparative study of anomaly detection techniques for smart city wireless sensor networks," *Sensors*, vol. 16, no. 6, p. 868, 2016.

[240] A. Fleury, M. Vacher, and N. Noury, "Svm-based multimodal classification of activities of daily living in health smart homes: sensors, algorithms, and first experimental results," *IEEE trans-*

actions on information technology in biomedicine, vol. 14, no. 2, pp. 274–283, 2010.

[241] B. Longstaff, S. Reddy, and D. Estrin, "Improving activity classification for health applications on mobile devices using active and semi-supervised learning," in *2010 4th International Conference on Pervasive Computing Technologies for Healthcare*, March 2010, pp. 1–7.

[242] H. Fang and C. Hu, "Recognizing human activity in smart home using deep learning algorithm," in *Proceedings of the 33rd Chinese Control Conference*, July 2014, pp. 4716–4720.

[243] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[244] P. Flajolet, É. Fusy, O. Gandouet, and F. Meunier, "Hyperloglog: the analysis of a near-optimal cardinality estimation algorithm," *DMTCS Proceedings*, no. 1, 2008.

[245] A. Z. Broder, "On the resemblance and containment of documents," in *Proceedings. Compression and Complexity of SEQUENCES 1997 (Cat. No.97TB100171)*, Jun 1997, pp. 21–29.

[246] Wikipedia, "Jaccard index," (Accessed on November 2016). [Online]. Available: https://en.wikipedia.org/wiki/Jaccard_index

[247] J. M. Phillips, "Minhashing," (Accessed on November 2016). [Online]. Available: https://www.cs.utah.edu/ jeffp/teaching/cs5955/L5-Minhash.pdf

[248] Apache, "Apache storm," (Accessed on November 2016). [Online]. Available: http://storm.apache.org/

[249] ——, "Apache spark," (Accessed on November 2016). [Online]. Available: http://spark.apache.org/

[250] J. Kreps, N. Narkhede, J. Rao *et al.*, "Kafka: A distributed messaging system for log processing," in *Proceedings of the NetDB*, 2011, pp. 1–7.

[251] A. Videla and J. J. W. Williams, *RabbitMQ in Action: Distributed Messaging for Everyone*. Manning Publications, 2012.

[252] Eclipse, "Mosquitto: An open source mqtt v3.1/v3.1.1 broker," (Accessed on December 2016). [Online]. Available: https://mosquitto.org/

[253] T. Buddhika and S. Pallickara, "Neptune: Real time stream processing for internet of things and sensing environments," (Accessed on November 2016). [Online]. Available: http://granules.cs.colostate.edu/papers/Neptune-IPDPS-2016.pdf

[254] C. Yin, Z. Xiong, H. Chen, J. Wang, D. Cooper, and B. David, "A literature survey on smart cities," *Science China Information Sciences*, vol. 58, no. 10, pp. 1–18, 2015.

[255] J. M. Schleicher, M. Vgler, S. Dustdar, and C. Inzinger, "Enabling a smart city application ecosystem: Requirements and architectural aspects," *IEEE Internet Computing*, vol. 20, no. 2, pp. 58–65, Mar 2016.

[256] J. A. C. Soto, O. Werner-Kytola, M. Jahn, J. Pullmann, D. Bonino, C. Pastrone, and M. Spirito, "Towards a federation of smart city services," 2016.

[257] RTInsights Team, "Population mapping with real-time mobile phone data," (Accessed on December 2016). [Online]. Available: https://www.rtinsights.com/dynamic-population-mapping-mobile-phone-data-lightbend/

[258] I. Herman, G. Melançon, and M. S. Marshall, "Graph visualization and navigation in information visualization: A survey," *IEEE Transactions on visualization and computer graphics*, vol. 6, no. 1, pp. 24–43, 2000.

[259] Z. Xiong, W. Luo, L. Chen, and L. M. Ni, "Data vitalization: a new paradigm for large-scale dataset analysis," in *16th International Conference on Parallel and Distributed Systems*. IEEE, 2010, pp. 251–258.

[260] Z. Xiong, Y. Zheng, and C. Li, "Data vitalization's perspective towards smart city: A reference model for data service oriented architecture," in *2014 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, May 2014, pp. 865–874.

[261] N. Ferreira, J. Poco, H. T. Vo, J. Freire, and C. T. Silva, "Visual exploration of big spatio-temporal urban data: A study of new york city taxi trips," *IEEE Transactions on Visualization and Computer Graphics*, vol. 19, no. 12, pp. 2149–2158, 2013.

[262] A. Anwar, T. Nagel, and C. Ratti, "Traffic origins: A simple visualization technique to support traffic incident analysis," in *2014 IEEE Pacific Visualization Symposium*, March, pp. 316–319.

[263] R. Wenge, X. Zhang, C. Dave, L. Chao, and S. Hao, "Smart city architecture: A technology guide for implementation and design challenges," *China Communications*, vol. 11, no. 3, pp. 56–69, 2014.

[264] L. Mei, X. Cai, H. Zhang, C. Hu, and L. Qi, "Video structured descriptionvitalization techniques for the surveillance video data," in *Advances on Digital Television and Wireless Multimedia Communications*. Springer, 2012, pp. 219–227.

[265] A. Tropea, "189 - accelerating processes towards smart cities involving private companies at local and national level," (Accessed on December 2016). [Online]. Available: https://eu-smartcities.eu/commitment/189

[266] S. Biswas and R. Morris, "Exor: opportunistic multi-hop routing for wireless networks," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4, pp. 133–144, 2005.

[267] V. Palma and A. M. Vegni, "On the optimal design of a broadcast data dissemination system over VANET providing V2V and V2I communications" the vision of Rome as a Smart City"," *Journal of telecommunications and information technology*, pp. 41–48, 2013.

[268] M. Bonola, L. Bracciale, P. Loreti, R. Amici, A. Rabuffi, and G. Bianchi, "Opportunistic communication in smart city: Experimental insight with small-scale taxi fleets as data carriers," *Ad Hoc Networks*, vol. 43, pp. 43–55, 2016.

[269] V.-D. Le, H. Scholten, and P. Havinga, "Unified routing for data dissemination in smart city networks," in *2012 3rd IEEE International Conference on the Internet of Things*, Oct 2012, pp. 175–182.

[270] D. Reina, R. Ciobanu, S. Toral, and C. Dobre, "A multi-objective optimization of data dissemination in delay tolerant networks," *Expert Systems with Applications*, vol. 57, pp. 178–191, 2016.

[271] A. Gorrieri, "Efficient multi-hop broadcast data dissemination for IoT and smart cities applications," in *Proceedings of the 2015 on MobiSys PhD Forum*, ser. PhDForum '15, New York, NY, USA, 2015, pp. 19–20. [Online]. Available: http://doi.acm.org/10.1145/2752746.2752788

[272] D. Wu, D. I. Arkhipov, M. Kim, C. L. Talcott, A. C. Regan, J. A. McCann, and N. Venkatasubramanian, "Addsen: Adaptive data processing and dissemination for drone swarms in urban sensing," *IEEE Transactions on Computers*, 2016.

[273] A. Morelli, C. Stefanelli, M. Tortonesi, and N. Suri, "Mobility pattern prediction to support opportunistic networking in smart cities," in *2013 International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, Nov 2013, pp. 166–175.

[274] M. Sneps-Sneppe and D. Namiot, "On mobile cloud for smart city applications," *arXiv preprint arXiv:1605.02886*, 2016.

[275] J. Hoffert, A. Gokhale, and D. C. Schmidt, "Timely autonomic adaptation of publish/subscribe middleware in dynamic environments," in *Innovations and Approaches for Resilient and Adaptive Systems*. IGI Global, 2013, ch. 10.

[276] L. Cajueiro, S. Neto, F. Ferraz, and A. Cavalvanti, "Towards an open smart city notification service," in *The Eleventh International Conference on Software Engineering Advances*, 2016.

[277] S. C. de Alvarenga, B. B. Zarpelão, and V. N. Soares, "A notification architecture for smart cities based on push technologies," in *2014 XL Latin American Computing Conference (CLEI)*, Sept 2014, pp. 1–8.

[278] City of Louisville, "Imagine louisville application for participation in beyond traffic: The smart city challenge," (Accessed on December 2016). [Online]. Available: https://louisvilleky.gov/sites/default/files/advanced_planning/louisville_smart_city_proposal_final_lr_2.pdf

[279] D. Rusu and S. Vert, "City alerts: smart city notification platform based on public open data," *Sci. Bull. Politech. Univ. Timis. Trans. Electron. Commun*, vol. 59, pp. 21–26, 2014.

[280] T. P. Lauriault, "Working paper 3: Republic of ireland's open data strategy: Observations and recommendations," 2014, (Accessed on December 2016). [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508016

[281] B. Tian, K. M. Hou, and H. Zhou, "The traffic adaptive data dissemination (trad) protocol for both urban and highway scenarios," *Sensors*, vol. 16, no. 6, p. 920, 2016.

[282] W. Islam and R. Palit, "Performance evaluation of EAEP and DV-CAST broadcasting protocols in VANET," in *Vehicular Adhoc Networks for Smart Cities*. Springer, 2015, pp. 65–74.

[283] A. Olaru, A. M. Florea, and A. El Fallah Seghrouchni, "Using context-aware multi-agent systems for robust smart city infrastructure," *Enablers for Smart Cities*, pp. 187–206, 2016.

[284] N. Bessis and C. Dobre, *Big data and internet of things: a roadmap for smart environments*. Springer, 2014.

[285] F. Lupi, V. Palma, and A. M. Vegni, "Performance evaluation of broadcast data dissemination over vanets," *Department of Applied Electronics, University of Roma Tre, Rome, Italy*, 2012.

[286] W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y.-Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 787–795, 2011.

[287] J. Hahner, C. Becker, and K. Rothermel, "A protocol for data dissemination in frequently partitioned mobile ad hoc networks," in *Proceedings of the Eighth IEEE Symposium on Computers and Communications. ISCC 2003*, June 2003, pp. 633–640 vol.1.

[288] The Supreme Legislation Committee in the Emirate of Dubai, "Regulating data dissemination and exchange in the emirate of Dubai," 2016, (Accessed on December 2016). [Online]. Available: http://ogp.dubai.gov.ae/documants/pdf/ltiwndiymjezmdk.pdf

[289] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[290] J. J. Zhao, S. Y. Zhao, and S. Y. Zhao, "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly*, vol. 27, no. 1, pp. 49 – 56, 2010.

[291] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security and Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[292] K. Shuaib, I. Khalil, and M. Abdel-Hafez, "Communications in smart grid: A review with performance, reliability and security consideration." *JNW*, vol. 8, no. 6, pp. 1229–1240, 2013.

[293] Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[294] B. Miller and D. Rowe, "A survey scada of and critical infrastructure incidents," in *Proceedings of the 1st Annual Conference on Research in Information Technology*, ser. RIIT '12. New York, NY, USA: ACM, 2012, pp. 51–56.

[295] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Commun. ACM*, vol. 56, no. 1, pp. 94–103, Jan. 2013. [Online]. Available: http://doi.acm.org.libproxy.library.wmich.edu/10.1145/2398356.2398377

[296] S. M. Amin, "For the good of the grid," *IEEE Power and Energy Magazine*, vol. 6, no. 6, pp. 48–59, 2008.

[297] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[298] B. A. Hamilton, J. Miller, and B. Renz, "Understanding the Benefits of the Smart Grid," National Energy Technology Laboratory, U.S. Department of Energy, Tech. Rep., 2010.

[299] NIST, "Framework and Roadmap for Smart Grid Interoperability Standards," Smart Grid and Cyber-Physical Systems Program Office and Energy and Environment Division, Engineering Laboratory, National Institute of Technology, U.S. Dept. of Commerce, Tech. Rep., 2014.

[300] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," *Computer Networks*, vol. 56, no. 11, pp. 2741–2771, 2012.

[301] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498 – 506, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404806000514

[302] A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Halderman *et al.*, "An internet-wide view of ics devices," in *14th IEEE Privacy, Security, and Trust Conference (PST16)*, 2016.

[303] D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. A. Beyah, "Who's in control of your control system? device fingerprinting for cyber-physical systems," in *NDSS*, 2016.

[304] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 55:1–55:29, Mar. 2014. [Online]. Available: http://doi.acm.org/10.1145/2542049

[305] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 252–260, March 2016.

[306] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Aug 2015, pp. 1–8.

[307] T. Cruz, J. Barrigas, J. Proena, A. Graziano, S. Panzieri, L. Lev, and P. Simes, "Improving network security monitoring for industrial control systems," in *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 878–881.

[308] W. H. Organization, *Global status report on road safety 2015*. World Health Organization, 2015.

[309] T. A. Litman, "Smart congestion relief: Comprehensive evaluation of traffic congestion costs and congestion reduction strategies," November 2016, (Accessed on December 2016). [Online]. Available: http://www.vtpi.org/cong_relief.pdf

[310] U.S. Department Of Transportation, "National intelligent transportations systems architecture," Tech. Rep., 2012. [Online]. Available: http://local.iteris.com/itsarch/index.htm

[311] F. Kargl, "Vehicular communications and VANETs," in *Talks 23rd Chaos Communication Congress*, 2006.

[312] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.

[313] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[314] C. Laurendeau and M. Barbeau, "Threats to security in dsrc/wave," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2006, pp. 266–279.

[315] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[316] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *INFOCOM*, 2010, pp. 1–9.

[317] P. Vinoth Kumar and M. Maheshwari, "Prevention of sybil attack and priority batch verification in VANETs," in *Proceedings of the International Conference on Information Communication and Embedded Systems, Chennal, India*, vol. 2728, 2014, p. 15.

[318] S. Ö. Tengstrand, K. Fors, P. Stenumgaard, and K. Wiklundh, "Jamming and interference vulnerability of ieee 802.11 p," in *International Symposium on Electromagnetic Compatibility*. IEEE, 2014, pp. 533–538.

[319] S. Najafzadeh, N. Ithnin, S. A. Razak, and R. Karimi, "Bsm: broadcasting of safety messages in vehicular ad hoc networks,"

Arabian Journal for Science and Engineering, vol. 39, no. 2, pp. 777–782, 2014.

[320] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[321] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 636–654.

[322] "Vault7 - Home," 2017. [Online]. Available: https://wikileaks.org/ciav7p1/index.html

[323] D. J. Wu, A. Taly, A. Shankar, and D. Boneh, "Privacy, discovery, and authentication for the internet of things," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 301–319.

[324] J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET communications*, vol. 4, no. 7, pp. 894–903, 2010.

[325] K. N. Qureshi and A. H. Abdullah, "A survey on intelligent transportation systems," *Middle-East Journal of Scientific Research*, vol. 15, no. 5, pp. 629–642, 2013.

[326] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1 – 13, 2014.

[327] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," *International Journal of Computer Science and Network*, vol. 2, no. 1, 2013.

[328] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for VANET by using digital certification to provide security with low bandwidth," in *2014 International Conference on Communication and Signal Processing*, April 2014, pp. 768–772.

[329] M. Rahbari and M. A. J. Jamali, "Efficient detection of sybil attack based on cryptography in VANET," *arXiv preprint arXiv:1112.2257*, 2011.

[330] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2012.

[331] M. Strasser, C. Ppper, S. Capkun, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Symposium on Security and Privacy*, 2008, pp. 64–78.

[332] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *INFOCOM*, 2011, pp. 1871–1879.

[333] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management - part 1: General (revised," in *NIST Special Publication*, 2006.

[334] B. N. Levine, M. K. Reiter, C. Wang, and M. Wright, "Timing attacks in low-latency mix systems," in *International Conference on Financial Cryptography*. Springer, 2004, pp. 251–265.

[335] A. A. Mbacke, N. Mitton, and H. Rivano, "Rfid reader anticollision protocols for dense and mobile deployments," *Electronics*, vol. 5, no. 4, 2016.

[336] J. Großschädl, "Tinysa: A security architecture for wireless sensor networks," in *Proceedings of the 2006 ACM CoNEXT conference*, 2006, p. 55.

[337] S. T. Patel and N. H. Mistry, "A survey: Lightweight cryptography in WSN," in *2015 International Conference on Communication Networks (ICCN)*, Nov, pp. 11–15.

[338] A. Swaminathan, "Secure routing methods for efficient data transmission for wireless sensor networks: A survey," in *Seventh International Conference on Dynamic Systems and Applications & Fifth International Conference on Neural, Parallel, and Scientific Computations*, 2015.

[339] R. K. Panta, S. Bagchi, and I. M. Khalil, "Efficient wireless reprogramming through reduced bandwidth usage and opportunistic sleeping," *Ad Hoc Networks*, vol. 7, no. 1, pp. 42–62, 2009.

[340] I. Khalil, "MCC: Mitigating colluding collision attacks in wireless sensor networks," in *2010 IEEE Global Telecommunications Conference*, Dec 2010, pp. 1–5.

[341] ——, "MIMI: Mitigating packet misrouting in locally-monitored multi-hop wireless ad hoc networks," in *2008 IEEE Global Telecommunications Conference*, Nov 2008, pp. 1–5.

[342] I. M. Khalil, A. Khreishah, F. Ahmed, and K. Shuaib, "Dependable wireless sensor networks for reliable and secure humanitarian relief applications," *Ad Hoc Networks*, vol. 13, pp. 94–106, 2014.

[343] I. Khalil, M. Awad, and A. Khreishah, "Ctac: Control traffic tunneling attacks countermeasures in mobile wireless networks," *Computer Networks*, vol. 56, no. 14, pp. 3300–3317, 2012.

[344] J. S. Warner and R. G. Johnston, "GPS spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[345] M. Alimohammadi and A. Pouyan, "Performance analysis of cryptography methods for secure message exchanging in VANET," *International Journal of Scientific & Engineering Research*, vol. 5, no. 2, p. 912, 2014.

[346] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[347] T. Morris, *Trusted Platform Module*. Boston, MA: Springer US, 2011, pp. 1332–1335. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-5906-5_796

[348] M. Swan, *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

[349] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[350] L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. Tygar, "Adversarial machine learning," in *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, 2011, pp. 43–58.

[351] P. McDaniel, N. Papernot, and Z. B. Celik, "Machine learning in adversarial settings," *IEEE Security & Privacy*, vol. 14, no. 3, pp. 68–72, 2016.

[352] S. Rhody and D. Dunn, "Government clouds," *Encyclopedia of Cloud Computing*, pp. 52–61, 2016.

[353] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan, pp. 812–813.

[354] A. Guerrero-Prez, A. Huerta, F. Gonzlez, and D. Lpez, "Network architecture based on virtualized networks for smart cities," IEEE-CCD Smart Cities White Paper, Tech. Rep., 2013.

[355] A. Manzalini and A. Stavdas, "The network is the robot," *Communications & Strategies*, no. 96, p. 73, 2014.

[356] G. Szabo and B. A. Huberman, "Predicting the popularity of online content," *ACM Communications Journal*, vol. 53, no. 8, pp. 80–88, 2010.

[357] S. Ouyang, C. Li, and X. Li, "A peek into the future: Predicting the popularity of online videos," *IEEE Access*, vol. 4, pp. 3026–3033, 2016.

[358] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 236–262, 2015.

[359] I. Mansour, R. Sahandi, K. Cooper, and A. Warman, "Interoperability in the heterogeneous cloud environment: A survey of recent user-centric approaches," in *Proceedings of the International Conference on Internet of things and Cloud Computing*. ACM, 2016, p. 62.

[360] J. M. Kang, H. Bannazadeh, H. Rahimi, T. Lin, M. Faraji, and A. Leon-Garcia, "Software-defined infrastructure and the future central office," in *2013 IEEE International Conference on Communications Workshops (ICC)*, June, pp. 225–229.

[361] C. Xu, F. Zhao, J. Guan, H. Zhang, and G.-M. Muntean, "Qoe-driven user-centric vod services in urban multihomed p2p-based vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2273–2289, 2013.

[362] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-defined networking for rsu clouds in support of the internet of

vehicles," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 133–144, 2015.

[363] M. Bagheri, M. Siekkinen, and J. K. Nurminen, "Cloud-based pedestrian road-safety with situation-adaptive energy-efficient communication," *IEEE Intelligent Transportation Systems Magazine*, vol. 8, no. 3, pp. 45–62, 2016.

[364] S. Ma, Y. Zheng, and O. Wolfson, "Real-time city-scale taxi ridesharing," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 7, pp. 1782–1795, 2015.

[365] M. Vögler, J. M. Schleicher, C. Inzinger, S. Dustdar, and R. Ranjan, "Migrating smart city applications to the cloud," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 72–79, 2016.

[366] H. Bannazadeh, A. Tizghadam, and A. Leon-Garcia, "Smart city platforms on multitier software-defined infrastructure cloud computing," in *2016 IEEE International Smart Cities Conference (ISC2)*, Sept 2016, pp. 1–6.

[367] T. Clohessy, T. Acton, and L. Morgan, "Smart city as a service (scaas): a future roadmap for e-government smart city cloud computing initiatives," in *Proceedings of the 7th International Conference on Utility and Cloud Computing*. IEEE Computer Society, 2014, pp. 836–841.

[368] Open Networking Foundation, "Openflow - open networking foundation," 2016, (Accessed on 5 November 2016). [Online]. Available: https://www.opennetworking.org/sdn-resources/OpenFlow

[369] Á. L. Valdivieso Caraguay, A. Benito Peral, L. I. Barona López, and L. J. García Villalba, "SDN: evolution and opportunities in the development IoT applications," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[370] N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, "Nox: towards an operating system for networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 3, pp. 105–110, 2008.

[371] "Project floodlight," 2016, (Accessed on December 2016). [Online]. Available: http://www.projectfloodlight.org/

[372] A. Voellmy and J. Wang, "Scalable software defined network controllers," in *Proceedings of SIGCOMM conference on Applications, technologies, architectures, and protocols for computer communication*, 2012, pp. 289–290.

[373] A. Guha, M. Reitblatt, and N. Foster, "Machine-verified network controllers," in *SIGPLAN Notices*, vol. 48, no. 6. ACM, 2013, pp. 483–494.

[374] A. Mckeown, H. Rashvand, T. Wilcox, and P. Thomas, "Priority SDN controlled integrated wireless and powerline wired for smart-home internet of things," in *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*, pp. 1825–1830.

[375] W. F. Elsadek and M. N. Mikhail, "Inter-domain mobility management using SDN for residential/enterprise real time services," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 43–50.

[376] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Computer Networks*, vol. 65, pp. 99–110, 2014.

[377] G. ETSI, "001,network functions virtualization (NFV): Use cases, 10-2013."

[378] M. Barcelo, A. Correa, J. Llorca, A. M. Tulino, J. L. Vicario, and A. Morell, "IoT-cloud service optimization in next generation smart environments," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 4077–4090, Dec 2016.

[379] A. Corici, R. Steinke, T. Magedanz, L. Coetzee, D. Oosthuizen, B. Mkhize, M. Catalan, J. C. Fontelles, J. Paradells, R. Shrestha, D. Nehls, and B. Riemer, "Towards programmable and scalable IoT infrastructures for smart cities," in *2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 1–6.

[380] A. Gember-Jacobson, R. Viswanathan, C. Prakash, R. Grandl, J. Khalid, S. Das, and A. Akella, "OpenNF: Enabling innovation in network function control," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 163–174, aug 2014. [Online]. Available: http://doi.acm.org/10.1145/2740070.2626313

[381] A. Gember, A. Krishnamurthy, S. S. John, R. Grandl, X. Gao, A. Anand, T. Benson, A. Akella, and V. Sekar, "Stratos: A network-aware orchestration layer for middleboxes in the cloud," *CoRR*, vol. abs/1305.0209, 2013. [Online]. Available: http://arxiv.org/abs/1305.0209

[382] Z. A. Qazi, C.-C. Tu, L. Chiang, R. Miao, V. Sekar, and M. Yu, "Simple-fying middlebox policy enforcement using SDN," *ACM SIGCOMM computer communication review*, vol. 43, no. 4, pp. 27–38, 2013.

[383] S. K. Fayazbakhsh, L. Chiang, V. Sekar, M. Yu, and J. C. Mogul, "Enforcing network-wide policies in the presence of dynamic middlebox actions using flowtags," in *11th USENIX Symposium on Networked Systems Design and Implementation*, 2014, pp. 543–546.

[384] P. Neves, R. Calé, M. R. Costa, C. Parada, B. Parreira, J. Alcaraz-Calero, Q. Wang, J. Nightingale, E. Chirivella-Perez, W. Jiang *et al.*, "The selfnet approach for autonomic management in an NFV/SDN networking paradigm," *International Journal of Distributed Sensor Networks*, vol. 2016, p. 2, 2016.

[385] E. Luengo, C. Weber, S. Shah Heydari, and K. El-Khatib, "Design and implementation of a software-defined integrated wired-wireless network testbed," in *Proceedings of the 13th ACM International Symposium on Mobility Management and Wireless Access*, ser. MobiWac '15, New York, NY, USA, 2015, pp. 47–52. [Online]. Available: http://doi.acm.org/10.1145/2810362.2826697

[386] F. Granelli, A. A. Gebremariam, M. Usman, F. Cugini, V. Stamati, M. Alitska, and P. Chatzimisios, "Software defined and virtualized wireless access in future wireless networks: scenarios and standards," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 26–34, 2015.

[387] 3GPP, "3rd generation partnership project: Technical speicification group services adn system aspects: Ip multimedia subsystem (ims)," 2006. [Online]. Available: http://www.3gpp.org/about-3gpp/about-3gpp

[388] G. Camarillo and M.-A. Garcia-Martin, *The 3G IP multimedia subsystem (IMS): merging the Internet and the cellular worlds*. John Wiley & Sons, 2007.

[389] C. Tranoris, S. Denazis, N. Mouratidis, P. Dowling, and J. Tynan, "Integrating openflow in ims networks and enabling for future internet researchand experimentation," in *The Future Internet Assembly*. Springer, 2013, pp. 77–88.

[390] A. N. Katov, B. Anggorojati, S. Kyriazakos, A. D. Mihovska, and N. R. Prasad, "Towards internet of services-SDN-enabled IMS architecture for IoT integration," in *The 18th International Symposium on Wireless Personal Multimedia Communications*, 2015.

[391] D. Puthal, B. P. S. Sahoo, S. Mishra, and S. Swain, "Cloud computing features, issues, and challenges: A big picture," in *2015 International Conference on Computational Intelligence and Networks*, pp. 116–123.

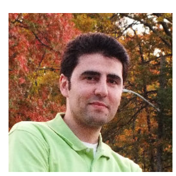
[392] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: taxonomy and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 369–392, 2014.

[393] W. Wang, B. Liang, and B. Li, "Multi-resource fair allocation in heterogeneous cloud computing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 10, pp. 2822–2835, 2015.

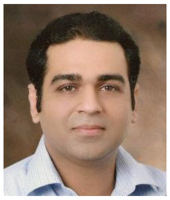
[394] D. M. F. Mattos, O. C. M. B. Duarte, and G. Pujolle, "Profiling software defined networks for dynamic distributed-controller provisioning," in *2016 7th International Conference on the Network of the Future (NOF)*, Nov 2016, pp. 1–5.

[395] M. F. Bari, A. R. Roy, S. R. Chowdhury, Q. Zhang, M. F. Zhani, R. Ahmed, and R. Boutaba, "Dynamic controller provisioning in software defined networks," in *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Oct 2013, pp. 18–25.

[396] X. Li, P. Djukic, and H. Zhang, "Zoning for hierarchical network optimization in software defined networks," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, May 2014, pp. 1–8.
[397] D. Kreutz, F. M. V. Ramos, P. E. Verssimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan 2015.
[398] I. F. Akyildiz, A. Lee, P. Wang, M. Luo, and W. Chou, "Research challenges for traffic engineering in software defined networks," *IEEE Network*, vol. 30, no. 3, pp. 52–58, May 2016.
[399] P. Thubert, M. R. Palattella, and T. Engel, "6TiSCH centralized scheduling: When SDN meet IoT," in *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*, Oct 2015, pp. 42–47.
[400] D. M. F. Mattos, O. C. M. B. Duarte, and G. Pujolle, "A resilient distributed controller for software defined networking," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.
[401] A. Ksentini, M. Bagaa, T. Taleb, and I. Balasingham, "On using bargaining game for optimal placement of SDN controllers," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.
[402] F. Chen, C. Wu, X. Hong, Z. Lu, Z. Wang, and C. Lin, "Engineering traffic uncertainty in the OpenFlow data plane," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, pp. 1–9.
[403] R. Abhishek, S. Zhao, and D. Medhi, "SPArTaCuS: Service priority adaptiveness for emergency traffic in smart cities using software-defined networking," in *2016 IEEE International Smart Cities Conference (ISC2)*, pp. 1–4.
[404] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, Feb 2015.
[405] J. Hwang, K. K. Ramakrishnan, and T. Wood, "NetVM: High performance and flexible networking using virtualization on commodity platforms," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 34–47, March 2015.
[406] Z. Ye, X. Cao, J. Wang, H. Yu, and C. Qiao, "Joint topology design and mapping of service function chains for efficient, scalable, and reliable network functions virtualization," *IEEE Network*, vol. 30, no. 3, pp. 81–87, May 2016.
[407] L. Qu, C. Assi, and K. Shaban, "Delay-aware scheduling and resource optimization with network function virtualization," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3746–3758, Sept 2016.
[408] S. Ma, B. Wang, X. Zhang, and X. Gao, "Appliancebricks: a scalable network appliance architecture for network functions virtualization," *China Communications*, vol. 13, no. Supplement 1, pp. 32–42, 2016.
[409] M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, "On orchestrating virtual network functions," in *2015 11th International Conference on Network and Service Management (CNSM)*, pp. 50–56.
[410] P. Tang, F. Li, W. Zhou, W. Hu, and L. Yang, "Efficient auto-scaling approach in the telco cloud using self-learning algorithm," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6.
[411] J. Fan, Z. Ye, C. Guan, X. Gao, K. Ren, and C. Qiao, "GREP: Guaranteeing reliability with enhanced protection in NFV," in *Proceedings of the SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization*. ACM, 2015, pp. 13–18.
[412] T. Khan, A. Hoban, P. Mohan, A. Thulasi, and P. Willis, "Distributed NFV & openStack: Challenges and potential solutions," 2016. [Online]. Available: https://www.openstack.org/assets/presentation-media/OpenStack-2016-Austin-D-NFV-vM.pdf
[413] J. F. Riera, J. Batallŷ, J. Bonnet, M. Dŷas, M. McGrath, G. Petralia, F. Liberati, A. Giuseppi, A. Pietrabissa, A. Ceselli *et al.*, "TeNOR: Steps towards an orchestration platform for multi-pop NFV deployment," in *NetSoft Conference and Workshops*. IEEE, 2016, pp. 243–250.
[414] K.-H. Lee, D. Mougouei, M. K. Yeung, H. J. Park, J. H. Bae, and A. Hameed, "Mobility management framework in software defined networks," *International Journal of Software Engineering and Its Applications*, vol. 8, no. 8, pp. 1–10, 2014.
[415] T. Q. Thanh, S. Covaci, T. Magedanz, P. Gouvas, and A. Zafeiropoulos, "Embedding security and privacy into the development and operation of cloud applications and services," in *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*, pp. 31–36.
[416] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," *IEEE Cloud Computing*, vol. 2, no. 2, pp. 30–38, 2015.
[417] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," *Computers*, vol. 3, no. 1, pp. 1–35, 2014. [Online]. Available: http://www.mdpi.com/2073-431X/3/1/1
[418] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the internet of things," in *12th International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2015, pp. 190–198.
[419] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[420] "CityFlow," (Accessed on 5 November 2016). [Online]. Available: http://www.onesource.pt/cityflow/site/module=publicPages&target=details&id=1
[421] R. Vilalta, A. Mayoral, R. Casellas, R. Martnez, and R. Muoz, "SDN/NFV orchestration of multi-technology and multi-domain networks in cloud/fog architectures for 5g services," in *2016 21st OptoElectronics and Communications Conference (OECC) held jointly with 2016 International Conference on Photonics in Switching (PS)*, pp. 1–3.
[422] W. Yang, M. Xu, G. Li, and W. Tian, "Cloudsimnfv: modeling and simulation of energy-efficient NFV in cloud data centers," *arXiv preprint arXiv:1509.05875*, 2015.
[423] M. Condoluci, F. Sardis, and T. Mahmoodi, "Softwarization and virtualization in 5g networks for smart cities," (Accessed on December 2016). [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.725.4145&rep=rep1&type=pdf

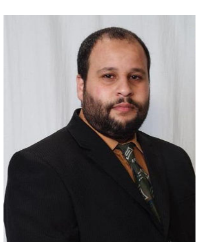


Ammar Gharaibeh is an Assistant Professor in the Computer Engineering Department at the German Jordanian University. He received his Ph.D. degree from the ECE department of New Jersey Institute of Technology in 2017. He received his M.S. degree in Computer Engineering from Texas A& M University in 2009. Prior to that, he received his B.S. degree with honors from Jordan University of Science and Technology in 2006. His research interests spans the areas of wireless networks and network caching.



Mohammad A. Salahuddin (S'09, M'15) is a postdoctoral fellow with the David R. Cheriton School of Computer Science, University of Waterloo. He received his Ph.D. degree in computer science from Western Michigan University in 2014. His research interests include wireless sensor networks, QoS/QoE in vehicular ad hoc networks, the Internet of Things, content delivery networks, software-defined networks, network functions virtualization and cloud resource management. He serves on the Technical Program Committee (TPC) for international conferences and is a reviewer for various peer-reviewed conferences, journals and magazines.

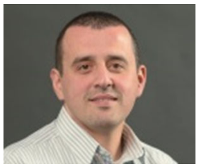
Sayed Jahed Hussini is a PhD student at the CS department of Western Michigan University since 2014. He received his M.S. degree in Computer Science from Technical University of Berlin in 2010. Prior to that he received his B.S. degree from Chemical Engineering department of Balkh University.



Abdallah Khreishah is an assistant professor in the Department of Electrical and Computer Engineering at New Jersey Institute of Technology. His research interests fall in the areas of visible-light communication, green networking, network coding, wireless networks, and network security. Dr. Khreishah received his BS degree in computer engineering from Jordan University of Science and Technology in 2004, and his MS and PhD degrees in electrical & computer engineering from Purdue University in 2006 and 2010. While pursuing his PhD studies, he worked with NEESCOM. He is a Member of the IEEE and the chair of North Jersey IEEE EMBS chapter.

Issa Khalil received PhD degree in Computer Engineering from Purdue University, USA in 2007. Immediately thereafter he joined the College of Information Technology (CIT) of the United Arab Emirates University (UAEU) where he served as an associate professor and department head of the Information Security Department. In June 2013, Khalil joined the Cyber Security Group in Qatar Computing Research Institute (QCRI), a member of Qatar Foundation, as a Senior Scientist, where he recently promoted to Principal Scientist. Khalils research interests span the areas of wireless and wireline network security and privacy. He is especially interested in cloud security, botnet detection and takedown, and security data analytics. His novel technique to discover malicious domains following the guilt-by-association social principle attracts the attention of local media and stakeholders. Dr. Khalil served as organizer, technical program committee member and reviewer for many international conferences and journals. He is a member of IEEE and ACM and delivers invited talks and keynotes in many local and international forums. In June 2011, Khalil was granted the CIT outstanding professor award for outstanding performance in research, teaching, and service.

Mohsen Guizani (S'85, M'89, SM'99, F'09) received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering from Syracuse University, New York, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor and ECE Department Chair at the University of Idaho. Previously, he served as the associate vice president of Graduate Studies and Research, Qatar University, chair of the Computer Science Department, Western Michigan University, and chair of the Computer Science Department, University of West Florida. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He currently serves on the Editorial Boards of several international technical journals, and is the Founder and Editor-in-Chief of Wireless Communications and Mobile Computing (Wiley). He is the author of nine books and more than 400 publications in refereed journals and conferences. He has guest edited a number of special issues in IEEE journals and magazines. He has also served as a member, Chair, and the General Chair of a number of international conferences. He was selected as the Best Teaching Assistant for two consecutive years at Syracuse University. He was Chair of the IEEE Communications Society Wireless Technical Committee and TAOS Technical Committee. He served as an IEEE Computer Society Distinguished Speaker from 2003 to 2005.



Ala Al-Fuqaha (S'00-M'04-SM'09) received his M.S. and Ph.D. degrees in Electrical and Computer Engineering from the University of Missouri-Columbia and the University of Missouri-Kansas City, in 1999 and 2004, respectively. Currently, he is Professor and director of NEST Research Lab at the Computer Science Department of Western Michigan University. His research interests include Wireless Vehicular Networks (VANETs), cooperation and spectrum access etiquettes in cognitive radio networks, smart services in support of the Internet of Things, management and planning of software defined networks (SDN) and performance analysis and evaluation of high-speed computer and telecommunications networks. In 2014, he was the recipient of the outstanding researcher award at the college of Engineering and Applied Sciences of Western Michigan University. He is currently serving on the editorial board for John Wileys Security and Communication Networks Journal, John Wileys Wireless Communications and Mobile Computing Journal, EAI Transactions on Industrial Networks and Intelligent Systems, and International Journal of Computing and Digital Systems. He is a senior member of the IEEE and has served as Technical Program Committee member and reviewer of many international conferences and journals.