J Inf Process Syst, Vol.15, No.4, pp.765~784, August 2019
https://doi.org/10.3745/JIPS.03.0124

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures

Jeong Hoon Jo*, Pradip Kumar Sharma*, Jose Costa Sapalo Sicato*, and Jong Hyuk Park*

Abstract

The smart city is one of the most promising, prominent, and challenging applications of the Internet of Things (IoT). Smart cities rely on everything connected to each other. This in turn depends heavily on technology. Technology literacy is essential to transform a city into a smart, connected, sustainable, and resilient city where information is not only available but can also be found. The smart city vision combines emerging technologies such as edge computing, blockchain, artificial intelligence, etc. to create a sustainable ecosystem by dramatically reducing latency, bandwidth usage, and power consumption of smart devices running various applications. In this research, we present a comprehensive survey of emerging technologies for a sustainable smart city network. We discuss the requirements and challenges for a sustainable network and the role of heterogeneous integrated technologies in providing smart city solutions. We also discuss different network architectures from a security perspective to create an ecosystem. Finally, we discuss the open issues and challenges of the smart city network and provide suitable recommendations to resolve them.

Keywords

Blockchain, Edge Computing, Internet of Things, Network Security, Smart City

1. Introduction

Smart city is emerging as a new alternative to solve various urban issues such as urban aging, traffic congestion, energy shortage, environmental pollution, and crime. Smart city is the key to discovering converged new industries that will dominate the 4th industrial revolution through data, network, and artificial intelligence (AI). Recently, there has been an increase in the number of attempts to solve urban problems using network technology both domestically and internationally. The smart city market is emerging as an innovative growth engine centered on energy, transportation, and security by utilizing information and communication technology (ICT) such as AI, big data, 5G, and network. According to a UN report, population growth in urban areas is expected to reach 66% by 2050, with 70% of the world's resources consumed in cities [1].

Markets & Markets is expected to grow from $0.4 trillion in 2004 to $1.1 trillion in 2020, whereas Frost & Sullivan expects $1 trillion in 16 years and $1.5 trillion by 2020 [2]. The overall size of the smart cities

Manuscript received February 1, 2019; first revision April 5, 2019; accepted April 18, 2019.
Corresponding Author: Jong Hyuk Park (jhpark1@seoultech.ac.kr)
* Dept. of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech), Seoul, Korea ({jojeong3766, pradip, josecostasicato, jhpark1}@seoultech.ac.kr)

market is forecast to reach $ 2.57 trillion by 2025; thus, recording strong CAGR of 18.4% over the forecast period according to a new report from Grand View Research [3]. In other words, smart city is an effective way of supporting economic growth by applying new technologies to control climate change and improve the quality of life for urban citizens. In addition, smart city focuses on security and sustainable, efficient control of available resources to improve economic and social performance. In the big data environment, the Internet has grown rapidly in terms of heterogeneous data consisting of complex media content such as text, images, video, audio, and graphics. These heterogeneous data are provided in various media, and they have various characteristics. Such heterogeneous data are made up of a mixture of cross-media data content and provided in a variety of sources and in various structured and unstructured formats. Data complexity, size, diversity, and uncertainty make it difficult to analyze and build models using traditional machine learning approaches. These situations need to address issues, challenges, and countermeasures for various papers and related research to meet heterogeneous computing requirements.

1.1 Motivation

Today, urban population growth rates are high. Efforts have been made to process increasing data in the information society efficiently, but the interpretation, combination, analysis, and proper consumption of data are very difficult to achieve due to the heterogeneous nature of the data. In the environment of the Internet of Things (IoT), which is expected to grow rapidly, convergence with other technologies is required to process the large volume of data in the smart city efficiently. In the smart city, people, systems, and things generate a lot of data. Therefore, data from diverse media are the most scalable assets of the smart city. Due to the heterogeneity of the data, however, there are many difficulties in constructing, interpreting, combining, analyzing, and consuming them. The data is larger than ever, occurring in heterogeneous environments such as water, energy, transportation, and buildings. Multidimensional and multidisciplinary technologies such as artificial intelligence, databases, data mining, and distributed systems have emerged as the ideal way of addressing most of the challenges of big data. One of the breakthroughs today, the blockchain, is widely known and has been on the rise in recent years, and it is evolving rapidly. The blockchain has revolutionary potential in smart cities, and it can be used to build intelligent, securely distributed autonomous big data collections in the data production layer of a smart city [4-7].

1.2 Research Methodology

We study and present the different application domains within a smart city environment. We also present the technical requirements to establish a sustainable smart city. We study the critical technologies required and currently in practice to develop smart city systems. We introduce the latest research work done in implementing these technologies. We also review the different architecture models available to establish a smart city-based network. The study includes the merits and demerits of each architecture application. We discuss separate application-based research works done by highlighting the use of each architecture. Finally, we will study the current open issues and challenges in our suggested survey and present our recommendations.

1.3 Research Contribution

We have done a comprehensive survey that includes all the necessary aspects to consider when

designing a sustainable smart city. Based on our research of the latest studies of smart city surveys, our paper is the only one that covers the technical requirements to establish smart cities and the various technologies required such as edge computing, blockchain, AI, software-defined networking, and big data analytics. Furthermore, we discussed different network architectures that serve as the arteries of the smart city, open issues, challenges, and recommendations. Table 1 summarizes and compares our survey with other surveys done recently.

Table 1. Contribution of our study in relation to existing surveys

Research work	Year	Technical requirements to form smart city	Integrated technologies	Study of different network architectures	Open issues	Challenges	Recommendations
Arasteh et al. [8]	2016	Limited	No	No	No	Yes	No
Gharaibeh et al. [9]	2017	Yes	No	No	No	Yes	No
Sookhak et al. [10]	2018	Yes	No	Limited	Yes	Yes	No
Eckhoff & Wagner [11]	2017	Yes	No	No	No	Yes	Yes
Cui et al. [12]	2018	No	Yes	No	Yes	Yes	No
Our study	2019	Yes	Yes	Yes	Yes	Yes	Yes

1.4 Structure of the Survey

This paper surveys and discusses emerging technologies for sustainable smart city network issues, challenges, and countermeasures. The rest of this paper is organized as follows: Section 2 discusses the requirements and design principles for a sustainable smart city network; Section 3 discusses emerging technologies for the smart city network and classifies it into each architecture outline of AI, big data analytics, software-defined networking, Blockchain, and edge computing; Section 4 surveys the various security issues in a network architecture for the smart city and analyzes and discusses related works; Section 5 focuses on the issues, challenges, and recommendations for a sustainable smart city; and Section 6 summarizes the main details of this paper and presents the conclusions and future research.

2. Design Principles for a Sustainable Smart City Network

The term sustainable smart city network is known to allow smart city connection; this concept is a new phenomenon that spread mid-2010 [8-10,13-18]. The same concept emerged in five different developments: smart cities, urban ICTs, sustainable cities, sustainable urban development, sustainability and environmental issues, urban growth, and urbanization [10]. To design the basic principle of planning a sustainable smart city network, the registration process below is followed. In this research, we will study the smart city application deployments.

2.1 Deployments of Smart City Applications

The idea of deployment applications in smart cities is closely linked to several concepts of communication technology (ICT), that is, the mass adoption of interconnected physical objects, devices, and so on based on the research of Atzori et al. [19]. It can be considered a system of systems when deploying intelligent city applications consisting of several interconnected objects [11,12]. The simplification of the system involves the diffusion of sensor technologies that allow identifying objects, collecting data and communication resources, and facilitating data distribution, information processing, computational analysis, and connection systems to improve and save urban functions and resources for the improvement of environmental performance [20,21]. Therefore, in digitalization, a new digital layer is placed between the conceptualization of the infrastructure of the city and the layer of service of the city. Fig. 1 shows an abstract view of a typical smart city application.

- Smart city governance: In the case of smart governance, the government is transparent in its actions if they are active participants in its decision making. Using emerging technologies, the city's functionality can be effectively delivered to citizens through a well-connected governance system.
- Smart mobility: Promoting sustainable urban mobility is a hallmark of smart cities. One of the main goals of smart cities is to provide innovative transport services through smart traffic management. It allows for safer and smarter decisions on how to use the transport network by providing the required information to users. For instance, to facilitate services such as surveillance, traffic control, car navigation, parking guidance, etc., various technologies can be applied to improve traffic management [22].
- Smart utility: Smart streetlights are considered to be applications that help reduce energy consumption and which can work depending on the traffic and weather conditions. This can enable the smart city to create a sustainable eco-friendly ecosystem.
- Smart community: A social service system can be set up to handle people's complaints in everyday life, personal management of social affairs, requests for assistance, and various other aspects to cover the management of the city and the functioning of the market. A single integrated system is needed to provide a platform for facilitating these services [23].

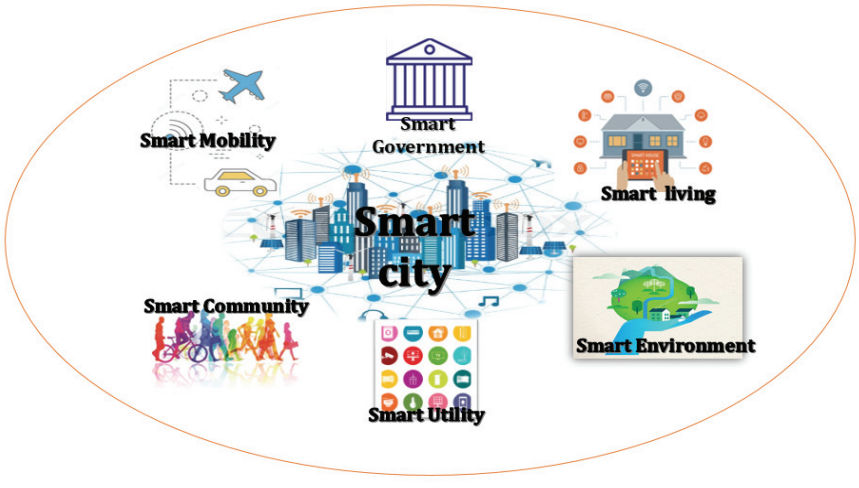


Fig. 1. Smart city applications.

- Smart living: The current health system is faced with significant challenges in the provision of low-cost, quality health services. With an increase in the elderly population, these challenges are compounded, which translates into a chronic horde of diseases as well as greater demand for health services [24]. In some cities, too, getting a proper healthcare service is difficult due to the lack of limited resources. Because of these aspects, it is necessary to evolve the current health system into an intelligent health system. Smart health is defined by a concept that involves several technologies and entities, which include various portable devices, sensors, ICT, and many other devices [25]. Smart healthcare includes several different components: intelligent hospitals, emerging in-body sensors, and intelligent response to emergencies. Different technologies are used for its operation in smart hospitals, including cloud computing, ICT information technologies, advanced data analysis techniques, and smartphone applications. From several smart city hospitals or several hospitals, offices can access patient data in real time, allowing the test data to be shared among several physicians, technicians, and nurses; thus leading to real-time decision-making about patients' health conditions and corresponding medications.
- Smart environment: Smart services are considered to be capable of providing real-time information about environmental pollution in cities by monitoring environmental changes. Citizens and governments may be aware of the adverse effect of changing their behavior in relation to public services, such as gas, electricity, and water [26].

2.2 Characteristics and Requirements of a Sustainable Network

Technical requirements for a sustainable smart city: According to Mohanty et al. [27], building a smart city needs the composition of multiple attributes. In the majority of the proposals given for the construction of smart cities, it was found to consist of four main attributes: urbanization, quality of life, smartness, and sustainability. The attributes of deploying the characteristics of a smart city are shown in Fig. 2.

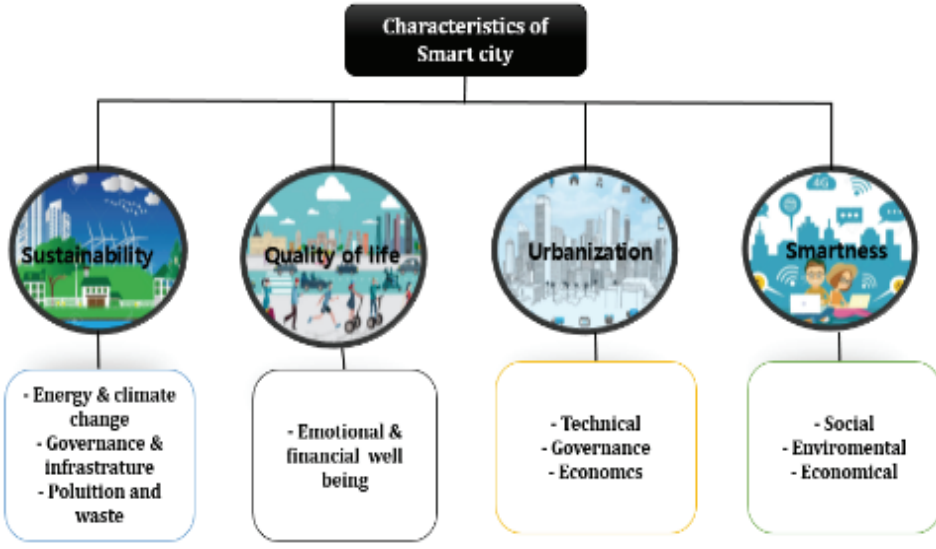


Fig. 2. Technical requirements for a sustainable smart city.

- Sustainability: The capacity to make a city achieve ecosystem balance, at the same time assisting in and performing the operations of the city.
- Quality of life: Nowadays, we can say that the financial and emotional well-being of the urban citizen indicates improvement of the quality of life, where the citizens are the key for city development; these applications aim to improve education facilities, social cohesion of health conditions, and housing quality.
- Urbanization: The attribute urbanization focuses on technological, economic, infrastructure, and governing aspects of the transformation of the rural environment into an urban environment.
- Smartness: Seen as the desire to improve the social, environmental, and economic standards of the city and its inhabitants.

Communication technology for smart city environment: Emerging communication technologies in the smart city enable connectivity among heterogeneous devices. These key technologies include WiMAX, Bluetooth, ZigBee, Wi-Fi, and many more. The main purpose of these emerging technologies' requirements is to allow high-rate data communication, high coverage, robustness, better network infrastructure, and high authentication. Table 2 presents the communication technologies that can be used as requirements for a sustainable smart city network.

Table 2. Communication technologies for a sustainable smart city network

Technology	Medium	Range	Limitations
Ethernet	Copper cables	50–70 km	Physical medium
Wi-Fi	Wireless	Up to 100 m	Coexistence interference
5G (cellular)	Millimeterwave spectrum (30–300 GHz)	2 km	Multi-hop relay optimization [28]
xDSL	Twisted pair & copper cable	Up to 4 km [29]	Asymmetric communication
Wimax	Wireless	50–70 km	Low data rate
PLC	Electrical power system	100 m between devices	Mutual interference with other technology
ZigBee	Wireless 2.4 GHz	0–20 m	Limited communication

Deploying power line communication in the smart city network is an important technology that allows network access through the electrical power system. It is related to another connected mechanism for cost-effectiveness since it operates in 2.4 GHz with other technologies such as ZigBee and Bluetooth, so it is advantageous [30].

Data acquisition technology of the smart city environment: It is essential in emerging technologies for the smart city network, in order to share the different applications and devices in smart cities using IoT technology and gather different types of data. Therefore, there is a need to apply some key requirements such as sensors, actuators, cameras, GPS terminals, social networks, and device to devices. Radio frequency identification (RFID) is known as a technology incorporating a portion of the electromagnet spectrum radio frequency that allows identifying object, people, or animal [31].

- Sensor networks: They are used by a large number of applications in environmental monitoring, waste management, health monitoring, smart grids, etc.; thus becoming one of the key technologies in data collection in smart cities, for example, in networks for intelligent traffic management, network sensors for smart street lighting, network sensors for virtual power plants, sensor networks

for smart emergency systems, networks of intelligent health sensors and more.

- 5G: Nowadays, with the increasing number of mobile devices in cities, 5G technology is expected to play a vital role in the development of smart city applications since it will allow connection in multiple devices with data exchange at speed.
- IoT: The Internet of Things (IoT) is the network that would allow connectivity enabling interconnection and communication between physical devices including vehicles, buildings, and other devices; it is also believed to be the next step in the evolution of the Internet.
- Device to device: This refers to radio communication technology wherein devices can directly exchange data without crossing access points or base stations. They can benefit greatly from device-to-device communications if the services are infrastructure-less.
- MANETs: These are considered networks without infrastructure and consisting of mobile devices, wherein wireless communication and communication with each other are allowed [18].

3. Integrated Technologies in Smart City Network Security

This section describes edge computing, Blockchain, AI, software-defined networking, and big data analytics technologies implemented in a smart city environment and explains the data problems and solutions that occur in a smart city.

3.1 Edge Computing

Smart cities require applications that provide real-time services to its citizens, which is challenging to achieve when IoT nodes connected directly with the cloud layer result in data traffic bottleneck. To address this problem, Wang et al. [32] proposed an edge cloud-assisted cyber-physical-social systems (CPSS) framework that helped reduce load from the cloud by utilizing the data processing of edge networks. These network devices are closer to the users, so they benefit from faster response due to low latency. The proposed edge cloud-assisted CPSS model uses tensors to represent data generated from smart city-based IoT devices. Data pre-processing is done at the edge layer, ensuring that only high-quality, small-scale data is transported to the cloud layer where all the intensive processing is done. The intersect tensor power method retrieves the rules established from the large-scale transition tensor at the cloud layer to the edge layer. Based on data analysis, correlations between data are determined and sent to the application layer to provide real-time, efficient smart solutions to citizens of smart-cities.

As users of smart cities move around, it is essential that data latency remain at the minimum when migrating data from one edge node to another. Taleb et al. [33] suggested a follow me edge (FME) architecture by using video streaming as an example. A service level agreement is used wherein the origin edge node using an edge orchestrator (EO) will hand over data to another EO of a different mobile access network (MNA). If the mobile device is unable to establish connection with the new edge node, however, it will receive data temporarily from the cloud to ensure uninterrupted services.

3.2 Blockchain

The blockchain solution is a disruptive technology that can provide a public-based, trustless environment where every data stored is secure from foreign data tampering. Data shared between sensors

can be further secured by using smart contracts, which only accept or release if they satisfy a given condition. Smart cities require absolute security of data communication between devices to ensure a functioning, long-term sustainable solution. Cyber-security threats are an ever-growing threat; as such, there is a visible trend in the growth of adopting a decentralized solution. Nagothu et al. [34] proposed a blockchain-based solution for a smart surveillance system. Features such as audio, facial recognition, license plate recognition, and behavior analysis are decoupled from the video footage and placed in separate private databases. These decoupled services are called microservices, which are collected at a master database where the blockchain technology is implemented for synchronizing the data. The trustless environment ensures that the data does not get tampered with as it is stored in the form of hash values. Smart contracts are used to maintain data security between the microservices and the master database. Ibba et al. [35] suggested a blockchain-based security solution of data related to a smart city, so that it is open and available to general users who are aware of city functioning without compromising data security. Data collected from sensors on user devices are stored in blocks using smart contracts. These smart contracts are based geographically, and they only accept environment data related to that area.

3.3 Artificial Intelligence

AI is often dubbed as the technology that justifies the term smart in smart city. AI is commonly used to provide solutions such as voice and facial recognition, provision of security to networks from foreign intrusion, device profiling for authentication, analytics to optimize IoT device performance in a smart city, etc. Cognitive science is recognized as the next frontier for AI where smart applications can provide personalized solutions based on human brain-like thinking. Human traits, such as brain activity, emotions, spatial-temporal data, gestures, etc., are used as features to train machines to think and behave like human beings. Chen et al. [36] suggested the use of combining brain activity such as perceptual and rational thinking with Deep Reinforcement learning algorithms. Applications can be used to detect and analyze objects the way humans do. Traditional machine learning methods suffer from limitations, i.e., they cannot recognize new objects apart from the ones they have been trained to identify. Cognitive computing-based AI allows a mapping relation to be established between the figure of the object and logical definition of the object. Alhussein et al. [37] proposed a cognitive-based IoT smart healthcare framework where the network communicates with hospital IoT devices to monitor a patient's EEG and provide low-cost, timely care. The proposed framework uses the patient's gestures, movements, and facial expressions as features to train the system and identify the patient's health. Based on a probability score, data processing is done at the cloud layer where the signals are classified as either seizure or non-seizure. Their model showed an accuracy level of 99.2% and a sensitivity level of 93.5%.

3.4 Software-Defined Networking

Smart cities can have an emergency or a popular event that requires constant availability of network to maintain open channels of communication. Network congestion is such a critical problem during such critical events. To circumvent this, Abhishek et al. [38] proposed a software-defined framework (SDN) that can route network traffic based on priority. Using Open Virtex (OV), a network virtualization platform is used with SDN to establish virtual networks. A middlebox layer is used to assign priority to the selected virtual network. A separate virtual network is allocated the highest priority while the

remaining unused network resources are reallocated accordingly. The reallocation ensures that the remaining services are not affected, and services resume normally as required. Usman et al. [39] proposed an SDN architecture that supports device-to-device (D2D) communication. The aim is to establish a stable, constant connection between disaster victims and first responders. The central SDN controller has a global view of the entire network and controls the user equipment in different clouds. The network consists of local controllers that make the proposed architecture scalable. In a disaster scenario, the SDN controller maintains communications between the first responders and victims by selecting a multi-hop routing path. The multi-hop routing serves a secondary purpose, i.e., aiding first responders in locating the disaster victims. The cloud environment fulfills the needs for storage and intense computing. The raw data gathered from sensors are routed to cloud for processing and then to first responders.

3.5 Big Data Analytics

Smart cities generate enormous amounts of data, so they can be used to serve its citizens more efficiently. Big data offers smart cities the means of obtaining insights from the data collected from various IoT devices spread throughout the city. This data is used to provide valuable insights that are used to optimize the performance of machines in smart city domains such as energy, industrial IoT, homes, buildings, etc. Rathore et al. [40] proposed a helpful 4-tier model for big data analysis in urban planning. Data is extracted from IoT devices in smart city domains such as automobile networks, smart parking, weather, pollution, surveillance, etc., to allow authorities to make intelligent decisions that are implemented in real time. Hadoop and Spark are used to achieve real-time processing. The model test results recorded increasing efficiency as the size of data increased, which is helpful as IoT device data are expected to outgrow currently available volumes exponentially. Rathore et al. [41] proposed a system for smart city urban planning with data extracted from IoT sensors and applied big data analytics for knowledge purposes. The model allows municipal authorities to make municipalities smart and efficient. Data collection is done in real time using Hadoop working under Apache Spark. The use case of the smart transportation system has been implemented in tests wherein live vehicle data is used to provide real-time information to citizens on traffic alerts. Big city graph processing is accomplished by using Giraph over Hadoop. The analysis of test results revealed that the efficiency of the system increased as the size of data increased and yielded real-time results that are ideal for a smart city use case.

4. Security in Network Architecture

In this section, we discuss the different architecture types present in a smart city environment from the perspective of providing security. These include centralized architecture, decentralized architecture, and distributed architecture. We discuss related issues and challenges and their respective countermeasures. In Table 3, we present the advantages and disadvantages associated with each architecture type and classify them based on existing research.

4.1 Centralized Architecture

A centralized architecture is more straightforward to manage since there is only a single system with server point of failure; in the event of system failure, however, the entire network would come to a halt.

Table 3. Summary of network security description and related works

Category	Subject	Description	Ref.
Centralized architecture	A survey on IoT security	Extensive investigation into existing research on IoT security threats and vulnerabilities	Alaba et al. [42]
	CCN in smart cities	Hierarchical approach and analysis of proposed CCN based on SDN	Fekih et al. [43]
Decentralized architecture	A communications-oriented perspective for smart cities	The research discusses the TMS of smart cars and social media, presents the challenges and visions through security threats and project investigations of various technologies.	Djahel et al. [44]
	Zenith	The research proposed Zenith, an edge computing platform for computing resources.	Xu et al. [25]
	CF-CloudOrch	The research proposed CF-CloudOrch for IoT networks with SDN, VM, and container of network security service and management services.	Kim et al. [45]
	Edge-fog cloud	The research suggested the Edge-Fog cloud, a distributed cloud model for large-volume and data processing.	Mohan & Kangasharju [46]
	Secure IoT architecture for smart cities	The study proposed a secure IoT architecture via black network for smart city.	Chakrabarty and Engels [47]
Distributed architecture	Edge computing: vision and challenges	The research examined various case studies and collaborative advantages for implementing cloud offload and smart city.	Shi et al. [48]
	Survey on IoT: security and privacy, applications	The research proposed fog and edge computing by integrating IoT for computing services devices at the network edge.	Lin et al. [23]
	DistArch-SCNet	The research proposed a blockchain-based distributed network architecture with Li-Fi communications for reduced end-to-end latency, response time, and processes in smart city.	Sharma et al. [24]
	Software-defined fog node-based blockchain cloud architecture	The research proposed a blockchain cloud architecture for improving the security and performance of IoT networks.	Sharma et al. [26]
	DistBlockNet	The research proposed a block-chain-based SDN architecture for large-scale IoT network security.	Sharma et al. [13]
	MIST	The research proposed MIST with a fog-based approach that supports crowd-aware applications to minimize response time.	Arkian et al. [14]

There is a constant risk of instability in the whole network if it is attacked. A centralized architecture-based environment is easy to set up, but it is also open to malicious attacks. Under a cyber-attack, centralized network security can be easily thwarted, with the network brought to a halt. Smart city-based centralized architecture has the challenge of being less scalable and unable to accommodate various networks. SDN is implemented to overcome the issue of scalability. Many researchers have attempted to address the issue of scalability and availability, mainly by reducing the overhead of the centralized controller in various aspects. Below is a survey of the centralized architecture and related research.

Alaba et al. [42] focused on vulnerabilities and security threats in cutting-edge IoT through existing IoT security research. Administrators based on the SDN architecture are offered a holistic view of possible attacks, threats to the network, and ability to protect and control the network against such threats.

Separating SDN data and control planes degrades packet processing and causes serious problems such as distributed DoS (DDoS) attacks and loss or delay of packets. Fekih et al. [43] proposed a hierarchical approach and a comparative study of content centric networks (CCN) based on SDN architecture. Their research focuses on the architectural model and its results and lists how to evaluate the performance of these solutions regarding complexity and speed. Smart City lists how CCN and SDN are applied, but there is no mention of proofs and experiments.

4.2 Distributed Architecture

Distributed architecture refers to the network that can be laid out physically in a wide geographical area or close together but is connected to a local network. These devices have their own computational memory and communicate with each other. Edge computing is part of the distributed architecture and is used to bring the processing of data near the devices; thus reducing network latency. Instead of sending and processing data from the device to the cloud layer, the data is gathered and processed near the devices. This adds the benefit of a reduction in usage of bandwidth, helping run real-time applications in smart cities. Mist computing has taken the processing even nearer to the edge-points of the devices. This method maintains the privacy of data of users via local device processing.

Djahel et al. [44] investigated the various technologies used in the stages of traffic management systems (TMS) and discussed them with social media smart cars, which allow accurate detection and fast mitigation of traffic congestion. This system enables looking at the latest trends in security threats and projects. This survey identifies the open challenges and visions in the future smart city for robust TMS development.

Xu et al. [25] proposed Zenith to allocate computing resources to edge computing platforms. Unlike traditional solutions, Zenith has adopted a new, separate architecture wherein the infrastructure management of the edge computing infrastructure (EC) is performed independently of the service provision and service management performed by the service provider. It also proposed a latency scheduling scheme through the mechanism that demonstrates, tests, and evaluates efficiency, scalability, and performance. Therefore, it can improve efficiency, scalability, and performance to fit Smart City.

Kim et al. [45] proposed CF-CloudOrch using VM, container, and SDN networking. CF-CloudOrch supports scheduling, management services load balancing, and security service management. This architecture reduces data throughput and improves performance for IoT networks. This in turn allows smart city to monitor various cyber-attacks quickly through real-time management. The edge-fog cloud was proposed by Mohan and Kangasharju [46], and it is a distributed cloud model for processing large volumes and data. Least processing cost first (LPCF) allocates processing tasks to nodes that provide optimal processing time and optimal networking costs. This has been proven effective in evaluating LPCF in various scenarios and finding processing task assignments. Smart city can show efficiency in allocating processing tasks to the network. Chakrabarty and Engels [47] proposed a secure IoT architecture for smart city that emphasizes security via black networks, authentication using a unified registry, secure key management system, and secure routing via a trusted SDN. The four models above can be implemented across different smart city domains.

4.3 Decentralized Architecture

Decentralized architectures are more expensive to establish and maintain compared to centralized

systems. Unlike a centralized architecture network, a decentralized system does not suffer from a single point of failure. Devices on this network are individual, and no central authority exists. In the event of an attack should a device fail, other devices in the system will continue to function with no effect on them since there is no central machine handling all of the processes within the network. Decentralized systems do not suffer from the issue of scalability as more devices can be added to the network system, thereby lending their computing power to the network. A second benefit from scalability is decentralized systems to accommodate a standard network in a smart city. As information does not traverse through a single point, there is a higher likelihood of maintaining the privacy of data. We discuss below the survey of the decentralized architecture and related research.

Shi et al. [48] introduced the definition of edge computing and investigated the collaborative edge for various case studies and materialization of cloud offloading and smart city. This included service management, privacy and security, and optimization metrics in the field of edge computing. This survey considers smart city's large data volume, low latency, and location awareness and looks at the challenges and opportunities of edge computing. Lin et al. [23] proposed fog and edge computing to computing services devices on the network edge by integrating with IoT, with the aim of improving user experience and resilience of services in the event of a failure. This survey is closely related to spoofing attacks, various hall attacks, MITM, and other network security in smart city, and it can also include data related to personal information. Sharma et al. [24] proposed a distributed blockchain network architecture model that significantly reduces end-to-end latency, response time, and processes at the heart of a smart city network. The proposed model takes into account difficult issues such as how to place cache nodes according to context and how to filter raw data at the network edge. In addition, this architecture efficiently handles buffer overflow and flooding attacks on flow tables and provides better performance than other methods in terms of bandwidth. Sharma et al. [26] proposed a blockchain cloud architecture for cloud computing infrastructures in IoT networks. They also use SDN and blockchain technology to achieve economical, high-performance computing and apply computing resources to the edge network for the IoT network. This architecture provides secure, distributed fog node architecture for secure and efficient control of large volumes of data. This reduces induced delay and response time, increases throughput, and improves performance by detecting real-time attacks on the IoT network with low-performance overhead. In this paper, the network in the smart city is considered to have both security and efficiency. Sharma et al. [13] proposed a secure SDN architecture distributed over SDN-based networks using blockchain techniques to analyze issues faced by large-scale IoT networks. The role of this architecture is to create and deploy protection features such as threat prevention, data protection and access control, cache flooding, ARP spoofing, DDoS and DoS attacks, and network attack mitigation such as threat detection. Arkian et al. [14] presented a fog-based scheme to provide the cost-effective provisioning of limited resources and support crowd sensing applications. To meet the quality of service requirements and reduce overall costs, they collectively address the issues of virtual machine placement, task distribution, and data consumer association.

5. Open Issues, Challenges, and Recommendations

Even though cities nowadays are seeking to become smarter, the abovementioned emerging technologies in smart cities applications in terms of security and privacy raise a series of issues and

challenges. All devices connected within the network are susceptible to cyber-attacks, which can bring about serious consequences when you start connecting essential systems like the entire city power grid. The key requirements that we must know in relation to security and privacy include integrity, confidentiality, availability, non-repudiation, access control, and privacy [34], and they must be met in the fields of information, communication, and physics. In addition, there is the issue of a constantly expanding attack surface. With the rapid development of information technologies such as artificial intelligence, big data analysis, blockchain, and edge computing, more and more hackers are becoming more intelligent when it comes to hacking a network. Fig. 3 shows a diagram of some open issues and challenges that we are facing in smart city networking.

5.1 Data Integration Challenges

Data from smart city technologies use various data formats using the wide variety of intelligent objects implemented throughout the city. In recent years, various technologies have been integrated and deployed in smart cities, where they can reduce many technical barriers to data handling. According to Gouveia et al. [16], however, one of the challenging problems of data quality in any data integration mechanism, usually if such data is missing, is incorrect or incomplete use or use of the wrong format.

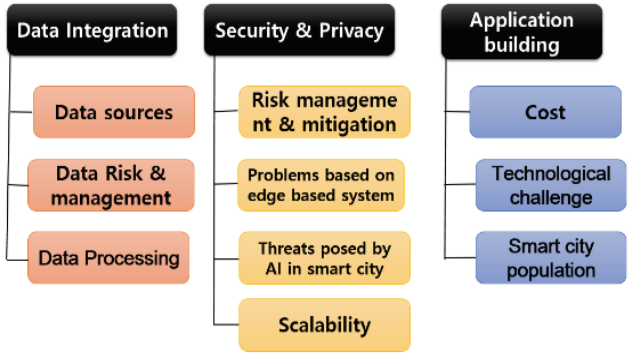


Fig. 3. Smart city issues and challenges.

- Data sources: One of the first and major challenges is the change in data sources and the need for data quality assurance. From a single source to various sources, the data source is considered to be changing with regard to the integration of data into intelligent city developments. The value of the data is changing from a single purpose to various purposes. From the organizational level, data functions are shifting to the regional level in sectors and agencies. In addition, various sources are becoming the main issue with regard to ensuring data quality related to data integrity, reliability, authenticity, and reuse. There is a growing need to ensure consistency of data quality across systems platforms. Data is generated from several different sources in many different formats. It is known that there are several new data formats, many of which are not structured (such as images, audio, tweets, video, server records and more). Michalik et al. [17] cited the need to manage and classify this data in structured format using some kind of advanced database system.
- Data processing: The changes in data processing activities are one of the challenges of data continuity. Where data is used as a single source for various data sources and formats, some of this

static data for real-time data, structured data for unstructured data, and data capture is changing. For the distributed refrigerated storage for centralized cloud storage, this type of data storage is being moved. Using this data is changing open access for public information wherein it can open public data [38]. There are several problems, including data loss and information overlap.

- Data risk and data management: In some applications and in big data technologies, there is known to be maximum risk in disclosing the privacy and identity of people in certain communities in terms of data integration, with negative impacts on data analysis and dissemination of data. Due to the lack of information systems' supervision and security use, current industry standards are not adequate considering the limitations of reusing personal data by big data applications and technologies [38]. Data risk is one of the major challenges.

5.2 Security and Privacy

Nowadays, the use of sustainable emerging technologies for the smart city network to improve the functionality of urban systems and promote sustainable development is expected to improve the quality of daily life. Security and privacy issues are becoming a major challenge that requires effective countermeasures based on the emergence and implementation of this technology in several intelligent systems. Kitchin [49] and Li et al. [50] noted that, in smart cities, even if the developments mentioned above can contribute to the improvements of the whole society, almost all smart applications are vulnerable to hackers through update attacks like attacks of knowledge, collision attacks, espionage, attacks of spam, and sympathy attacks. According to Ferrag et al. [51], the basic requirements for good security and privacy often include integrity, confidentiality, availability, access control non-repudiation, and privacy; because of these unique features, security and privacy challenges are becoming problems and preventing smart cities from encouraging further use.

- Threats posed by AI in smart city: AI systems are considered to present indispensable tasks in many types of intelligent applications such as automatic system control, pacemakers, and home appliances in so far as the increasing use of artificial intelligence presents several risks regarding security. One example is that the Device Manufacturers and Service Providers may use data mining technologies that may allow them to extract sensitive information and analyze personal data that exceed several primary service-related objectives [42]. In addition, invaders possessing knowledge of artificial intelligence are themselves more intelligent [43]. Some hackers can see how machine learning (ML) protection mechanisms are designed and trained to adopt targeted approaches to reduce and weaken algorithm reliability. With the increasing use of artificial intelligence technologies, however, there are several security risks.
- Problems based on edge-based system: As emerging technologies to be implemented in smart cities' network, their edge-based structures are presented with new security challenges because some of their edge distributed systems operation environments are vulnerable to attacks compared to centralized clouds [44]. Therefore, we must consider which protections in intelligent systems the edge-based intelligent devices should pay considerable attention [25].
- Security risk management and mitigation: Smart city technologies consist of sensor devices deployed around hostile environments and present a large number of security threats. It is important to design methods that can mitigate such threats in order to facilitate their applications deployed in smart cities and increase users' willingness to use these smart city applications.

Therefore, considering the heterogeneity of devices and sensor networks in smart cities, implementing a scheme that covers risk mitigation is a very critical challenge. Based on the example [45,46], mentioning the existence of some risk mitigation models for different networks and detection devices, it is impossible to use a combination of such schemes for intelligent cities. We can say that smart cities need a security mitigation model to decide whether they are migrating from the data to the virtual server considering the degree of sensitivity of the data.

- Scalability: With the high number of smart devices that have increased, and with the heterogeneous type of devices, interactions, and applications, scalability is considered to be one of the major technical challenges for the large-scale deployment of sensors and detection environment. Large volumes of sensor data should be analyzed and aggregated in the mobile cloud, as they are issues related to security and privacy. The heterogeneity mentioned above gives rise to issues related to interoperability. Data processing presents a major challenge in providing unified models of rich, interoperable data description.

5.3 Application Building

Cost: The adoption of smart cities is one of the big challenges that are costly. Since a smart city technology requires the integration of a variety of components, it is very expensive to implement, because acquiring them can be burdensome for the government due to the scarcity of natural and human resources. Thus technologies and open-standards structures [31] provide cost reduction in this area according to Luong et al. [30]. Note, however, that structures and technologies should be intensified by some open standard efforts, which will facilitate interoperability and data exchange among different applications, devices, services, or products in the smart city technology.

Technological challenges: Nowadays, with the increasing demand for smart city, big data, artificial intelligence, and edge computing are stimulating the innovation, development, and emergence of new intelligent applications that are becoming more important. In order to improve such smart city services, however, the data collected must be well-managed. This subsection aims to address some of the major technological challenges related to the big data and smart city.

Smart city population: It is considered to be a challenge because high growth will generate increased social inequality, traffic congestion, and pollution, and the increase in urbanization gives rise to variances in organizational and economic technical problems that tend to jeopardize the economy and environment of smart cities. People are affected by smart applications [52].

5.4 Recommendation

The widespread use of smart applications has given rise to many security and privacy issues. Therefore, with emerging technologies, the smart city network consists of various devices, and a single compromised device will make the entire collection vulnerable and allow hackers to perform a series of cyber-attacks by exploiting such vulnerabilities. Smart city security is essential for a city to incorporate the technologies into smart city cyber infrastructure and to improve the conditions of life for its citizens. With such technologies in smart cities, we cannot consider a city smart unless it provides the required maximum level of security. General requirements recommended for security and privacy include confidentiality, availability, integrity, privacy, non-repudiation, and access control. The detected data of physical spaces taken advantage of by the smart city contain granular details about people who live in those

environments.

With the blockchain-based security framework, secure communication of data is enabled in a smart city. One of the main advantages of the use of blockchain is that it is resilient against many threats. In addition, this technology provides several unique features such as improved reliability, improved fault tolerance, faster, more efficient operation, and scalability. Therefore, the integration of blockchain technology with devices in a smart city will allow the creation of a common platform wherein all devices can communicate security in a distributed environment.

6. Conclusion

Cities are growing quickly; at present, cities account for more than half of the world's population, and 2.5 billion new residents are expected to be added by 2050. Therefore, it is not surprising that smart technologies are seen as a way of meeting the challenges of fast-growing cities. The creation of a sustainable ecosystem for the smart city network has drawn the attention of the academe and industry to emerging integrated technologies. In this study, we presented a comprehensive survey on the role of emerging technologies in building a sustainable smart city network. A discussion of advanced enabling integrated technologies used in smart cities is presented to help the reader understand recent efforts in this direction. We also classified the network architecture based on the structure from the security perspective. Finally, we discussed open research issues, challenges, and recommendations as future directions for research.

Acknowledgement

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B01070416).

References

[1] 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.

[2] H. March, "The smart city and other ICT-led techno-imaginaries: any room for dialogue with degrowth?," *Journal of Cleaner Production*, vol. 197, pp. 1694-1703, 2018.

[3] K. Saravanan, E. G. Julie, and Y. H. Robinson, "Smart cities & IoT: evolution of applications, architectures & technologies, present scenarios & future dream," in *Internet of Things and Big Data Analytics for Smart Generation*. Heidelberg: Springer, 2019, pp. 135-151.

[4] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: a distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184-195, 2017.

[5] V. Suryani, S. Sulistyo, and W. Widyawan, "Two-phase security protection for the Internet of Things object," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1431-1437, 2018.

[6] A. Souri and R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Human-centric Computing and Information Sciences*, vol. 8, article no. 3, 2018.

[7] P. K. Sharma, J. H. Ryu, K. Y. Park, J. H. Park, and J. H. Park, "Li-Fi based on security cloud framework for future IT environment," *Human-centric Computing and Information Sciences*, vol. 8, article no. 23, 2018.

[8] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, and P. Siano, "IoT-based smart cities: a survey," in *Proceedings of 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, Florence, Italy, 2016, pp. 1-6.

[9] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, "Smart cities: a survey on data management, security, and enabling technologies," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2456-2501, 2017.

[10] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: a survey, research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1718-1743, 2018.

[11] D. Eckhoff and I. Wagner, "Privacy in the smart city: applications, technologies, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489-516, 2017.

[12] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134-46145, 2018.

[13] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "Distblocknet: a distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78-85, 2017.

[14] H. R. Arkian, A. Diyanat, and A. Pourkhalili, "MIST: fog-based data analytics scheme with cost-efficient resource provisioning for IoT crowdsensing applications," *Journal of Network and Computer Applications*, vol. 82, pp. 152-165, 2017.

[15] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 136-141, 2013.

[16] J. P. Gouveia, J. Seixas, and G. Giannakidis, "Smart city energy planning: integrating data and tools," in *Proceedings of the 25th International Conference Companion on World Wide Web*, Montreal, Canada, 2016, pp. 345-350.

[17] P. Michalik, J. Stofa, and I. Zolotova, "Concept definition for big data architecture in the education system," in *Proceedings of 2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Herl'any, Slovakia, 2014, pp. 331-334.

[18] D. Li, Y. Yao, and Z. Shao, "Big data in smart city," *Geomatics and Information Science of Wuhan University*, vol. 39, no. 6, pp. 631-640, 2014.

[19] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[20] S. Al-Nasrawi, C. Adams, and A. El-Zaart, "A conceptual multidimensional model for assessing smart sustainable cities," *Journal of Information Systems and Technology Management*, vol. 12, no. 3, pp. 541-558, 2015.

[21] M. Ibrahim, C. Adams, and A. El-Zaart, "Paving the way to smart sustainable cities: transformation models and challenges," *Journal of Information Systems and Technology Management*, vol. 12, no. 3, pp. 559-576, 2015.

[22] M. Hojer and J. Wangel, "Smart sustainable cities: definition and challenges," in *ICT Innovations for Sustainability*. Cham: Springer, 2015, pp. 333-349.

[23] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017.

[24] P. K. Sharma, S. Rathore, and J. H. Park, "DistArch-SCNet: blockchain-based distributed architecture with Li-Fi communication for a scalable smart city network," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 55-64, 2018.

[25] J. Xu, B. Palanisamy, H. Ludwig, and Q. Wang, "Zenith: utility-aware resource allocation for edge computing," in *Proceedings of 2017 IEEE International Conference on Edge Computing (EDGE)*, Honolulu, HI, 2017, pp. 47-54.

[26] P. K. Sharma, M. Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115-124, 2017.

[27] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: the internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60-70, 2016.

[28] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the Internet of Things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64-71, 2016.

[29] J. P. Vasseur, G. Mermoud, and S. Dasgupta, "Mixed centralized/distributed algorithm for risk mitigation in sparsely connected networks," U.S. Patent No. 9565111, 2017.

[30] 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, 2016.

[31] M. Ortiz-Rangel, L. Rueda-Vasquez, C. Duarte-Gualdron, J. Petit, and G. Ordonez-Plata, "Towards a smart city: design of a domestic smart grid," in *Proceedings of 2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM)*, Montevideo, Uruguay, 2015, pp. 863-868.

[32] P. Wang, L. T. Yang, and J. Li, "An edge cloud-assisted CPSS framework for smart city," *IEEE Cloud Computing*, vol. 5, no. 5, pp. 37-46, 2018.

[33] T. Taleb, S. Dutta, A. Ksentini, M. Iqbal, and H. Flinck, "Mobile edge computing potential in making cities smarter," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 38-43, 2017.

[34] D. Nagothu, R. Xu, S. Y. Nikouei, and Y. Chen, "A microservice-enabled architecture for smart surveillance using blockchain technology," in *Proceedings of 2018 IEEE International Smart Cities Conference (ISC2)*, Kansas City, MO, 2018, pp. 1-4.

[35] S. Ibba, A. Pinna, M. Seu, and F. E. Pani, "CitySense: blockchain-oriented smart cities," in *Proceedings of the XP2017 Scientific Workshops*, Cologne, Germany, 2017.

[36] M. Chen, F. Herrera, and K. Hwang, "Cognitive computing: architecture, technologies and intelligent applications," *IEEE Access*, vol. 6, pp. 19774-19783, 2018.

[37] M. Alhussein, G. Muhammad, M. S. Hossain, and S. U. Amin, "Cognitive IoT-cloud integration for smart healthcare: case study for epileptic seizure detection and monitoring," *Mobile Networks and Applications*, vol. 23, no. 6, pp. 1624-1635, 2018.

[38] R. Abhishek, S. Zhao, and D. Medhi, "SPArTaCuS: service priority adaptiveness for emergency traffic in smart cities using software-defined networking," in *Proceedings of 2016 IEEE International Smart Cities Conference (ISC2)*, Trento, Italy, 2016, pp. 1-4.

[39] M. Usman, A. A. Gebremariam, U. Raza, and F. Granelli, "A software-defined device-to-device communication architecture for public safety applications in 5G networks," *IEEE Access*, vol. 3, pp. 1649-1654, 2015.

[40] 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.

[41] M. M. Rathore, A. Paul, W. H. Hong, H. Seo, I. Awan, and S. Saeed, "Exploiting IoT and big data analytics: defining smart digital city using real-time urban data," *Sustainable Cities and Society*, vol. 40, pp. 600-610, 2018.

[42] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10-28, 2017.

[43] A. Fekih, S. Gaied, and H. Yousef, "A comparative study of content-centric and software defined networks in smart cities," in *Proceedings of 2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*, Sfax, Tunisia, 2017, pp. 147-151.

[44] 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, 2014.

[45] N. Y. Kim, J. H. Ryu, B. W. Kwon, Y. Pan, and J. H. Park, "CF-CloudOrch: container fog node-based cloud orchestration for IoT networks," *The Journal of Supercomputing*, vol. 74, no. 12, pp. 7024-7045, 2018.

[46] N. Mohan and J. Kangasharju, "Edge-fog cloud: a distributed cloud for Internet of Things computations," in *Proceedings of 2016 Cloudification of the Internet of Things (CIoT)*, Paris, France, 2016, pp. 1-6.

[47] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for smart cities," in *Proceedings of 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2016, pp. 812-813.

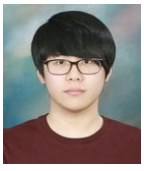
[48] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, 2016.

[49] R. Kitchin, "Getting smarter about smart cities: improving data privacy and data security," Department of the Taoiseach, Dublin, Ireland, 2016.

[50] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68-75, 2011.

[51] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 3015-3045, 2017.

[52] A. Kramers, M. Hojer, N. Lovehagen, and J. Wangel, "Smart sustainable cities: exploring ICT solutions for reduced energy use in cities," *Environmental Modelling & Software*, vol. 56, pp. 52-62, 2014.



Jeong Hoon Jo https://orcid.org/0000-0002-9073-4993

He received B.S. degrees in School of Computer Science and Engineering from Seokyeong University in 2012 and 2018, respectively. Since March 2018, he is with the School of Computer Science and Engineering from Seoul National University of Science and Technology as a MS student.

Pradip Kumar Sharma https://orcid.org/0000-0001-6620-9083

He is a Ph.D. scholar at the Seoul National University of Science and Technology. He works in the Ubiquitous Computing & Security Research Group. Prior to beginning the Ph.D. program, he worked as a software engineer at MAQ Software, India. He worked on a variety of projects, proficient in building large-scale complex data warehouses, OLAP models and reporting solutions that meet business objectives and align IT with business. He received his Master's degree in Computer Science from the Thapar University, in 2014, India. His current research interests are focused on the areas of ubiquitous computing and security, cloud computing, SDN, SNS, and IoT. He is also reviewer top cited journals such as IEEE Com. Mag., IEEE Net. Mag., IEEE SJ, IEEE TII, IEEE IoT, IEEE TNSM, FGCS, and IEEE CE Mag.

Jose Costa Sapalo Sicato https://orcid.org/0000-0002-7834-2268

He is a Master's Degree Scholar at the Seoul National University of Science and Technology. He received Bachelor's degree in Telecommunication engineer at the International University of Management in Namibia. He worked as an Information Technology engineer at Angola Telecom Company. His current research interests are focused on security, blockchain, AI and IoT.

James J. (Jong Hyuk) Park https://orcid.org/0000-0003-1831-0309

He received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences – MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, The Journal of Information Processing Systems (JIPS) by KIPS, and Journal of Convergence (JoC) by KIPS CSWRG. He is Associate Editor / Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.