International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

Digital modeling as a service (DaaS) to improve smart city infrastructure architecture

Mohaddeseh Pasban
[1] Master of Science in Information Technology Engineering
Mehdi Pasban
[2]PhD in Industrial Engineering, Islamic Azad University, Qazvin, Iran

Abstract
Digitalization has driven infrastructures and cities to become "smarter"; the utilization of physical space and energy resources, data exchange, user management, assets, processes, and how businesses operate have been gradually redesigned in a digital context. The fundamental challenges of a smart city include its conceptual definition, implementation dimensions, and inter-system communications. Approaches to implementing a smart city range from multidisciplinary and collaborative models to the integration of information and communication technology (ICT) in the physical context and the use of big data in more abstract decision-making. This article introduces the concept of "Digital as a Service" (DaaS); a model in which the complete digitalization process can be realized in a cloud environment, independent of the physical infrastructure. DaaS enables greater integration and flexibility by creating a compatible virtual digital infrastructure (VDI). In addition, this article analyzes existing digital systems, transmission networks, servers, and management mechanisms. The future industrial revolution will be based on artificial intelligence; a revolution that will replace many human functions with decision-making based on the Internet of Things (IoT), cloud computing, blockchain, big data, virtual reality, and the convergence of digital and physical infrastructure. The "Digital as a Service" model will act as a key enabler of this transformation by creating a complete link between the interconnection, integration, and virtualization of space, services, and structure (3S).

Keywords: Digital systems, Internet of Things, smart grids, information and communication technology, artificial intelligence, smart cities

Introduction

Digitalization has driven infrastructure towards increased intelligence. The optimal use of physical spaces and energy, the proactive management of users, assets and processes, as well as improved efficiency of organizations and companies, have gradually been achieved in the context of digital transformation. Countries that have developed digitalization not only in the manufacturing sector—such as the use of robotics or the Internet of Things (IoT)—but also on a broader scale, including "smart city" solutions such as e-health and smart grids, have experienced a reduction in operating expenses (OPEX) and an increase in gross domestic product (GDP) [1].

The main challenge in realizing a smart city lies in defining it comprehensively and determining its scope of application. The concept of a smart city ranges from implementing digital systems on top of information and communication technology (ICT) infrastructures—such as IoT, cloud computing, mobile phones, or big data analytics—to designing analytical models for real-time decision-making. In addition, a smart city can be built on multidisciplinary frameworks with the participation of government agencies and citizens to promote social empowerment. Meanwhile, the ICT sector of a smart city faces technical challenges arising from the interoperability of enabling technologies, communication protocols, and heterogeneous architectures developed by independent companies. One of the key technology-enabled services in the energy domain of smart cities is defined based on the three driving forces of decarbonization, digitalization, and decentralization [3]. This approach is implemented in smart grids of electricity distribution, enabling the integrated management of energy generation, transmission, distribution and storage to meet the growing needs of cities in low-carbon environments and protect citizens from CO_2 emissions. Smart cities are considered as large-scale networked systems, composed of interconnected and interdependent components [4]. In this way, the smart city model can be defined, analyzed and optimized with the aim of increasing sustainability. The digital twin goes beyond the simulation of Building Information Modeling (BIM) and is seamlessly integrated into the artificial city structure and digital space. The critical components of the effectiveness of smart cities include drivers that define success by increasing the quality of life of citizens and improving the return on investment. These drivers should encompass a wide range of interdisciplinary fields, including applied social

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

sciences, engineering, earth sciences and humanities [5].

Project management in the context of smart cities is implemented by clarifying the requirements of stakeholders through independent delivery organizations and overseeing design, construction, implementation and operation. [6] These organizations must deliver high-quality outputs aligned with digital objectives by adhering to the principles of the "project management triangle"—time, cost and scope.

The Fourth Industrial Revolution [7] has begun with the integration of new technologies such as IoT, cloud computing, blockchain, virtualization, robotics and autonomous vehicles; technologies that have replaced some of the human activities and increased productivity. Subsequently, the Fifth Industrial Revolution will be based on artificial intelligence and deep learning; a revolution that will completely replace humans in some areas with automated decision-making in production and management.

This paper introduces the concept of Digital as a Service (DaaS), a model in which the digitalization process can be implemented independently of the physical infrastructure in a cloud environment. DaaS enables access to a compatible virtual digital infrastructure (VDI) and focuses on the digitalization of real infrastructure as the creation of "smart infrastructure"—an infrastructure that will be the foundation of future smart cities and countries, where all independent elements and systems are integrated, connected, and virtualized.

The integration of these functional components of a smart city enables the development of high-level abstraction structures, while improving the efficiency and quality of services, while reducing operational and maintenance costs. In the meantime, DaaS will play a role as a key driver of the Fifth Industrial Revolution by combining big data, connecting sensors and assets, and virtualizing space, services, and structure (3S).

In the second part of the paper, an overview of the concepts and definitions of smart city and the digitalization process is provided, including inter-sectoral cooperation, ICT requirements, big data applications, energy requirements, and blockchain technology. The third part explains the evolution of digitalization at the sensor, network, server, and workstation levels. The fourth part describes the concept and mathematical model of DaaS, and the fifth to eighth parts are devoted to examining its key components, including digital systems, digital transmission, digital servers, and digital management. Finally, the challenges and results of the research are summarized in the ninth and tenth parts.

2. Research Background

2.1 Definition

The concept of "smart city" has been defined in many ways, but no single, universally accepted definition has yet been adopted [8]. Analysis of the scientific literature shows that the most common terms used in academic research to describe the "smartness" of a city are "smart city" and "digital city". Reviews of various scientific publications have focused on the aspects of "smart" cities [9]. These studies often conclude that many of the claims in this area are self-aggrandizing and heavily dependent on specific and consistent entrepreneurial roadmaps for their development.

A conceptual framework for understanding smart cities is often based on eight critical factors: 1) management and organization, 2) technology, 3) governance, 4) policy context, 5) people and communities, 6) economy, 7) built infrastructure, and 8) natural environment [10]. These factors form the basis of an integrated framework that proposes guidelines and programs for local governments to anticipate and guide smart city initiatives. The relationship between the concepts of "smart city" and "digital city" is defined based on the main content of the applied systems, the challenges of constructability and their impacts on the urban development process [11].

Smart city infrastructure, as a first step, is considered the basis for creating the overall framework and architecture of the smart city [12]. The framework for developing this infrastructure and the spatial accuracy of asset positioning, as the basis of the smart city development architecture that is integrated with all facilities and systems, are linked to the overall framework of the smart city.

It is worth noting that the United Nations (UN) does not officially use the term "smart city" because the concept is still evolving and is often perceived by private companies as a branding strategy [13]. Instead, the United Nations Urban and Cultural Agenda emphasizes the need to make cities "more inclusive, safe, resilient and sustainable"; principles that embrace the values, cultural and historical characteristics that some

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

cities have inherited since their inception and evolution.

2.2 Collaboration

Smart cities are being explored as platforms for open innovation and user-centered approaches to test and validate future research, Internet-based services and urban pilot projects [14]. Effectively harnessing shared resources to shape innovation ecosystems requires the establishment of sustainable partnerships and the development of collaboration strategies among different stakeholders. To this end, professional communities composed of experts from multidisciplinary fields such as architecture, planning, engineering, transportation, utilities, information technology, operations research, social sciences, geography, environmental sciences, finance, public policy, and communications have been formed to promote mutual learning [15]. The result of this process is the emergence of a new urban theory based on extensive and innovative sources of information about near-real-time events in the urban context. This theory seeks to analyze the consequences of information and communication technologies (ICT) on the urban structure and behavioral norms of citizens.

The concept of a smart city is based on a set of shared multidimensional components that include "technology", "people," and "institutions" [16]. Also, the key factors for the success of a smart city initiative have been defined as the integration of infrastructure and technology-based services, social learning to enhance human capital, and strong governance to promote institutional and citizen participation.

2.3. Information and Communication Technology (ICT)

A smart city is defined as a city in which information and communication technology (ICT) is integrated with traditional infrastructure and is coordinated and integrated through new digital technologies [17]. The smart vision is drawn by setting goals, defining research challenges, and considering operational scenarios in different project areas. The concept of smart and connected communities is based on the Internet of Things (IoT), crowdsensing, and cloud computing to provide a comprehensive network of connected devices [18]. In addition, advanced sensors and big data analytics are designed to facilitate the transition from IoT to real-time control. To support this vision, urban IoT uses the most advanced communication technologies to provide value-added services to city management and citizens [19]. This field adapts enabling technologies, protocols and architectures with the most optimal technical solutions and implementation guidelines. Smartphones equipped with sensing technologies such as GPS, gyroscope, microphone, camera and accelerometer [20] also provide innovative services within the framework of smart city architecture. The concept of "Sensing-as-a-Service" is explored from technological, economic and societal perspectives [21]. The research also identifies key challenges, including how to connect ICT to existing IoT infrastructures and cloud-based software platforms and applications. The Future Internet (FI) and its specialized components, namely IoT and Internet of Services (IoS), can act as building blocks to achieve a unified ICT platform at the city scale that transforms the smart city into an open innovation environment [22]. The proposed general implementation is based on the ubiquitous sensor network (USN) model, which meets the requirements of open, federated, and trusted platforms. The main challenge that can hinder the effective support of IoT for the sustainable development of future smart cities is the incompatibility between connected objects and the unreliable nature of related services [23]. In The applications and potentials of big data in smart cities, through the analysis of their data, enable understanding of the urban environment and making immediate changes to solve problems and improve the quality of life of residents [28]. Data must be collected from all networks, devices, and sensors embedded in the infrastructure. After going through various processing stages, using advanced big data analysis platforms and finally outputting in an application platform, this data is transformed into valuable data and helps improve the usability of urban systems. Urban big data flowing from urban sensors will become a vital source of smart city information [29] and will enable long-term strategic planning instead of short-term thinking about how cities operate and manage. Two emerging converging technologies, namely IoT and big data, can make smart cities efficient and responsive [30]. However, these technological advances require integration into the physical infrastructure; Where digital technologies lead to better public services for residents, more efficient use of resources and reduced environmental impacts.

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

2.5. Energy

Hierarchical and centralized energy networks do not meet the needs of smart cities. Smart Grids increase throughput and efficiency by optimizing demand, energy and network access. These networks require security, quality of service (QoS) in data transmission networks and technology standards for interoperability to provide reliable and real-time monitoring information that enables flexible operations [31]. In this regard, information and communication technology (ICT) is a fundamental element in the growth and functioning of smart grids. A reliable and fast communication infrastructure [32] is essential to connect a large number of distributed elements such as generators, distribution substations, consumption points, storage systems and users [33]. Smart grids can also be embedded in frameworks that consider return on investment (ROI) for producers, operators, and customers. These frameworks are divided into three interactive smart components: smart control centers, smart transmission networks, and smart substations [34]. Key challenges of smart grids include communication interoperability between the smart grid and smart meters, as well as reliability, availability, latency, and quality of service (QoS) of the communication network in wireless environments, which are vulnerable to denial-of-service (DoS) attacks [35]. Standardization efforts are underway to harmonize communication standards and protocols across Europe, the United States, and China [36]. A review of smart grids [37] includes three main systems: smart infrastructure, management, and protection. In addition to management objectives such as improving energy efficiency, demand profiling, maximizing utility, reducing costs and controlling emissions, this review also covers smart energy, information, security and communication subsystems.

In addition to smart cities, information and communication technology (ICT) also increasingly requires significant energy for its data centers and communication transmission equipment. Energy Packet Networks (EPNs) use energy storage units to adapt to the irregular supply of renewable energy sources and the intermittent demand of cloud computing servers [38]. The EPN model stores and distributes quantized energy units or energy packets to a wide range of devices based on mechanisms similar to computer networks [39]. Energy packets are managed and optimized by energy distribution centers that receive requests from consumer storage centers that wish to recharge [40].

2.6. Blockchain

Blockchain technology enables the digitization of contracts by providing authentication between parties and encryption of information that is gradually enhanced as it is processed in a decentralized network. Blockchain technology has the potential to transform the banking industry by enabling digital currencies [41], global money transfers, payment solutions [42], smart contracts [43], automating bank records and digital assets [44], and ensuring user anonymity [45]. Blockchain-based decentralized personal data management systems ensure users' personal control over their data [46] and the distribution of digital content governed by user rights [47]. Decentralization is applied to contract management, such as digital rights management [48], by using a consensus method based on reputation scores.

Blockchain has already been applied in smart grids, providing security for energy transactions in decentralized transactions [49], intelligent transportation systems based on a seven-layer conceptual model simulating the OSI model [50], smart devices providing a secure communication platform in a smart city [51], control and configuration of IoT devices [52], smart homes [53] and digital documentation [54].

3. Evolution of Digitalization

Digitalization has gradually been embedded in infrastructures in four distinct stages: Siloed Approach, Shared Network, Shared Workstation and Shared Server.

3.1. Siloed Approach

In its early stages, Information and Communication Technology (ICT) was developed in a siloed approach, in which each digital system operated independently, with its own communications infrastructure, servers, and workstations. Although the early systems were electronic, they were largely

3.2. Shared Network

The first digital systems focused on communication infrastructure. Internet Protocol (IP) and local area networks (LANs) allowed for the transmission of information over shared switches and routers, with each digital system having an associated virtual local area network (VLAN). The advantage of the shared network was the flexibility of the shared cabling,

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

switching, and routing infrastructure, which enabled the protocol independence of IP-based digital systems, as information was transmitted over a shared IP layer 3 and Ethernet layer 2.

3.3. Shared Workstation

The next step in digitalization was the integration of workstations into a single management desktop using system integration software that combined data feeds from different systems and presented a single graphical user interface (GUI) to the user. This integration approach led to the development of management systems that were capable of analyzing data, automating operator tasks, and filtering alarms. In addition, management workstations eliminated the need for a physical presence in the intelligent infrastructure using virtual private networks (VPNs). Remote management decouples control and infrastructure, increasing resilience.

3.4. Shared Server

Finally, server capacity (including CPU and memory) is shared across virtual private or public cloud applications hosted in data centers. Server virtualization eliminates the need to deploy dedicated servers physically installed in the smart infrastructure. Shared servers can be hosted privately in the smart infrastructure's equipment rooms or remotely installed in data centers. The benefits of shared servers include reduced operating expenses (OPEX) and capital expenditures (CAPEX) with simplified management, as server utilization is optimized based on user demand.

3.5. Next Stage

Increasingly, autonomous control centers are integrated into dedicated remote locations with access via virtual private networks (VPNs). Virtual reality (VR), laptops or mobile devices eliminate the need for physical electronics such as phones, video walls or monitors; a human operator does not need to be physically present in the control center to manage the smart infrastructure. Artificial intelligence (AI) will eventually eliminate the need for human presence altogether; management will be done in the same data centers where the servers are hosted.

4. Digital as a Service (DaaS)

Digital as a Service (DaaS) abstracts digital infrastructure from the physical infrastructure features in a cloud environment. DaaS provides a consistent virtual digital infrastructure that creates a higher layer that manages and virtualizes the digital infrastructure. This layer is divided into four elements, which are explained in the following sections: digital systems, transport, servers, and workstations.

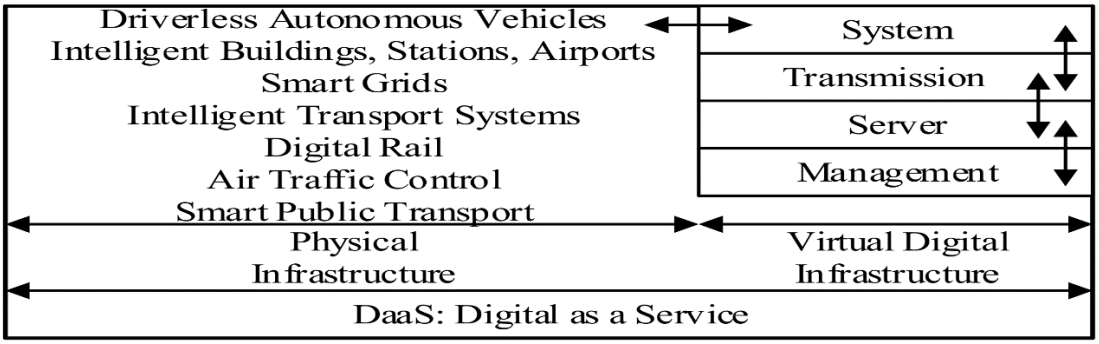

Figure 1. DaaS: Digital as a Service.

Digital systems provide sensors to the physical infrastructure to enable information interaction. Sensor functions range from asset management, industrial processes, and equipment to communication between users via mobile devices. Digital systems will be designed to be physically compatible with the smart infrastructure while providing optimal coverage, flexibility, and performance (Appendix A).

Digital transmission enables communication between sensors using wired solutions such as local area networks (LANs), wide area private networks (WANs), and public Internet service providers (ISPs) or wireless solutions including Global System for Mobile (GSM)/Long Term Evolution (LTE), radio trunking, Wi-Fi, Bluetooth, radio frequency identification (RFID), and near field communication (NFC). Digital transmission technology will be compatible with digital system requirements such as quality of service (QoS), bandwidth, number of users, and coverage.

Digital servers will manage digital systems and transport networks. Data interfaces between servers will enable Internet of Things (IoT), Software Defined Networks (SDN) with Blockchain to provide data security and decentralization when virtualized in the cloud. Higher levels of CPU and memory virtualization will provide greater reliability for smart infrastructure with reduced CAPEX.

Digital management will govern and manage smart infrastructure through system integration, where data

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

received from servers is combined. Higher levels of integration will enable big data analytics for comprehensive management decisions, leading to more efficient management of resources, assets and users to reduce operational costs. Digital management will enable the Digital Twin between the physical and virtual infrastructure.

The digital experience provided by DaaS will abstract digital systems, transport, servers and management . The virtual digital infrastructure will be accessible through a transparent, shared platform that is tailored to the user's function and role.

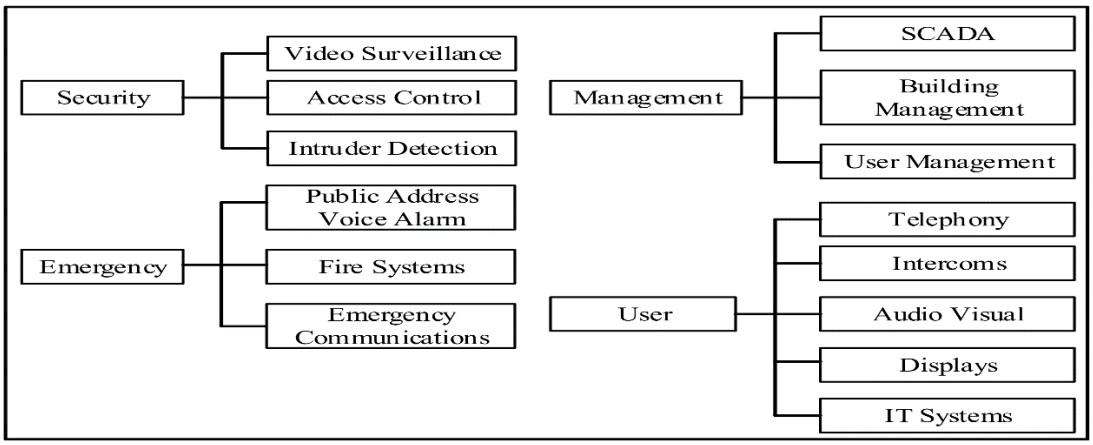

Figure 2. Digital as a Service (DaaS): Digital Experience

, abstracts underlying digital technologies in a cloud environment to provide a flexible, scalable, and interoperable modular virtual digital infrastructure (VDI) where independent physical infrastructure (PI) such as autonomous vehicles, smart buildings, and smart grids are integrated. DaaS defines the virtual digital infrastructure model as follows:

• PI = {PInfrastructure-1, PInfrastructure-2, . . . PInfrastructure-m} as a set a set of m Physical Infrastructures
PInfrastructure;

• VDI = {dvi1, dvi2, . . . dvin} as a set of n dvi vectors associated to one or several Physical Infrastructures PInfrastructure;

• dvi = {vSystem, vTransmission, vServer, vManagement} as a set that consists of the four Virtual Digitalizations; • vSystem = (vSystem-1, vSystem-2, vSystem-p) as a P dimensional vector that represents the Digital Systems; • vTransmission = (vTransmission-1, vTransmission-2, vTransmission-q) as a Q Dimensional vector that represents
the Digital Transmissions;

• vServer = (vServer-1, vServer-2, vServer-r) as a R Dimensional vector that represents the Digital Servers; • vManagement = (vManagement-1, vManagement-2, vManagement-s) as a S Dimensional vector that represents
the Digital Managements.

Theoretically; DaaS enables a single Virtual Digital infrastructure that manages the entire set of physical infrastructures with a modular Virtual Management layer.

Physical Infrastructure (PI)			
Digital System	Digital Transmission	Digital Server	Digital Management
Voice Video Data	Wired Radio Mobile Satellite	CPU Memory Power	Integration Artificial Intelligence User
Virtual System (V_{System})	Virtual Transmission ($V_{Transmission}$)	Virtual Server (V_{Server})	Virtual Management ($V_{Management}$)
Virtual Digital Infrastructure (VDI) Digital as a Service (DaaS)			

Figure 3. Virtual digital infrastructure

5. Digital Systems

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

There are several digital systems or sensors that monitor the smart infrastructure and enable its interaction with the environment. The relevant digital systems are classified according to their functionality.

5.1. Security Systems

Security systems electronically protect and monitor the smart infrastructure against threats, mitigate risks and vulnerabilities, and deter potential attackers.

Closed-circuit television (CCTV) or video surveillance systems (VSS) [55, 56] capture images and video frames of the smart infrastructure for security purposes using video cameras. Video analytics enables the automatic generation of alarms that can be filtered based on priority and event tracking, and retrieve frames with relevant features, such as the user's face. Video streams are typically recorded for crime-proofing purposes. When facial recognition technology is widely used, it could enable the use of images as a biometric tool in conjunction with other identification capabilities such as ticketing.

Access Control [57] manages user access to smart infrastructure via smart cards, mobile app credentials, or user biometrics. Security zones with different priorities are created where physical access is limited to user credentials. Access control also allows for user location tracking in the event of an emergency or evacuation.

Intrusion Detection [58] monitors unauthorized access to smart infrastructure. Primary sensors operate based on physical properties such as infrared, sound, pressure, and volumetric metrics inherent to any physical attacker. A combination of different sensors is usually applied to increase defense in depth.

5.2. Voice and Telephony

5.2. Communication Systems

Telephone systems primarily facilitate voice transmission and enable full-duplex communication between users. However, the use of AI-based and digital call centers can minimize human interaction in processing incoming calls.

Intercom devices allow smart infrastructure users to communicate with security operators or operational personnel, which are mainly used to request access through secure entrances such as parking lots or backyards. These devices usually have an integrated camera for audio and video communication. iPhones act as a backup solution, especially when access control credentials cannot be verified, such as when visitors are absent or their access cards are forgotten. The advent of touchscreens has enabled the integration of card readers with iPhone devices; In this configuration, different buttons can route calls based on priority and destination (such as information or emergency).

Telephones provide voice communication between users. While traditional telephones were standalone devices, the introduction of Session Initiation Protocol (SIP) enabled voice transmission over Internet Protocol (IP) to laptops and mobile devices**.**

5.3. Emergency Systems

Emergency systems are essential for evacuation scenarios, especially in the event of a fire, and are primarily used to direct users in critical situations by emergency services. These systems require strict adherence to standards and technical requirements, including the use of an uninterruptible power supply (UPS) and the use of fire-rated cabling and equipment.

The Public Address/Voice Alarm (PA/VA) system [59] has a dual function. The PA system broadcasts general audio announcements relevant to the purpose of the smart infrastructure, while the VA system provides emergency alerts in critical or fire situations to guide users. Both PA/VA systems are zoned to allow for the broadcast of separate audio information and warnings.

Emergency communication equipment [60] is typically installed in fire escape areas or elevator lobbies to provide communication between users and the fire department in protected environments. These telephones are often fixed, wall-mounted, and connected to a server via digital IP connections.

A fire detection system [61, 62] detects fire using heat or smoke sensors. The system generates audio-visual alerts via lights and sirens, informing users of the occurrence of a fire so that evacuation can begin. When integrated with the voice alarm system, the two systems are directly connected and ensure the automatic activation of intelligible voice alarms upon fire detection.

5.4. Information Systems

Information systems present data to users through visual sensors. The information provided can include navigation data to facilitate navigation within the smart infrastructure, display real-time notifications, or even advertising data for revenue generation purposes.

Audio-visual systems include capabilities such as teleconferencing in meeting rooms, interactive conferencing systems such as smart boards, and multi-purpose audio devices.

Display systems provide the physical screens and data streams to present the required information.

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

This data stream can be generated by the smart infrastructure through the digital media component or can be obtained from sources.

Digital transmission systems in smart infrastructure are implemented with two main technologies: wired communications, which use physical cables for security and higher data rates, but confine sensors to fixed locations; and wireless communications, which provide user mobility and flexibility, but come with limitations in data transfer rates and security.

6.1. Local Area Networks (LANs) and Wide Area Networks (WANs)

Local Area Networks (LANs) [63] are confined to a physical location and provide wired OSI Layer 2 (Ethernet) connectivity to typically fixed sensors such as CCTV cameras or wireless access points. LANs use twisted-pair copper cables (such as CAT) or fiber optics to connect Ethernet devices and switches (Table 1). Additionally, Power over Ethernet (PoE) capability enables simultaneous data and power transmission over a single cable, reducing the need for additional cabling and space.

. Wide Area Networks (WAN)

Wide Area Networks (WAN) (VA, USA, 1981). They interconnect a set of area networks that cover the entire intelligent infrastructure (Table 2). These networks provide IP connectivity at layer 3 of the OSI model for the transport of IP packets and are capable of prioritizing traffic based on quality of service (QoS). WANs are typically connected through Internet Service Providers (ISPs) using a variety of protocols and technologies such as Integrated Services Digital Network (ISDN), Multiprotocol Label Switching (MPLS), Asynchronous Transfer Mode (ATM), and Frame Relay (FR). In addition, the intelligent infrastructure can implement its own private WANs through dedicated routers and routing protocols such as Routing Information Protocol (RIP), Interior Gateway Protocol (IGRP), Open Shortest First Path (OSPF), or Enhanced Interior Gateway Routing Protocol (EIGRP).

6.2. Wireless Local Area Networks (WLAN)

Wireless Local Area Networks (WLAN) (NJ, USA, 2018). Also known as Wi-Fi, provide wireless connectivity at Layer 2 of the OSI model through access points. These access points create wireless channels for users' mobile devices or sensors. WLAN controllers are responsible for managing network configuration and facilitating data roaming between access points and external networks. Service Set Identifier (SSID) allows for the creation of separate WLANs with predefined QoS criteria for different users. Wireless networks carry voice and data and play a fundamental role in changing the way users interact with smart infrastructure, both mobile and location-independent.

6.3. Bluetooth

Bluetooth (Kirkland, WA, USA, 2018). It enables direct connection between devices over very short distances and has been developed as a wireless alternative to cables and RS-232 connectors. Bluetooth networks are Personal Area Networks (PANs) or Piconets that operate in a master-slave configuration. Bluetooth Low Energy (BLE) is used for more precise positioning than GPS, which is used to manage interactions with users in physical space and to transmit location information without the need for a LAN or WLAN.

6.4. Near Field Communication (NFC)

Near Field Communication (NFC) (Geneva, Switzerland, 2013). It allows the transmission of information between just two electronic devices over very short distances (Table 1). NFC devices support Card Emulation, Tag Reading/Writing, and Peer-to-Peer data transfer. NFC technology is used in contactless payment systems, billboards, and collaborative networks by sharing data across smart infrastructure.

Table 1. Near Field Communication (NFC) specifications

Type	Frequency	Data Rate	Power	Range
Active	**13.56**	**106/212/424 Kbps**	**10 mW**	**4–20 cm**
Passive	**MHz**			

6.5. Trunked Radio Networks

Trunked radio networks (Piscataway, NJ, USA, 2018). They provide a two-way radio system that multiplexes user conversations onto multiple dedicated frequencies. These networks enable the use of talk groups and fleet maps for external communications and critical applications in smart infrastructure such as police, fire, and railroads. Due to their low frequency, radio networks offer wide geographic coverage (on a city scale) with reduced infrastructure costs. In addition, radio devices can communicate directly with each other and act as tracking devices for user management.

6.6. Mobile Networks

Mobile networks (Brussels, Belgium, 2017). They support voice and data transmission to user devices such as mobile phones, tablets, and laptops, and enable their connection to the public switched telephone network (PSTN) or an Internet service provider (ISP). These networks provide extensive coverage on a

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

country-wide scale using cells distributed by base stations. Mobile networks perform better than radio networks in larger, more congested environments because they offer more capacity, since the same frequency can be used in different cells. Mobile devices also consume less energy. Mobile networks are very expensive to implement, as they require additional circuit-switched and packet-switched networks for voice and data transmission.

6.7. Satellite Communications

Satellite communications allow for communications between a sender and a receiver at different locations on Earth. Satellites receive, amplify, and rebroadcast radio signals. This type of transmission requires line-of-sight, which can be hindered by the curvature of the Earth. Satellite communications are used for smart infrastructure to connect two remote locations where physical cabling is not possible (such as deserts or islands). They are also used in television, telephone, Internet, GPS, and other security applications.

7. Digital Servers

In addition to managing the status of physical equipment and sensors, digital servers also control the quality of service (QoS) of digital transmissions and service level agreements (SLAs). These servers are logically interconnected, enabling system integration and data analysis through digital interfaces. Digital servers can be installed locally at the physical site of the smart infrastructure or hosted in centralized data centers, either private or public clouds. Autonomous smart devices (such as vehicles, trains, and airplanes) will also have dedicated integrated servers that leverage Edge Computing solutions.

7.1. Server Virtualization

Servers must operate at high speed and without interruption, and have high availability and reliability. Server virtualization enables more efficient use, lower costs, and increase reliability by sharing hardware and software resources. Virtual servers are typically hosted on modular blade servers and managed by hypervisors that separate the virtual server from the physical hardware.

7.2. Storage Virtualization

Memory and storage can be virtualized as blocks, providing a logical memory of physical storage resources using Fibre Channel or iSCSI protocols. In addition, file virtualization eliminates the dependency between physical storage location and data access. Storage Area Networks (SANs) can also be hosted in data centers with intelligent infrastructure servers.

7.3. Software-Defined Networking (SDN)

Software-Defined Networking (SDN) enables efficient network management and configuration, and improves network performance and monitoring on a simple physical infrastructure. SDN separates the data plane (packet transport) from the control plane (packet routing). This technology provides real-time network resources on demand, with automatic load balancing, scalable to meet application and data needs.

7.4. Time Synchronization

Network time synchronization establishes a single reference time for all intelligent infrastructure digital systems, transmission systems, and servers. This is done through the Network Time Protocol (NTP) or the Precision Time Protocol (PTP), which achieve millisecond or microsecond accuracy from Coordinated Universal Time (UTC), respectively. Time synchronization is based on a layered hierarchy, where layer 0 is the high-precision reference clock (synchronized with atomic clocks, GPS, GNSS or radio sources) and the lower layers are related to the topology of digital transmission equipment.

8.Digital Management

The data and information collected by the sensors of digital systems, transmitted by the digital transmission infrastructure and processed by digital servers are managed in real-time by the digital management layer of the smart infrastructure. This management covers the status of all components of the smart infrastructure, including sensors, digital systems, transmission infrastructure and processing servers.

Digital management provides a hierarchical layer of software, middleware, and application programming interfaces (APIs). This l This layer facilitates system integration, Big Data analytics, and alert management with a graphical user interface (GUI) on workstations or mobile applications. The end users of these systems can be humans or artificial intelligence (AI) agents. Given the complexity of the information, effective visual representation through video walls or virtual reality (VR) is essential for accurate human decision-making. However, the advancement of AI will gradually reduce the need for dedicated human equipment.

8.1. Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition (SCADA) Systems (Piscataway, NJ, USA, 2017). Smart infrastructure equipment and assets, including industrial and manufacturing processes, are monitored and managed through programmable logic controllers (PLCs), remote terminal units (RTUs), and remote input/output modules (RIOs). Initially, SCADA relied on proprietary protocols such as Modbus and Conitel. Newer versions of standards such as IEC and DNP3 are based on the Transmission Control Protocol/Internet Protocol (TCP/IP) and are vendor-agnostic.

8.2. Building Management (BMS)

Building Management System (BMS) (Gaithersburg, MD, USA, 2018). It controls and monitors the mechanical and electrical equipment of facilities (such as heating, ventilation, and air conditioning - HVAC, lighting, power, elevators, escalators, and fire systems) in smart infrastructure buildings, stations, and airports. Similar to SCADA, early BMS protocols such as C-Bus and Profibus were proprietary. However, the migration to IP has led to the development of open standards such as DeviceNet, SOAP, XML, BACnet and LonWorks. BMS plays a

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

key role in managing the energy consumption of smart infrastructure.

8.3. User Management (UMS)

The User Management System (UMS) (Piscataway, NJ, USA, 2018). It manages the users of smart infrastructure (employees, contractors, customers, passengers) through telecommunications and digital information systems (such as waypoints, VSS surveillance cameras, indoor iPhones, mobile phones, telephones and displays). In emergencies, public address/voice (PA/VA) systems, VSS cameras and mobile phone or radio positioning are used to guide and manage users.

The use of dedicated mobile applications and social media platforms (such as Instagram or Facebook) allows for the personalization and segmentation of user notifications in real time. These notifications can also be sent to selected groups of contacts.

9. Virtual Infrastructure: Challenges and Considerations

The implementation of "Digital as a Service" (DaaS) faces several challenges:

1. Cybersecurity Threats: With the increasing importance of digitalization and big data, cybersecurity threats have increased dramatically. Cybersecurity guidelines cover the layers of the OSI model. The use of proxy servers, firewalls, cryptographic servers, and authentication, authorization, and accounting (AAA) systems can reduce the risk of cyberattacks. Additionally, blockchain technology, with its decentralized model, adds a layer of security and eliminates single points of failure.
2. Competition and Intellectual Property: As digital services become more integrated, companies may not allow access to vendor-independent protocols or interoperability with third-party software to protect their intellectual property and economic interests.
3. Virtualization and Market Competition: Virtualization of infrastructure systems poses economic challenges. Internet service providers (ISPs) or mobile network operators (MNOs) may be reluctant to virtualize their services because it eliminates the need to compete in areas where multiple service providers operate with duplicate equipment.
4. Ownership, Maintenance, and Liability: Digitization and virtualization complicate issues related to ownership and maintenance. The responsibilities and ownership of each stakeholder should be clearly defined. This includes the procurement of equipment and software, as well as the payment of maintenance costs such as energy bills and software upgrades. Lack of preventive maintenance increases the risk of cyberattacks.
5. Cost-Effectiveness: Reducing capital (CAPEX) and operational (OPEX) costs is the main driver of DaaS. The success of this model depends on economic business plans that consider the requirements of stakeholders and users throughout the full life cycle (design, procurement, installation, operations).
6. Dependency on Advanced Technologies: The level of dependence on technologies such as big data, artificial intelligence and machine learning algorithms is increasing. This dependence must be balanced by increasing the reliability, performance and redundancy of services and equipment.

10. Conclusion

This paper has introduced the concept of "Digital as a Service" (DaaS). It virtualizes infrastructure and smart cities at four levels of systems, transport, server and management. Any comprehensive digitalization can be implemented independently of the associated physical infrastructure. DaaS enables a virtual and compatible digital infrastructure. As standalone systems and solutions are becoming smarter, this paper proposes their full connectivity, integration and virtualization at a higher abstraction layer. The fifth industrial revolution, based on the advancement of artificial intelligence, is expected to completely remove humans from operational and management decisions.

The implementation of DaaS brings major challenges. With big data becoming the most valuable asset, it is crucial to protect it from cyberattacks. Also, the commercial and economic interests of different actors need to be managed effectively. DaaS business plans should consider the requirements of stakeholders, users and the entire life cycle (capital and operational costs). Technology is already changing the layout of smart cities, with robotics and automation replacing physical stores in favor of e-commerce, and office and residential spaces are being transformed into mixed-use and collaborative environments. Future trends in smart cities will include the continued automation of transportation with autonomous vehicles and self-managing assets. Infrastructure will become increasingly interconnected as energy needs are digitized in smart grids. Big data will enable citizens and users to benefit from the space, services and structures of a smart city (3S).

International Journal of Innovation Engineering and Technology Development
Vol.2, NO.2 , P:30-43
Received: 20 December 2026
Accepted: 08 March 2026

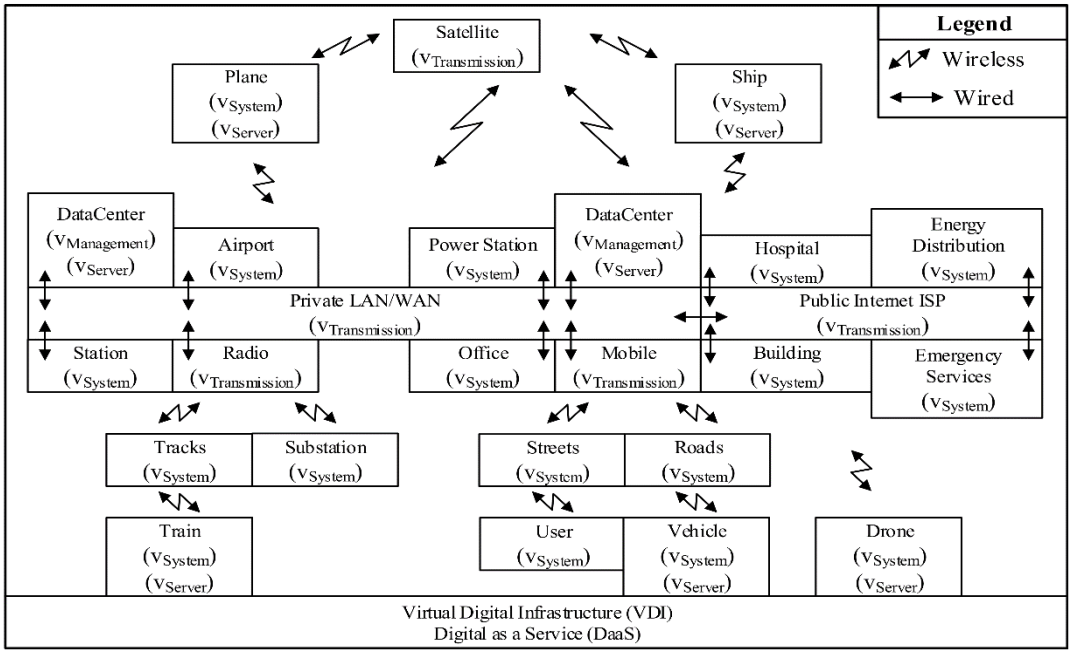

Figure 4. Digital as a Service schematic.

References

1. Kagermann, H. Change through Digitization Value Creation in the Age of Industry 4.0. In Management of Permanent Change; Springer Fachmedien Wiesbaden: Wiesbaden, Germany, 2015; pp. 23–32. [Google Scholar]
2. Astarloa, B.; Kaakeh, A.; Lombardi, M.; Scalise, J. The Future of Electricity: New Technologies Transforming the Grid Edge; World Economic Forum: Geneva, Switzerland, 2017; pp. 1–32. [Google Scholar]
3. Di Silvestre, M.L.; Favuzza, S.; Sanseverino, E.R.; Zizzo, G. How Decarbonization, Digitalization and Decentralization are changing key power infrastructures. Renew. Sustain. Energy Rev. 2018, 93, 483–498. [Google Scholar] [CrossRef]
4. Amini, H.; Boroojeni, K.; Iyengar, S.; Blaabjerg, F.; Pardalos, P.; Madni, A. A Panorama of Future Interdependent Networks: From Intelligent Infrastructures to Smart Cities. Sustain. Interdepend. Netw. Stud. Syst. Decis. Control 2018, 145, 1–10. [Google Scholar]
5. Guedes, A.L.A.; Alvarenga, J.C.; Goulart, M.d.S.S.; Rodriguez, M.V.; Soares, C.A.P. Smart Cities: The Main Drivers for Increasing the Intelligence of Cities. Sustainability 2018, 10, 3121. [Google Scholar] [CrossRef]
6. Schipper, R.; Silvius, G. Characteristics of Smart Sustainable City Development: Implications for Project Management. Smart Cities 2018, 1, 5. [Google Scholar] [CrossRef]
7. Schwab, K. The Fourth Industrial Revolution; World Economic Forum: Geneva, Switzerland, 2016. [Google Scholar]
8. Cocchia, A. Smart and Digital City: A Systematic Literature Review. In Smart City; Springer: Cham, Switzerland, 2014; pp. 13–43. [Google Scholar]
9. Allwinkle, S.; Cruickshank, P. Creating Smart-er Cities: An Overview. J. Urban Technol. 2011, 18, 1–16. [Google Scholar] [CrossRef]
10. Chourabi, H.; Nam, T.; Walker, S.; Gil-Garcia, R.; Mellouli, S.; Nahon, K.; Pardo, T.; Jochen, H.; Chourabi, S. Understanding Smart Cities: An Integrative Framework. In Proceedings of the 2012 45th International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2289–2297. [Google Scholar]
11. Su, K.; Li, J.; Fu, H. Smart city and the applications. In Proceedings of the International Conference on Electronics Communications and Control, Ningbo, China, 9–11 September 2011; pp. 1028–1031. [Google Scholar]
12. Al-Hader, M.; Rodzi, A. The Smart City Infrastructure Development and Monitoring. Theor. Empir. Res. Urban Manag. 2009, 4, 87–94. [Google Scholar]
13. Allam, Z.; Newman, P. Redefining the Smart City: Culture, Metabolism and Governance.

Smart Cities 2018, 1, 2. [Google Scholar] [CrossRef]
14. Schaffers, H.; Komninos, N.; Pallot, M.; Trousse, B.; Nilsson, M.; Oliveira, A. Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. In Proceedings of the Future Internet Assembly, Budapest, Hungary, 17–19 May 2011; pp. 431–446. [Google Scholar]
15. Harrison, C.; Donnelly, I.A. A Theory of Smart Cities. In Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences, Hull, UK, 17–22 July 2011; pp. 1–15. [Google Scholar]
16. Nam, T.; Pardo, T. Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times, College Park, MD, USA, 12–15 June 2011; pp. 282–291. [Google Scholar]
17. Batty, M.; Axhausen, K.; Giannotti, F.; Pozdnoukhov, A.; Bazzani, A.; Wachowicz, M.; Ouzounis, G.; Portugali, Y. Smart cities of the future. Eur. Phys. J. Spec. Top. 2012, 214, 481–518. [Google Scholar] [CrossRef]
18. Sun, Y.; Song, H.; Jara, A.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. IEEE Access 2016, 4, 766–773. [Google Scholar] [CrossRef]
19. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of Things for Smart Cities. IEEE Internet Things J. 2014, 1, 22–32. [Google Scholar] [CrossRef]
20. Balakrishna, C. Enabling Technologies for Smart City Services and Applications. In Proceedings of the International Conference on Next Generation Mobile Applications, Services and Technologies, Paris, France, 12–14 September 2012; pp. 223–227. [Google Scholar]
21. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Sensing as a service model for smart cities supported by Internet of Things. Transa. Emerg. Telecommun. Technol. Spec. Issue Smart Cities Trends Technol. 2014, 25, 81–93. [Google Scholar] [CrossRef]
22. Muñoz, J.H.; Vercher, J.B.; Muñoz, L.; Galache, J.; Presser, M.; Gómez, L.H.; Pettersson, J. Smart Cities at the Forefront of the Future. In Proceedings of the Future Internet Assembly, Budapest, Hungary, 17–19 May 2011; Volume 6656, pp. 447–462. [Google Scholar]
23. Vlacheas, P.; Giaffreda, R.; Stavroulaki, V.; Kelaidonis, D.; Foteinos, V.; Poulios, G.; Demestichas, P.; Somov, A.; Biswas, A.R.; Moessner, K. Enabling smart cities through a cognitive management framework for the internet of things. IEEE Commun. Mag. 2013, 51, 102–111. [Google Scholar] [CrossRef]
24. Li, D.; Cao, J.; Yao, Y. Big data in smart cities. Sci. China Inf. Sci. 2015, 58, 1–12. [Google Scholar] [CrossRef]
25. Strohbach, M.; Ziekow, H.; Gazis, V.; Akiva, N. Towards a Big Data Analytics Framework for IoT and Smart City Applications. In Modeling and Processing for Next-Generation Big-Data Technologies; Springer: Berlin, Germany, 2015; Volume 4, pp. 257–282. [Google Scholar]
26. Al Nuaimi, E.; Al Neyadi, H.; Mohamed, N.; Al-Jaroodi, J. Applications of big data to smart cities. J. Internet Serv. Appl. 2015, 6, 1–25. [Google Scholar] [CrossRef]
27. Abaker, I.; Hashem, T.; Chang, V.; Anuar, N.B.; Adewole, K.; Yaqoob, I.; Gani, A.; Ahmed, E.; Chiroma, H. The role of big data in smart city. Int. J. Inf. Manag. 2016, 36, 748–758. [Google Scholar]
28. Alshawish, R.; Alfagih, S.; Musbah, M. Big data applications in smart cities. In Proceedings of the International Conference on Engineering & MIS, Agadir, Morocco, 22–24 September 2016; pp. 1–7. [Google Scholar]
29. Batty, M. Big data, smart cities and city planning. Dialogues Hum. Geogr. 2013, 3, 274–279. [Google Scholar] [CrossRef] [PubMed]
30. Mohanty, S.P.; Choppali, U.; Kougianos, E. Everything you wanted to know about smart cities: The Internet of Things is the backbone. IEEE Consum. Electron. Mag. 2016, 5, 60–70. [Google Scholar] [CrossRef]
31. Gungor, V.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. Smart Grid Technologies: Communication Technologies and Standards. IEEE Trans. Ind. Informat. 2011, 7, 529–539. [Google Scholar] [CrossRef]
32. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. Comput. Netw. 2011, 55, 3604–3629. [Google Scholar] [CrossRef]
33. Gungor, V.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G. A Survey on Smart Grid Potential Applications and Communication Requirements. IEEE Trans. Ind. Inform. 2013, 9, 28–42. [Google Scholar] [CrossRef]
34. Li, F.; Qiao, W.; Sun, H.; Wan, H.; Wang, J.; Xia, Y.; Xu, Z.; Zhang, P. Smart Transmission Grid: Vision and Framework.

IEEE Trans. Smart Grid 2010, 1, 168–177. [Google Scholar] [CrossRef]
35. Colak, I.; Sagiroglu, S.; Fulli, G.; Yesilbudak, M.; Covrig, Ca. A survey on the critical issues in smart grid technologies. Renew. Sustain. Energy Rev. 2016, 54, 396–405. [Google Scholar] [CrossRef]
36. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities. IEEE Commun. Surv. Tutor. 2013, 15, 21–38. [Google Scholar] [CrossRef]
37. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid The New and Improved Power Grid: A Survey. IEEE Commun. Surv. Tutor. 2012, 14, 944–980. [Google Scholar] [CrossRef]
38. Gelenbe, E. Energy Packet Networks: ICT Based Energy Allocation and Storage. In Proceedings of the International Conference on Green Communications and Networking; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Berlin, Germany, 2011; Volume 51, pp. 186–195. [Google Scholar]
39. Gelenbe, E. Energy packet networks: Smart electricity storage to meet surges in demand. In Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques, Sirmione-Desenzano, Italy, 19–23 March 2012; pp. 1–7. [Google Scholar]
40. Gelenbe, E. Energy packet networks: Adaptive energy management for the cloud. In Proceedings of the 2nd International Workshop on Cloud Computing Platforms, Bern, Switzerland, 10 April 2012; Volume 1, pp. 1–5. [Google Scholar]
41. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008; pp. 1–10. Available online: Bitcoin.org.
42. Peters, G.; Panayi, E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money. In Banking Beyond Banks and Money; New Economic Windows Springer International Publishing: Cham, Switzerland, 2016; pp. 239–278. [Google Scholar]
43. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016; pp. 839–858. [Google Scholar]
44. Beck, R.; Stenum, J.; Lollike, N.; Malone, S. Blockchain The Gateway to Trust-Free Cryptographic Transactions. In Proceedings of the European Conference on Information Systems, Istanbul, Turkey, 12–15 June 2016; pp. 1–14. [Google Scholar]
45. Heilman, E.; Baldimtsi, F.; Goldberg, S. Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. In Proceedings of the International Conference on Financial Cryptography and Data Security Financial Cryptography and Data Security; Springer: Berlin/Heidelberg, Germany, 2016; pp. 1–15. [Google Scholar]
46. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the Security and Privacy Workshops, San Jose, CA, USA, 21 May 2015; pp. 180–184. [Google Scholar]
47. Kishigami, J.; Fujimura, S.; Watanabe, H.; Nakadaira, A.; Akutsu, A. The Blockchain-Based Digital Content Distribution System. In Proceedings of the IEEE Fifth International Conference on Big Data and Cloud Computing 2015, Dalian, China, 26–28 August 2015; pp. 187–190. [Google Scholar]
48. Watanabe, H.; Fujimura, S.; Nakadaira, A.; Miyazaki, Y.; Akutsu, A.; Kishigami, J. Blockchain contract: Securing a Blockchain applied to smart contracts. In Proceedings of the International Conference on Consumer Electronics, Las Vegas, NV, USA, 7–11 January 2016; pp. 467–468. [Google Scholar]
49. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams. IEEE Trans. Dependable Secure Comput. 2016, 15, 1–14. [Google Scholar] [CrossRef]
50. Yuan, Y.; Wang, Fe. Towards Blockchain based intelligent transportation systems. In Proceedings of the International Conference on Intelligent Transportation Systems, Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668. [Google Scholar]
51. Biswas, K.; Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. In Proceedings of the International Conference High Performance Computing and Communications/Smart City/Data Science and Systems, Sydney,

Australia, 12–14 December 2016; pp. 1392–1393. [Google Scholar]
52. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using BlockChain platform. In Proceedings of the International Conference on Advanced Communication Technology, Pyeongchang, Korea, 19–22 February 2017; pp. 464–467. [Google Scholar]
53. Dorri, A.; Kanhere, S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the Pervasive Computing and Communications Workshops, Big Island, HI, USA, 13–17 March 2017; pp. 1–6. [Google Scholar]
54. Serrano, W. The Random Neural Network with a BlockChain Configuration in Digital Documentation. In Proceedings of the International Symposium on Computer and Information Sciences, Poznan, Poland, 20–21 September 2018; pp. 196–210. [Google Scholar]
55. Cohen, N.; Gattuso, J.; MacLennan Brown, K. CCTV Operational Requirements Manual; Publication No. 28/09; Home Office Scientific Development Branch: St. Albans, UK, 2009. [Google Scholar]
56. BS EN 62676. Video Surveillance Systems for Use in Security Applications; European Union: Brussels, Belgium, 2018. [Google Scholar]
57. BS EN 60839. Alarm and Electronic Security Systems. Electronic Access Control Systems. System and Components Requirements; European Union: Brussels, Belgium, 2013. [Google Scholar]
58. BS EN 50518. Monitoring and Alarm Receiving Centre. Technical Requirements; European Union: Brussels, Belgium, 2014. [Google Scholar]
59. BS 5839-8. Code of Practice for the Design, Installation, Commissioning and Maintenance of Voice Alarm Systems; European Union: Brussels, Belgium, 2013. [Google Scholar]
60. BS 5839-9. Code of Practice for the Design, Installation, Commissioning and Maintenance of Emergency Voice Communication Systems; European Union: Brussels, Belgium, 2011. [Google Scholar]
61. BS 5839-1. Fire Detection and Fire Alarm Systems for Buildings. Code of Practice for Design, Installation, Commissioning and Maintenance of Systems in Non-Domestic Premises; European Union: Brussels, Belgium, 2017. [Google Scholar]
62. BS EN 54. Fire Detection & Alarm Systems; European Union: Brussels, Belgium, 2016. [Google Scholar]
63. IEEE 802.3. Physical Layer and Data Link Layer's Media Access Control (MAC) of Wired Ethernet; IEEE: Piscataway, NJ, USA, 2018. [Google Scholar]
64. RFC 791. Internet Protocol; DARPA Internet Program Protocol Specification; DARPA: Arlington County, VA, USA, 1981. [Google Scholar]
65. IEEE 802.11. Standards for Media Access Control and Physical Layer for Wireless Local Area Network; IEEE: Piscataway, NJ, USA, 2018. [Google Scholar]
66. Bluetooth; Bluetooth Special Interest Group: Kirkland, WA, USA.
67. ISO/IEC 18092. Information Technology Telecommunications and Information Exchange between Systems Near Field Communication; ISO/IEC: Geneva, Switzerland, 2013. [Google Scholar]
68. ETS/EN 300 392. Terrestrial Trunked Radio TETRA-Voice + Data; European Union: Brussels, Belgium, 2017. [Google Scholar]
69. IEEE 802.16. Standards for Broadband for Wireless Metropolitan Area Networks; WirelessMAN and WiMax; IEEE: Piscataway, NJ, USA, 2017. [Google Scholar]
70. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.