sustainability

MDPI

Article

Future Development of Taiwan's Smart Cities from an Information Security Perspective

Shiann Ming Wu [1], Dongqiang Guo [1], Yenchun Jim Wu [2,*] and Yung Chang Wu [1]

[1] College of Business Administration, National Huaqiao University, Quanzhou 362021, China; wuming@cute.edu.tw (S.M.W.); gdq@hqu.edu.cn (D.G.); Jasonwu988@gmail.com (Y.C.W.)

[2] Graduate Institute of Global Business and Strategy, National Taiwan Normal University, Taipei 10645, Taiwan

* Correspondence: wuyenchun@gmail.com; Tel.: +886-2-7734-3996

Received: 11 November 2018; Accepted: 28 November 2018; Published: 30 November 2018

Abstract: Smart cities are primarily based on information and communications technology development and applications across various academic subjects and domains. Integrating new-generation information and communications technologies, including the Internet of Things data collection, cloud computation, big data applications, and mobile network, smart cities organize the people and things of a city according to application needs to perform real-time computation and processing. Information transmission must be rapid and reliable to protect personal privacy and to secure data. All types of information security problems can lead to disastrous consequences; in particular, they pose great challenges to traditional information security systems. To explore possible solutions to the challenges that Taiwan's smart city information security faces, this study used the enterprise architecture method and discussed the emphasis and investment capacity of the government and enterprises on information security. Moreover, this study reviewed correct methods of using a smart information security collaborative system to protect not only privacy, however also networks with a large attack surface; the purpose was to establish a reliable data sharing practice and alleviate the cascading effect of failures of smart networks. Finally, this paper provides future research directions for building smart cities and encouraging further explorations in this domain. It is hoped that smart cities can conduct overall planning for information security during the process of construction. Future researchers will be able to propose more effective solutions for smart city information security while developing information and communication technologies.

Keywords: smart city; information security; cloud computation security; big data information security; Internet of things information security

1. Introduction

In the report "Transforming Our World: The 2030 Agenda for Sustainable Development", the United Nations announced its Sustainable Development Goals (SDGs), which cover economic development, quality of life, human resource education, infrastructure, distributive justice, green energy development, and a sustainable environment. The United Nations set the target of 2030 to achieve the SDGs [1].

The white book of the Global Future Cities Industry Alliance delineates the connotation of smart cities to using information and communications technology (ICT) to achieve sustainable city development and to improve people's quality of life, as well as using data to create insights [2]. Built on an ICT infrastructure, smart cities take advantage of the Internet of Things (IoTs) for information collection, as well as big data mining and analysis, and cloud computation, which are the three major cores and applications of IC [3,4].

Taiwan's government has promulgated various policies on information security to provide directions for building the information security systems of Taiwan's smart cities. The smart city concept, based on integrating and using the new generation of ICT, offers a new mode of development for future cities [5]. However, it is crucial to recognize that smart cities pose severe challenges to conventional information security systems; any type of information security problem can lead to disastrous consequences and greatly affect people's livelihood [6].

1.1. Overall Structure of Smart Cities

The building of smart cities must be based on an elevated macro-level perspective, as well as on multidimensional integration, which includes technology, public infrastructure, data, services, security protection, and human resources. The integration of these various application domains must be considered when setting up smart city systems with a unified platform, city operations center, and a perception–network–platform-incorporated smart network that can grow and expand and is sustainable [7]. To ensure the effective construction and operation of a smart city, well-defined top-down smart city development goals should be defined; simultaneously, it is critical to build smart infrastructure, achieve highly effective information system operations, and establish an effective network and information security protection system and supporting infrastructure. This structure is shown in Figure 1 [8]. The ultimate goal is to achieve sustainable city development for convenient public services, refined city management, a suitable living environment, smart infrastructure, and long-term information security [9].

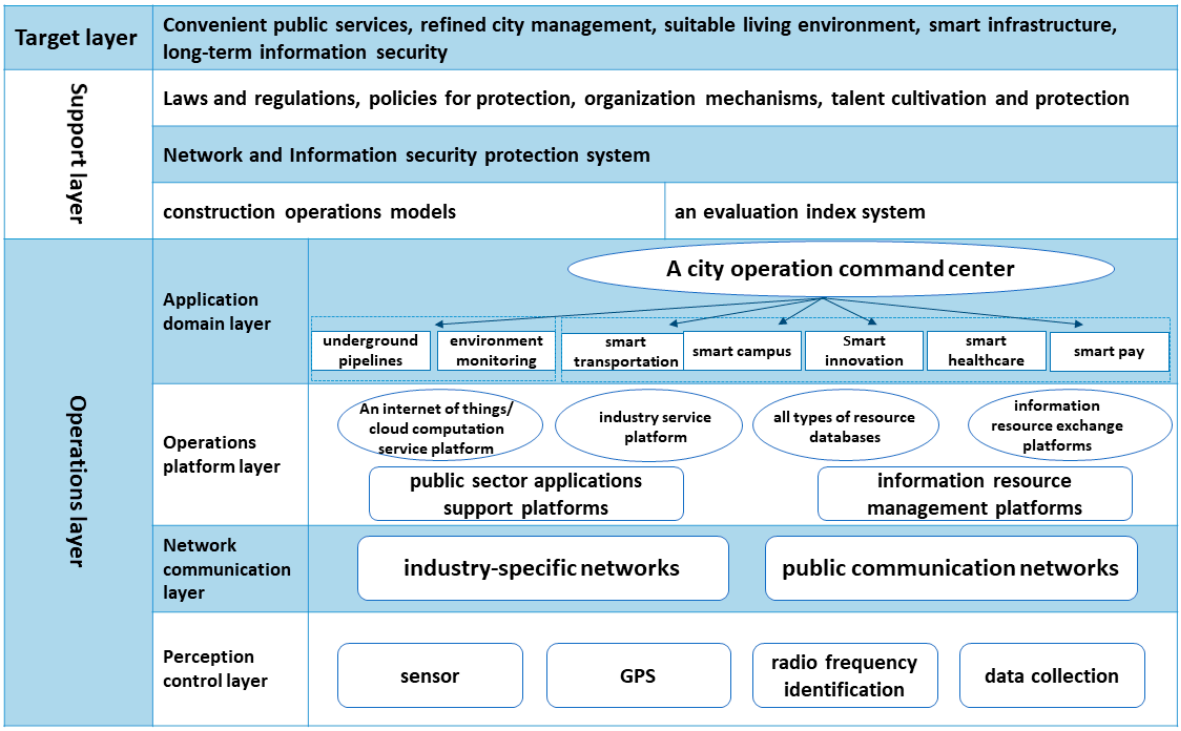

Figure 1. Top layer framework of a smart city.

1.1.1. Target Layer

To improve people's overall sense of well-being and Taiwan as a whole, the Taiwanese government has worked at its full capacity to comprehensively promote national construction. In addition, according to the SDGs and the spirit of inclusive development, the government has set the following five major goals for building Taiwan's smart cities: stimulating cultures, promoting green high-technology industries, building a smart country, achieving social justice, and creating a happy living environment [10].

1.1.2. Support Layer

Information security protection and supportive laws and regulations are essential for constructing a smart city. The government should plan and set up a smart city security protection system based on unified standards and should coordinate smart information security measures and resources. It is crucial to build a comprehensively planned smart city security framework with a definite structure, as well as protect and support the framework in all dimensions through laws and regulations, standards and specifications, organization management, technology, infrastructure, and manpower cultivation. Another crucial task is to establish evaluation indicators, assessments, and construction and operations models to provide a complete foundation and support for smart city development. The principles of the Information Assurance Technical Framework (IATF) should be adopted as guidelines for building a smart city security protection system that covers the three areas of people, technology, and operations [11].

1.1.3. Operations Layer

The operations layer is the core of smart city operations. Unified standards and specifications should be established for building smart infrastructure, a highly effective information system, and constructing supporting platforms for cloud computation and big data, thereby optimizing and integrating resources in areas such as city operations, city management, and smart industries. In addition, city management and operations procedures should be set to provide smart economic development and effective and convenient smart services for the public. The operations layer is focused on comprehensive ICT applications and can be divided into four sublayers: perceptual control, mobile network, supporting platform, and application domain [4].

The perpetual control layer primarily comprises the end-point perceptual infrastructure. Data related to the operations and states of a city's big data are digitalized and informatized to provide numerous end-point perceptual capabilities as well as interactive capability between the public and enterprises. As for information sharing, information is transparently transmitted through the network communication layer to the city's supporting platform. The mobile network layer is a crucial part of smart city infrastructure that comprises high-speed, ubiquitous, and highly reliable wired optic fiber networks and wireless broadband networks. Its key function is to set the foundation for realizing smart city applications and high-speed information transmission. The supporting platform layer mainly comprises an information resource management platform and a public sector applications platform. With extensively deployed perceptual end-points and peripheral perceptual capability, smart cities will be able to generate a massive volume of data and information that requires not only information databases, however also secure and effective data management. Moreover, public-oriented IoT, cloud computation, and industry-based public service platforms will be available for users from various industries, and smart city core public capabilities will be developed [12]. The fourth and final layer is the application domain layer, which provides smart cities with convenient public services, refined city management, a suitable living environment, smart infrastructure, and other application and information systems based on long-term information security. It is critical to simultaneously aggregate and interconnect data from the information systems of various institutions and government agencies to construct a smart city operations command center.

Information security working space demarcation and protection strategies of the operations layer are described in detail in Section 2.1.

1.2. Smart City Construction in Taiwan

In 2017, Taiwan launched a project called Development, Innovation, Governance, Inclusion, plus, or DiGi+, to achieve the following three fundamental digital nation supportive measures: establishing a friendly legal environment, cultivating multidisciplinary digital talent, and promoting advanced digital technology. The ultimate goal is to create a safe and reliable digital and innovative infrastructure

environment and a digital government in a network society [13]. The critical infrastructure includes the energy, water resources, high-technology parks, communications and broadcasting, transportation, banks and financial institutions, emergency rescue, and hospitals of central as well as local governments [3]. Simultaneously, large funds, partly from nongovernmental sources, are to be invested into building ultra-broadband networks for the information society infrastructure.

1.3. Smart City Information Security Framework

The information security specifications from the National Institute of Standards and Technology (NIST) have been applied by countries worldwide. According to the NIST, organizations should adopt a top-down information security management structure, enabling continuous feedback to reduce information security risks [14]. The US Federal Enterprise Architecture Framework (FEAF) [15] covers the five dimensions of businesses, data, applications, performance, and technology, and provides public structures that facilitate the coordination of public business procedures, technology introductions, information flows, and system investments among federal agencies. Furthermore, the framework lists the principles and goals of information security and provides directions for interoperability, open systems, public access, end-user satisfaction, and security problems among various domains. The information security management guidelines of ISO27001 [16] and of the Information Technology Infrastructure Library (ITIL) are focused on constructing, implementing, operating, monitoring, reviewing, maintaining, and improving information security based on the essence of plan–do–check–act or plan–do–check–adjust (PDCA) to achieve information security using an organized approach. The IT management structuralized method of the IT service domain has been widely accepted. Information technology service management (ITSM) has been developed for integrating people, processes, and tools [17]. Whether from the perspective of the best practices of ITIL or ISO, the goal is for smart cities to offer the highest information service quality built on accumulated and shared experiences.

ISO/IEC 27001 provides the most standard and complete risk analysis and processing procedures to assist organizations in establishing a complete information security management system in order to effectively solve current asset security problems and reduce the risks that information security management may encounter in the future. ITIL® is a framework for standardizing IT service management. It utilizes processes to optimize existing resources that enhance the level of IT services and combines with business purposes to prove the value of IT organizations for enterprises.

Smart city information security is pluralistic, and under the NIST's information security specifications, a comprehensive smart city information security structure can be built to complete the long-term information security of a smart city, covering the three areas of information security technology, operations, and the management system. These are based on the essence of the IATF and the FEAF framework, simultaneously incorporating ISO27001 PDCA as advanced management standards and the best practice guide of ITIL/ITSM.

2. Information Security

In the 2017 Global Risks Report of the World Economic Forum, data fraud or theft ranked fifth worldwide and large-scale cyber-attacks ranked sixth. This indicates that information security has deeply affected people's lives [18]. The Global State of Information Security Survey 2018 by PricewaterhouseCoopers showed that more than 40% of enterprises globally lack a comprehensive information security strategy [19]. When risks increase substantially because of complex systems, the real danger is no longer more damages, however it becomes runaway collapses or an abrupt transition to a new yet suboptimal condition [18]. Smart cities are closely related to various sectors and the livelihood of people. As a result, a complete information security concept is essential. To increase the breadth, depth, and speed of information security, the Taiwanese government has planned to incorporate big data analysis and artificial intelligence (AI) technology to structure a smart information collaborative system for government agencies, critical infrastructure, and the regional governance of

local governments. Such a system will be capable of forecasting the trends of information security attacks, thereby improving the speed of responses to information security incidents [20].

2.1. Scope of Smart City Information Security

Smart cities are composed of different information technology objects. Through systemic software/hardware and service integration, smart cities enable people to perceive, decide, and act according to the various application and scenario requirements. During the construction of smart cities, conventional information security technology will remain crucial and irreplaceable. The conventional classification, demarcation, and key protection strategies are still useful in the construction of a smart city's information security technology system. Simultaneously, the IATF will continue to provide the highest guiding principles. According to the smart city information procedure, five information security working spaces are demarcated (see Figure 2) [4,21]. The information security is responsible for authorization, verification, and encryption tools. Kerberos is a network authentication protocol used for secure identity authentication of personal communication on insecure networks. Lightweight Directory Access Protocol (LDAP) is an open, neutral, and industry-standard application protocol that uses IP protocol to control access and maintain the directory information of distributed messages. Guardium automates all compliance workflows in a heterogeneous environment to ensure the privacy and integrity of reliable information in the data center [4].

Intelligent Operations Center (I.O.C.) is a service monitoring platform for smart cities that can monitor the operations of a smart city information system at any time and can be processed by operators in real time. The Smart City Data Center is equipped with smart city-related information entity equipment and a traditional enterprise information center, which is similar to the traditional enterprise information center. Information security is the core that must be targeted under the operation of smart cities. In Figure 2, we only outlined several products that are commonly used in the industry, such as Kerbero, LDAP, ThreatSonar, Guardium, etc. These have been included in Table 1.

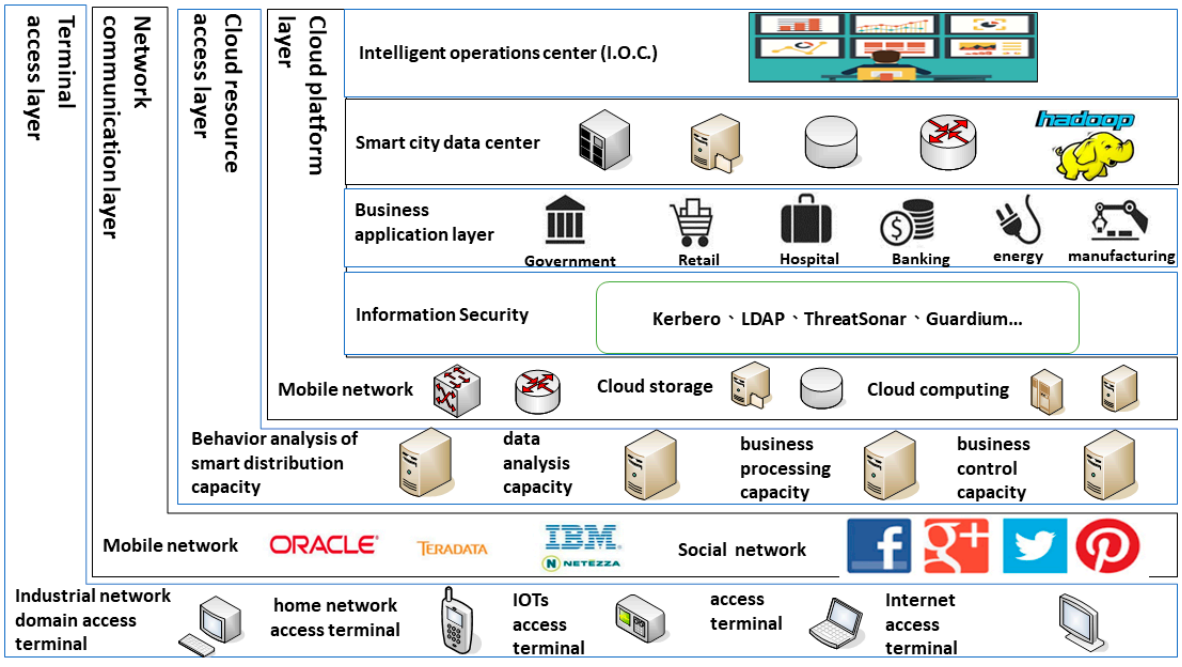

Figure 2. Smart city security demarcation layer map.

Information can be accessed from various types of terminal access layer (including end-user terminals of IoT devices and the smart city information system). Next, information reaches the data and service supporting layer of the smart city technology system, which comprises the data and service supporting layer and the cloud platform layer, through the border of the mobile network

communication layer and the cloud resource access layer, to drive the operation of the overall information flow. The whole process involves the IoT, mobile networks, cloud computation, big data, and other ICT domain-related security issues. See Table 1 for more details.

Table 1 shows the business application system paired with the business application layer. This application system operates in the cloud platform virtual environment. It implements rigorous access control, invasion detection, action and behavior audits, digital identity authentication and identification, scanning for security vulnerabilities, and other safety measures. Similarly, cloud platforms, cloud resources, and the network communication layer must be strictly controlled. The terminal access layer requires much more stringent virus filtering, alarm and isolation, terminal access authorization, terminal security management, field control, application layer filtering defense, IoT security defense, and other control measures.

Table 1. Smart city security working space demarcation and security protection strategies.

Information Security Working Domain	Applications Involved	Basic Information Security Protection Strategies
Business applications	All types of smart applications, user data, network data, business data, and big data	Access control, invasion control, and action and behavioral audits are rigorously implemented, and digital certificates are used for identity certification, identification, and scanning for vulnerabilities.
Cloud platform	Cloud storage, cloud computation, cloud networks, cloud resources, and big data	Protection is implemented according to the 13 critical domains listed in the Cloud Security Alliance cloud computation security guidelines.
Cloud resource access layer	Cloud resource controllers, load balancer, bandwidth aggregation, and distributed storage	Access control, invasion control, and action and behavioral audits are rigorously controlled, and digital certificates are used for identity certification and identification. Furthermore, application layer protection and data recovery are implemented.
Mobile network communication layer	Communication links, wide area network access devices, and wireless base station devices	Rigorous access control, invasion detection, and encrypted transmission are implemented to ensure network communication security.
Terminal access layer	Desktop terminals, mobile terminals, IoT (Internet of Things) sensor terminals, and smart electric appliances	Virus filtering, alarm and isolation, terminal access, terminal security management, field control, application layer filtering defense, and IoT security defense.

2.2. Cloud Computation Security

Commonly based on the dynamic, easily expandable functions, and virtual resource services provided by the Internet, cloud computation enables users to share platform resources. Data centralized in the shared data center and storage devices pose a threat to data securities. On 28 July 2017, the Cloud Security Alliance (CSA) issued the Security Guidance for Critical Areas of Focus in Cloud Computing Version 4.0 (CSA. V4.0) [22] and listed 13 critical areas of cloud platform layer security that require protection management. Under the existing information security standards, various related international organizations have individually started to adopt cloud computation information security measures. In this study, the key information is summarized for the following three categories: information security guidelines, application standards, and technical standards (see Table 2).

Table 2. Summary of cloud computation information security management standards.

Type	Name	Description
Information security guidelines	Cloud computation security guidance	CSA. V 4.0
	Guidelines for Improving Security and Privacy in Public Cloud, NIST (National Institute of Standards and Technology, Special Publication).	NIST SP 800-144
	27017 and 27018 for cloud computation data and privacy protection standards, the International Organization for Standardization (ISO).	ISO 270xx
	Business continuity management system (BCMS).	ISO 22301
Application standards	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy provisions for medical facilities and subcontractors.	HIPAA
	Data security check provisions for financial institutions, Federal Financial Institutions Examination Council (FFIEC).	Finance FFIEC
	Information privacy provisions for credit card and debit card information, the PCI (Payment Card Industry) Security Council.	PCI
	SAS 70 (the Statement on Auditing Standards No.70) for performing risk control audits of financial institutions and of institutions providing information services.	SAS 70
Technical standards	Key and certificate management: KMIP (Key Management Interoperability Protocol) and PKCS (Public Key Cryptography Standards).	KMIP stands for the Key Management Interoperability Protocol, whereas PKCS stands for Public Key Cryptography Standards.
	Information storage security: The Institute of Electrical and Electronics Engineers (IEEE) P1619.	Data storage encryption method and key management structure, the Security in Storage Working Group of IEEE.
	Identity authentication: SAML (Security Assertion Markup Language) and X.509 certificate.	SAML stands for Security Assertion Markup Language; Public key management and infrastructure (X.509 authentication) of the International Telecommunication Union Standardization Sector.

When evaluating security based on cloud computation, a key feature is that enterprises lose their physical control; the security infrastructure, platforms, and application programs are directly controlled by cloud suppliers. The primary security concern is legal compliance and the secondary concern is safety control. Although consumers may require all these security control measures, they should contemplate whether cloud suppliers' infrastructure is capable of providing comprehensive security protection [23].

2.3. Big Data Security

The contextual integrity principle of Helen Nissenbaum (2004) provides a conceptual or strategic framework to resolve privacy issues related to big data [24]. Data analysis technology concerns using data inputs, processing and computation analysis, and other programs with support from ICT technologies such as cloud computation and the Internet to generate computation results [25]. The Big Data Working Group of the CSA published the Expanded Top 10 Big Data Security and Privacy Challenges and the Big Data Analytics for Security Intelligence [26,27], the contents of which can be classified into the following four categories: infrastructure safety, data privacy, data management, and integrity and reactive security. More details are summarized in Table 3.

Table 3. Big data safety, privacy categories, and 10 major challenges.

Category	Ten Major Challenges for Big Data Security and Privacy
Infrastructure safety	Decentralized computing architecture security; Security best practices in nonrelational data stores.
Data privacy	Data mining and analysis of privacy protection; Data security with boosted cryptography; Refined access control.
Data management	Data storage and transaction record security; Refined audits; Data source.
Integrity and reactive security	Terminal input authentication and filtering; Real-time security monitoring.

The first category, infrastructure safety, can be divided into decentralized computing architecture security and security best practices in nonrelational data stores. Decentralized computing architecture security uses network interconnection for data transmission, communication, and coordination; some notable considerations here are critical security problems such as data leaks, privacy breaches, and incorrect computation results. For example, the MapReduce architecture divides data into multiple blocks; each block is first processed by the Mapper before the Reducer generates the result by clustering values of the same key. This procedure protects the security of Mapper programs and the data. In terms of security best practices in nonrelational data stores, because of a wide variety of big data sources and the complicated format types, security policies related to data classification and storage are essential for security and protection.

The second category, data privacy, faces the following three challenges: privacy-preserving data mining and analytics, cryptographically enforced data-centric security, and granular access control. In the process of automatically searching information with special relevance hidden in a massive amount of information, mining and analysis becomes extremely difficult because the information is often deidentified. For the security of sensitive or important data, attribute-based encryption is often adopted to ensure that access to the data is limited to authorized personnel [28]. Access control must be refined further to completely block nonauthorized parties from accessing the data.

The third category, data management, also faces three challenges: secure data storage and transaction logs, granular audits, and data provenance. The amount of big data is not only enormous, however it is also expanding rapidly; as a result, data saving strategies must meet security needs. In addition, the audits must be refined further to detect any potential information security risks or invasions. Data source reliability is another key concern here because inappropriate data will lead to incorrect analysis results.

For the fourth category, integrity and reactive security, two related issues must be tackled: end-point input validation and filtering and real-time security monitoring. For the various types of terminal device, it is important to study related algorithms and filter out malicious sources to ensure the validity of data sources. When applying the massive amount of information from big data, using the smart collaborative defense system [29,30] for real-time security monitoring enables administrators to handle a crisis immediately, accelerating the response to information security incidents effectively.

2.4. Mobile Network Security

According to the definition provided in the Regulations for Administration of Mobile Communications Business by the National Communications Commission, R.O.C., mobile communications refers to the use of radio terminal equipment for voice or nonvoice communications through a mobile communication network [31]. The term "mobile communication system" refers to a communication system composed of mobile stations, base stations, switching equipment, network management, and accounting management. A mobile communication network consists of a mobile communication system and

telecommunication line equipment. Cellular technology has become increasingly influential in mobile communication networks because for the majority of people, cellular technology is the main portal to the Internet. Lastly, a mobile communication network should be equipped with an effective switch certification protocol in terms of security and effectiveness [32,33].

As personal wearables and embedded devices rapidly become ubiquitous, the number of networks—large and small and of varying levels of complexity—are certain to multiply substantially [34]. Cisco suggested that with the use of IP network-based platforms for linking various mobile devices, networks, and applications, users will be able to access various information and keep in touch with others at any time and in any place. Centralized, easy-to-manage access points and highly secure mobile solutions can integrate voice, information, image, and wireless transmission into one infrastructure, overcoming the limitations of conventional communication and enhancing the effect of collaboration. It is known that blurring the boundary between work and personal activities has positive effects on both work productivity and the flexibility of applications in everyday life.

2.5. IoTs Security

The susceptibility of the IoT to all sorts of attacks has increased; incidents such as hacker invasions to store or control IoT equipment or systems have been frequently reported. People can be given a specific level of trust at different parts of the IoTs [35]. By 2020, according to an estimation by Cisco, more than 50 billion IoT-connected devices and objects will exist [36].

The IoTs is mainly composed of various commonly used devices [37]. The security issues here differ because the work model of IoT equipment varies depending on the application scenario [37]. The International Telecommunication Union Telecommunication Standardization Sector established the Internet of Things Global Standards Initiative and the Focus Group on Machine-to-Machine Service Layer for optimizing IoT special applications based on the international network communication standards protocol. OneM2M, a machine-to-machine (M2M) and IoT-focused international standard organization under the Telecommunications Standards Institute, was set up to handle various IoT applications, including heterogeneous networks and device networking management, data exchange, and information securities. Furthermore, OneM2M defines interface specifications and the data format of various applications to facilitate cross-equipment and cross-application interconnection.

For M2M communication in the IoT domain, each item of equipment "knows" how trustworthy each machine is for important or sensitive information transmission [36]. Trust can be defined using three approaches: determining how many machines can be trusted by a user, determining how trustworthy each other device is, and determining how trustworthy a user is for the device.

The Open web Application Security Project (OWASP) proposed the OWASP Internet of Things Top 10 [38], which lists the 10 major vulnerabilities of and risks to the IoT that should be taken seriously and complied with by industries. Most recent cases of distributed denial-of-service attacks have been mixed attacks; thus, IoT security design will definitely pose certain levels of threats and challenges to smart city information security [39].

3. Constructing Taiwan's Smart City Information Security

Digitalizing the information security industry is one key direction for Taiwan's industry development. The government has requested each critical infrastructure-related competent authority to establish its own industry-related information sharing and analysis center, security operation center, and computer emergency response team, which are the three critical infrastructure platforms of information security. In addition to centralizing the nation's security information, the Executive Yuan set up the Taiwan Computer Emergency Response Team/Coordination Center, which is in charge of integrating nongovernmental information security intelligence and reporting related information security incidents. Mr. Liao Chih-Ming, Director of the aforementioned center, stated that the value of information intelligence lies in data integration.

3.1. Taiwan's Smart City Information Security

The Personal Data Protection Act, which has been promulgated and implemented since October 2012 in Taiwan, is the core of information security. Due to the severe penalties, government units and enterprises at all levels have vigorously implemented and introduced various international standards, such as ISO27001, ITIL, etc. in order to objectively and effectively assist information security management, information security technology, and information security operation. In the smart city information security safety framework, there are three main information security axes requiring pluralistic consideration. These three domains are information security management, information security technology, and information security operations, and they are essential for achieving long-term information security. Take Taipei City as an example: the smart city construction there has information security at its core, which is encompassed by smart education, smart transportation, smart innovation, smart health care, smart payment, smart public housing, and other smart applications. Participants must follow the government's unified standards and regulations to share the platform and information (see Figure 3) [40].

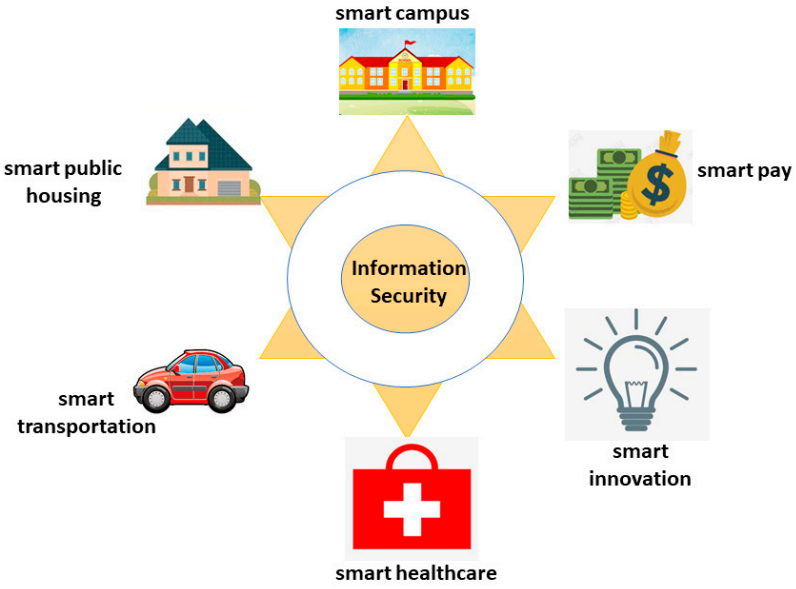

Figure 3. Information security-centered smart city.

3.2. Information Security Investment

According to Cisco's 2017 report [41], more than 55% of enterprises had their information security budget included under their IT budget, whereas 36% of enterprises had information security budgeted under IT. Only 9% of enterprises budgeted security independently (see Table 4). Most enterprises had information security accounting for 11% to 25% of their IT budget. As high as 10% of enterprises did not allocate any budget to information security. In Taiwan, most industries allocate their information security budget to their IT budget, however it is difficult to access such information. These data are often confidential, and enterprises are reluctant to provide detailed information.

Table 4. Percentages of enterprises' information security budgeted under IT.

Security Budget under IT Budget	2014 (Effective Number of Samples, n = 1673)	2015 (Effective Number of Samples, n = 2374)	2016 (Effective Number of Samples, n = 2828)
Fully under IT	61%	58%	55%
Partially under IT	33%	33%	36%
Completely independent	6%	9%	9%

Source: Cisco's 2017 Security Capabilities Benchmark Survey [41].

3.2.1. Investment

According to Gartner's latest forecast (August 2018) [42], the total global expenses of information security products and services will exceed US$114 billion in 2018, which is a 12.4% increase from 2017. It is anticipated that in 2019, the market will undergo a steady growth of 8.7%, reaching US$124 billion. Taiwan's 2018 information security expenses are anticipated to increase by 13.9%, reaching NT$21.8 billion, and information security service expenses will reach NT$9.7 billion. Among various types of product, information security products are the fastest growing, having seen a 21.5% increase, which is equal to approximately NT$1.2 billion. Siddharth Deshpande, Gartner's Research Director, indicated that information security officers are striving to achieve the safe use of technology platforms for their companies to increase their competitiveness and to drive sales. The ongoing technological shortages and the reform of laws and regulations, such as the European Union's General Data Protection Regulation, are driving the steady growth of the information security service market.

According to Taiwan's iThome survey on the percentages and distribution of money invested in information security, all industries in Taiwan have placed significantly more emphasis on information security than ever before [43]. The annual growth rate of the overall information security investment in 2018 has reached 73%. As for key investment items, IT infrastructure protection ranked top (see Figure 4), and authorization, end-points, and data-related control were also high on the list. Unexpectedly, boosting employee information security awareness ranked second, with a percentage of investment reaching 47.9%. This finding suggests that because the government has put much effort into advocating the importance of information security, companies have come to recognize that relying on information security products alone for threat prevention is no longer adequate; personnel information security awareness education and training are required.

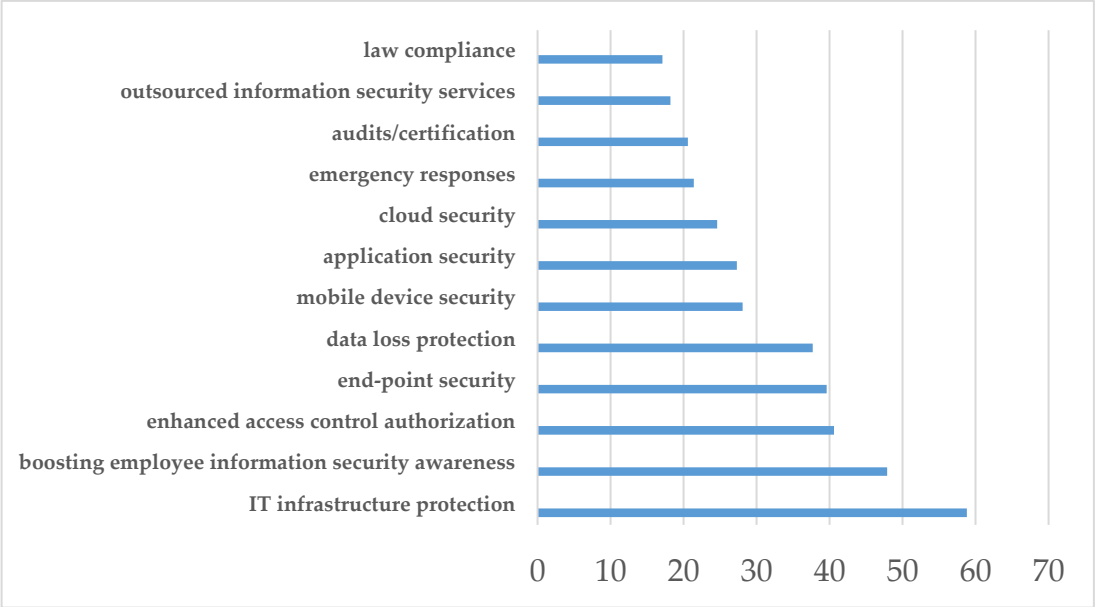

Figure 4. Taiwan's 2018 key corporate information security investment ranking. Source: iThome (2018) [43].

3.2.2. Threats to Information Security

Information security threats are detrimental for enterprises. According to iThome's survey [43], nearly 80% of Taiwanese enterprises that were surveyed experienced information security incidents in 2017, and 15.3% of them had experienced more than 50 information security incidents in that year. In terms of the sources of these information security threats, most were outsider threats: 55.3% were from hackers, 14.7% were related to organized crime, and 7.2% were state-level attacks by foreign

countries. Figure 5 shows the sources of major information security attacks in 2017, in which hackers and internal personnel are seen to pose a certain degree of threat to enterprises in Taiwan.

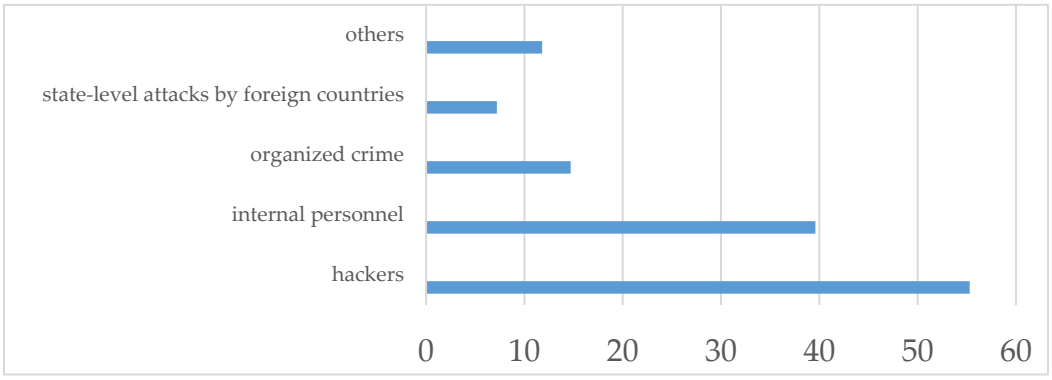

Figure 5. Major sources of information security attacks in 2017. Source: iThome(2018) [43].

Although the threat of external attacks remains, enterprises should also pay attention to insider threats. This survey revealed that among all enterprise information security incidents that occurred in 2017, 39.6% could be attributed to employees. In other words, internal personnel form another major source of threats to corporate information security.

3.2.3. Information Security Obstacles

Cisco's 2018 global survey [41] summarized the 11 largest obstacles to the adoption of advanced security processes and technology (see Table 5, Column A1, A2); each obstacle was organized by the percentage for each country and each region. Among all obstacles, budget constraints ranked first (34%), and compatibility issues with legal systems, certification requirements, and lack of trained personnel ranked joint-second (27%). Organization is not a high-value target for attacks and security is not an executive-level priority ranked in last place. This finding matched the trends of the last two years; first, senior management support is necessary for successful information security operations, and second, hacker organizations have become profit-oriented.

According to data from Taiwan's iThome 2018 Enterprise Information Security Survey [43], employees' lack of knowledge of advanced security processes and technology ranked top (63.1%), budget constraints ranked second (29.9%), compatibility issues with legal systems, certification requirements, and lack of trained personnel ranked joint-third (25–29%), and organization culture of/attitude to security and reluctance to purchase until proven in the market ranked last.

In this study, data from Taiwan's iThome 2018 enterprise information security survey report were reclassified according to items from Cisco's 11 advanced security procedures and technological obstacles (Table 5, Column B) to make comparisons between the two sources. Four items were found to be similar between Taiwan's and Cisco's global averages (with an error rate below 2%). A radar chart was used to compare Taiwan's figures with global averages, and general performance trends were expressed using the advanced security procedure and technological obstacles (see Figure 6). The percentage of employees lacking information security knowledge reached 63.1% (Table 5, Column B), indicating that Taiwanese enterprises in general valued information security, which was a result of the government's efforts. In terms of budget constraints, those of Taiwan were slightly lower than the global average; although Taiwan's information security budget increased, it was still not sufficient. In terms of compatibility issues with legal systems, certification requirements, and lack of trained personnel, Taiwan's values were similar to the global averages; in general, all were inadequate. Regarding reluctance to purchase until proven in the market (9%, Table 5, Column B), organizational culture/attitude (5%, Table 5, Column B) and security is not an executive-level priority (9%, Table 5, Column B), Taiwan had superior performance compared with the global averages, which can be attributed to the government's information security policies.

Table 5. Obstacles blocking the adoption of advanced security procedures or technology (defense weakening).

Item	Global: 2018 Cisco Global Survey		Taiwan: 2018 iThome Survey
	Column A1 2016 (Effective Number of Samples, n = 2912)	Column A2 2017 (Effective Number of Samples, n = 3651)	Column B 2017 (Effective Number of Samples, n = 462)
Budget constraints	35%	34%	30%
Compatibility issues with legal systems	28%	27%	26%
Certification requirements	25%	27%	29%
Lack of trained personnel	25%	27%	27%
Competing priorities	24%	24%	18%
Current workload too heavy to take on new responsibilities	23%	22%	16%
Lack of knowledge about advanced security processes and technology	22%	23%	63%
Reluctant to purchase until they are proven in the market	22%	22%	9%
Organizational culture/attitude about security	22%	23%	5%
Organization is not a high-value target for attacks	18%	18%	19%
Security is not an executive-level priority	17%	17%	9%

Source: cisco.com/go/acr2018 [41] and iThome [43].

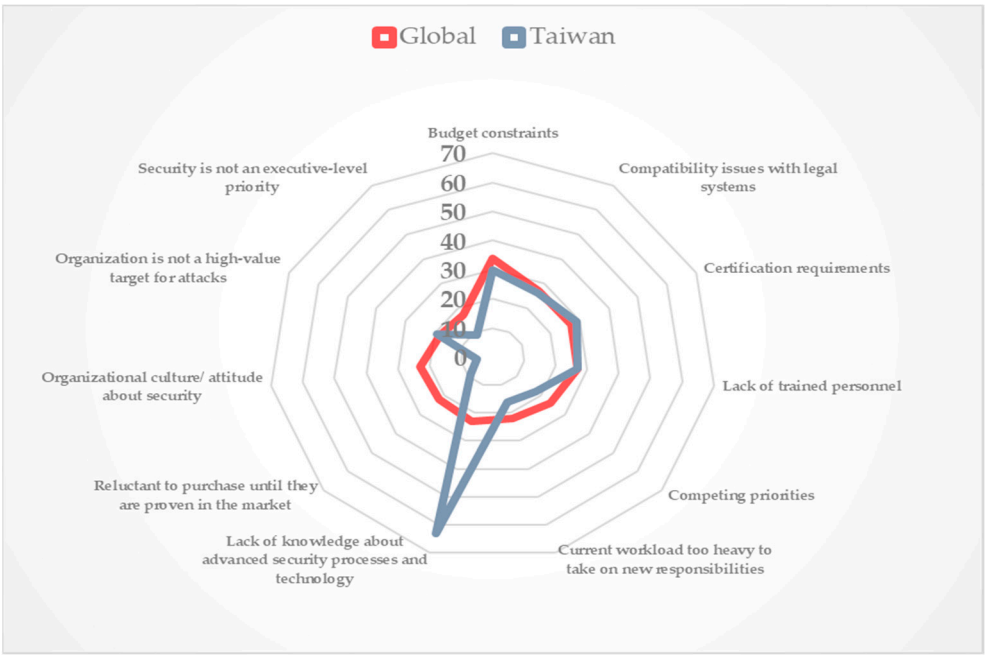

Figure 6. Obstacles blocking the adoption of advanced security procedures and technology: Taiwan vs. global averages [41,43].

3.2.4. Information Security Risks

The 2018 iThome chief information officer (CIO) survey results for Taiwan's corporate information security risk rankings are shown in Table 6 [44]. It can be observed that for CIOs, in addition to the invasion of malicious viruses, employee negligence and lack of information security awareness (which was as high as 56.7%) elicited the highest level of concern. This finding resonates with the information in Table 2 in that employees generally lack information security awareness. Moreover, this is what

Taiwanese enterprises have been striving to improve. As for virus attacks, according to 2017 statistics by Symantec on the increasing annual rates of global viruses, the types of attacks in descending order were malware (92%), phishing emails (71%), junk mail (55%), mobile device usage (54%), blackmail software (46%), and potential vulnerabilities for attacks or damage (13%). This result matched the list of information security risks that cause the greatest concern among Taiwanese CIOs.

Internal employees' negligence and lack of information security awareness pose threats to information security. It is also a great hidden risk for Taiwanese enterprises. Moreover, 56.7% of enterprises considered employees' negligence and lack of information security awareness to be the greatest information security risk and, thus, even more severe than that of phishing emails, malware, or blackmail software.

Table 6. Information security risks of greatest concern to Taiwanese CIOs by percentage as well as increasing annual rates of global viruses from Symantec's 2018 Internet Security Threat Report (ISTR) survey.

Risks	Information Security Risks of Greatest Concern to Taiwanese CIOs (Chief Information Officers) by Percentage (Effective Number of Samples, n = 462)	Increasing Annual Rates of Corresponding Types of Global Virus according to an ISTR 2017 Survey (Effective Number of Samples, n = 15,000)
Phishing emails	50.8%	71%
Malware	46.3%	92%
Blackmail software	45.2%	46%
Junk mail	35%	55%
Using mobile devices	23%	54%
Potential vulnerabilities for possible attacks or damage	18.7%	13%

Source: iThome CIO 2018 [44], ISTR 2018 Survey [39].

4. Conclusions

Information security will become a focus of corporate investment as impacts from information security threats intensify. This study integrated domestic and foreign survey data and drew conclusions regarding information security approaches for building smart cities in Taiwan from the aspects of information security manpower, information security threats, and information security management.

First, in terms of information security manpower, enterprises in Taiwan have started to hire more information security personnel than ever before because of the accentuated information security threats. According to iThome survey [43,44], enterprises on average had 3.5 information security staff members, and among all industries, those in the financial industry had the highest number of information security staff members (10 on average). Nonetheless, there was still a shortage in information security manpower. In 2018, 21% of enterprises would like to employ information security personnel, and in the financial industry, 62.5% of enterprises have information security job openings. Thus, 2018 can be said to be the year of information security manpower training and the beginning of the war for obtaining information security talents. In terms of security management, information security personnel have budgets, interconnection, and personnel as the critical limiting factors. With the development of machine learning, big data, intelligence threats, end-point detection and response, and changes in threat situations, how to acquire capabilities for in-process detection and quick threat response is a practical consideration for all enterprises. Therefore, managed detection responses and security services have become critical because they can resolve the problems of insufficient manpower and technology and, thus, have been adopted by many enterprises.

Second, regarding information security threats, because of extensively used digital equipment and applications, advancing ICT, AI-based information security, and AI technology-boosted future information security defense systems, information security will be more critical than ever before

because of the development of smart IoT devices. Information security incidents occurred frequently in 2017, and the types of attack have become increasingly complex and difficult to prevent. Moreover, with the boom of the IoT, even more conventional industries will have to implement an information security system. In the future, AI technology will be integrated into information security to enhance defense systems (e.g., a smart collaborative defense system) [45]. This is an area that is worthy of attention, and some key points include enhancing the precision of intelligence analysis, analyzing abnormality readings based on behavior, enhancing efficiency through identity certification, sandbox testing, and system vulnerability detection and fixing will be critical [40].

Third, regarding information security management, after several major information security incidents hit international headlines, Taiwan's competent authorities finally began to request that companies set up directors and divisions that are responsible specifically for information security. Whether this measure will affect the future trend is worthy of investigation. Known as the most stringent data protection law in history, the latest version of the General Data Protection Regulation of the European Union has caused great pressure for many enterprises worldwide because the penalty for breaching this regulation is the highest in the world: up to 4% of the global revenue of the enterprise. As a result, compliance with laws and regulations will be critical; enterprises in Taiwan must improve rapidly in this area to catch up. This year, the Executive Yuan proposed six sub-bills stipulating new information and communication security responsibility levels under the Capital Security Management Act. Government agencies will be required to take responsibility for the information security of their business domains. These bills will form a new set of unified information security management standards, similar to the information security operating standards of ISO27001, for Taiwan's government agencies. Sooner or later, this new set of standards will be applied to Taiwanese enterprises.

For people-oriented smart city development, all participating individuals and companies must take security and privacy seriously. For information security issues involving smart applications, adopting an appropriate information security approach is crucial. Network attacks are gradually shifting their target to critical infrastructures and strategic industries. In the worst-case scenario, network attacks may paralyze the social operating system [18,39]. When running a smart city, it is crucial to recognize that network attacks will inevitably and successfully break through the defenses [46]. In this era of fast network technology development, expansion, and popularization, network information security problems must be formally and cautiously handled and prevented by companies, the government, health and medical institutions, and schools of all sizes. In addition, insurance companies are responsible for assisting corporate legal personnel in risk prevention in advance and helping them with damage compensation restoration after the attacks to reduce losses. In this new era of network technology, the government should actively amend relevant laws to ensure that all companies fulfill their corporate responsibility to improve network information security [47].

The development of the new generation of information and communication technologies, such as Cloud computing, Big Data, Mobile Network, IoTs, etc., has brought vigorous business opportunities to smart cities [48] and has also brought new threats to information security. In the development of people-oriented smart cities, information security is a serious issue that must be confronted.

Author Contributions: S.M.W. and Y.J.W. conceptualize this paper and make the revision. S.M.W. and Y.C.W. assist in data collection and prepare for the original draft. D.G. is responsible for supervision and provides advice on the writing.

Funding: This research was partially funded by Ministry of Science & Technology, Taiwan under the project No. MOST 106-2511-S-003-029-MY3.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bibri, S.E.; Krogstie, J. Smart sustainable cities of the future: An extensive interdisciplinary literature review. *Sustain. Cities Soc.* **2017**, *31*, 183–212. [CrossRef]
2. Piggott, D. A Journey into Litecon Forensic Artifacts. Available online: https://www.sans.org/reading-room/whitepapers/forensics/paper/34595 (accessed on 2 November 2018).
3. Taskforce. *National ICT Security Development Program (2017–2020)*; National Information & Communication Security Taskforce: Taipei, Taiwan, 2017; pp. 1–58.
4. Wu, S.; Chen, T.-C.; Wu, Y.; Lytras, M. Smart cities in Taiwan: A perspective on big data applications. *Sustainability* **2018**, *10*, 106. [CrossRef]
5. Bibri, S.E.; Krogstie, J. On the social shaping dimensions of smart sustainable cities: ICT of the new wave of computing for urban sustainability. *Sustain. Cities Soc.* **2017**, *2017*, 1–45.
6. Lytras, M.; Visvizi, A. Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. *Sustainability* **2018**, *10*, 1998. [CrossRef]
7. Chen, J. *Global Smart City Development Trends and Innovative Applications*; Industrial Technology Research Institute (ITRI): Taipei, Taiwan, 2018; pp. 1–37.
8. Cheng, S.; Li, H.; Cao, S. *Strengthen the Use of New Generation Information Technology to Promote the Development of Smart Cities*, 1st ed.; People's Publishing House: Beijing, China, 2016.
9. Yuan, Y.; Yang, W.; Gao, L.; Dong, J.; Wang, C.; Liu, Y.; Shi, R.; Yu, Y.; Yao, X.; Li, F. *China Smart City Standardization White Paper*; National Information Center: Beijing, China, 2013; pp. 1–59.
10. NDC. *2018 National Development Plan—Building Taiwan, Seeing Execution*; National Development Council: Taipei, Taiwan, 2017; pp. 1–43.
11. Korotka, M.; Yin, L.R.; Basu, S.C. Information assurance technical framework and end-user information ownership: A critical analysis. *J. Inf. Priv. Secur.* **2016**, *1*, 1–16. [CrossRef]
12. Chilipirea, C.; Petre, A.-C.; Groza, L.-M.; Dobre, C.; Pop, F. An integrated architecture for future studies in data processing for smart cities. *Microprocess. Microsyst.* **2017**, *52*, 335–342. [CrossRef]
13. NDC. *Digital Country Innovative Economic Development Program 2017–2025*; National Development Committee: Taipei, Taiwan, 2017; pp. 1–428.
14. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018; pp. 1–55.
15. Federal. Federal Enterprise Architecture Framework. v2. Available online: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf (accessed on 1 September 2018).
16. Hugo, H.B. ISO/IEC 27001:2013, Your Implementation Guide. Available online: https://www.bsigroup.com/Documents/iso-27001/resources/iso-iec-27001-implementation-guide-SG-web.pdf (accessed on 4 October 2018).
17. Pillai, A.K.R.; Pundir, A.K.; Ganapathy, L. Improving information technology infrastructure library service delivery using an integrated lean six sigma framework: A case study in a software application support scenario. *J. Softw. Eng. Appl.* **2014**, *7*, 483–497. [CrossRef]
18. Collins, A. WEF the Global Risk Report 2018. Available online: https://outlook.stpi.narl.org.tw/index/focusnews/detail/443 (accessed on 20 October 2018).
19. Christopher, C. Revitalizing Privacy and Trust in a Data-Driven World- Key Findings from the Global State of Information Security Survey 2018. Available online: https://www.pwc.com/gsiss (accessed on 15 October 2018).
20. Jian, H. *Current Security Situation Analysis*; Communications Security Council: Taipei, Taiwan, 2017; pp. 1–15.
21. Fan, Y. *Smart City and Information Security*, 2nd ed.; Publishing House of Electronics Industry: Beijing, China, 2017; p. 330.
22. Mogull, R.; Arlen, J.; Gilbert, F.; Lane, A.; Mortman, D.; Peterson, G.; Rothman, M. The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. Available online: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf (accessed on 15 September 2018).
23. Lin, Y. A study on current situation and future trend of cybercrime and digital forensics in Taiwan—Take the 'innovative judicial police IEK intelligence model' as an example. *Proc. Crim. Policy Crime Res.* **2018**, *20*, 289–330.
24. Nissenbaum, H. Privacy as contextual integrity. *Wash. Law Rev.* **2004**, *79*, 101–140.

25. Lugmayr, A.; Stockleben, B.; Scheib, C.; Mailaparampil, M.A. Cognitive big data: Survey and review on big data research and its implications. What is really "new" in big data? *J. Knowl. Manag.* **2017**, *21*, 197–219. [CrossRef]
26. Fujitsu, S.R.; Verizon, W.V.G.; eBay, N.S. Expanded Top Ten Big Data Security and Privacy Challenges. Available online: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf (accessed on 1 October 2018).
27. Cárdenas, A.A.; Manadhata, P.K.; Fujitsu, S.R. Big Data Analytics for Security Intelligence. Available online: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf (accessed on 1 October 2018).
28. Yang, R.; Wu, S. *The Application of Big Data—Taking the Financial Industry as an Example*; Azion Group: Taipei, Taiwan, 2018; pp. 1–15.
29. Liao, W. Data Analysis, Data Integration, Data Quality, Omni-Directional Big Data Integration Platform. Available online: http://www.azion.com.tw/page2.aspx?cid=103&lid=112&cat_num=2 (accessed on 10 October 2018).
30. Wu, P. *Ainvr ai Deeping Learning Technologies and Case Study*; Aizon Group: Taipei, Taiwan, 2018; pp. 1–30.
31. MOTC. *Third Generation Mobile Communication Business Management Rules*; National Communications Commission: Taipei, Taiwan, 2018; pp. 1–22.
32. Cichonski, J.; Franklin, J.M.; Bartock, M. Guide to ITE Security. Available online: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-187.pdf (accessed on 10 October 2018).
33. He, D.; Chan, S.; Guizani, M. Handover authentication for mobile networks: Security and efficiency aspects. *IEEE Netw.* **2015**, *29*, 96–103. [CrossRef]
34. Zheng, Y.; Moini, A.; Lou, W.; Hou, Y.T.; Kawamoto, Y. Cognitive security: Securing the burgeoning landscape of mobile networks. *IEEE Netw.* **2016**, *30*, 66–71. [CrossRef]
35. CISCO. Cisco IoT Networking Deploy, Accelerate, Innovate. Available online: http://www.cisco.com/go/iot (accessed on 10 October 2018).
36. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
37. Zhou, W.; Zhang, Y.; Liu, P. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Access* **2018**, 1–11. [CrossRef]
38. The Open Web Application Security Project. The Ten Most Critical Web Application Security Risks. Available online: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (accessed on 12 October 2018).
39. Cleary, G.; Corpin, M.; Cox, O.; Lau, H.; Nahorney, B.; O'Brien, D.; O'Gorman, B.; Power, J.-P.; Wallace, S.; Wood, P.; et al. Internet Security Threat Report. Available online: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf (accessed on 15 September 2018).
40. Qin, W. *Taipei Smart City Development Policy and Application Cases*; Institute for Information Industry: Taipei, Taiwan, 2018; pp. 1–31.
41. CISCO. Cisco 2018 Annual Network Security Report. Available online: ahttps://www.cisco.com/c/dam/global/zh_tw/products/security/acr-report-2018/final_files_cisco_2018_acr_web_tw.pdf (accessed on 20 October 2018).
42. Gartner. 2018 Global Cio Survey. Available online: https://www.gartner.com/smarterwithgartner/the-2018-cio-agenda-infographic/ (accessed on 10 October 2018).
43. iThome. *Ithome 2018 Enterprise Security Survey: Information Security Investment Trends, Information Security Manpower Compilation, Corporate Information Security Defense Status, Information Security Incident Impact*; iThome (Taiwan): Taipei, Taiwan, 2018.
44. iThome. *Ithome 2018 Corporate Cio Survey*; iThome (Taiwan): Taipei, Taiwan, 2018.
45. Wu, P. Artificial Intelligence Network Video Recorder. Available online: http://www.azion.com.tw/page.aspx?cid=101&lid=107 (accessed on 20 October 2018).
46. Tu, J.; Xu, X.; Wang, Y.; Zeng, X.; Yang, Z.; Lin, S.; Yu, Q.; Wang, W. Ernst & Young 20th Global Information Security Survey Report. Available online: https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks-tw/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks-tw.pdf (accessed on 25 October 2018).

47. Visvizi, A.; Lytras, M.D. Rescaling and refocusing smart cities research: from mega cities to smart villages. *J. Sci. Technol. Policy Manag.* **2018**, *9*, 134–145. [CrossRef]
48. Sicilia, M.; Visvizi, A. Blockchain and OECD data repositories: opportunities and policymaking implications. *Libr. Hi Tech.* **2018**. [CrossRef]