DEVELOPMENT OF SMART CITIES IN TAIWAN FROM THE PERSPECTIVE OF CLOUD COMPUTING SECURITY

Shiann Ming Wu 1 and Yung Chang Wu 2

1 College of Information Administration China University of Technology Taipei, Taiwan. - wuming@cute.edu.tw

2 The department of Business National Open University Taipei, Taiwan. - 103081@webmail.nou.edu.tw

KEY WORDS—Cloud computing, Smart cities, Information security, Mobile network

ABSTRACT:

Cloud computing is an important part of the development of smart cities and also the focus of the information and communication technology (ICT) industry. From the concept of cloud computing, people and objects in cities are organized based on their application needs and computed in real time. It is a comprehensive utilization of the new generation of information and communication technology. This paper first introduces the concept of cloud computing, smart city construction in Taiwan, and the information security management standard of cloud computing, then describes the cloud computing security framework from three areas, and summarizes the implementation status of cloud computing in Taiwan, government policies, and measures, reaching the conclusion that information transmission must be fast and reliable and ensure personal privacy and security. Any type of information security problem will bring catastrophic consequences. Therefore, cloud computing also brings severe challenges to the traditional information security system.

I. INTRODUCTION

Cloud computing is not a new technology or a technology, but a kind of concept [1]. The cloud represents the Internet, which offers computing capabilities and services for various business activities. The development of cloud computing has brought a great deal of convenience to the lives of people, but information security and personal data confidentiality are still concerns that must be carefully evaluated in cloud computing services. Information security has been predicted to be an obstacle for sustainable computing in the future [2]. As cloud computing is a huge project that cannot be completed just by a single person or enterprise, how the government could give necessary support and assistance in the development of its technology is an issue worth investigating [3].

A smart city is a combination of interdisciplinary disciplines, including five main areas: Internet of Things (IoT), Mobile Network, Cloud Computing, Big Data and Smart Applications [4]. There are three important industrial trends. First, cloud computing and mass data services are the hottest topics in the information industry in recent years, which have triggered mass data processing, analysis, and applications based on the cloud architecture favored by enterprises. Second, although IoT is already a mature technology, its large-scale application relies on the key technology of cloud computing and mass data analysis. Third, the popularization of 4G networks and mobile devices has helped make cloud services and applications more diversified [5]. In recent years, Taiwan's major cities, supported by cloud computing bases, have devoted themselves to becoming smart cities and have achieved considerable success.

II. INFORMATION SECURITY MANAGEMENT STANDARD FOR CLOUD COMPUTING

The Cloud Security Alliance (CSA) issued the Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 in 2017 [6], identifying 13 key areas of cloud platform layers for security protection and management. Various relevant international organizations also added information security measures for cloud computing into their original information security standards. This paper presents three types of standards - information security guidelines, application standards, and technical standards as a reference for Taiwan's relevant government agencies and industry to develop the cloud technology industry.

Considering the security of cloud computing, the biggest difference is that enterprises lose physical control, while the security infrastructure, platforms, and applications are directly controlled by cloud providers. The security issues are first legal compliance and then security control. Although consumers may need all security control measures, they still doubt whether cloud providers' infrastructure can provide all security related safeguards [7].

III. CLOUD SECURITY ARCHITECTURE

The development of cloud computing has brought significant changes in the application modes of mobile Internet resources, business resources, and user resources. The appearance of multi-tenants, resource sharing, non-localization of data storage, diversification of business types, and the rapid growth of network bandwidth not only require further strengthening of traditional security issues, but have also introduced new security issues for mobile Internet applications. Hence, based on the understanding and cognition of cloud security, this study proposes a general cloud security architecture as shown in Figure 1, which is described in three areas: cloud service domain security, cloud user domain security, and cloud management domain security.

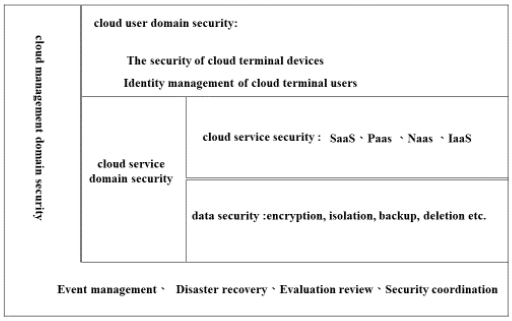

Fig. 1. Cloud Security Architecture Diagram

A. *Cloud service domain security, including layers of cloud service security and data security*

Cloud service security: divided into Infrastructure as a Service (IaaS), Networking Security as a Service (NaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), based on the business security of the cloud service. They are described respectively below.

IaaS security: As the core technology of IaaS, virtualization has two major security problems: the security of virtual machine itself and the security of virtualized software [8]. The typical security problem of the virtual machine itself is virtual machine escape, i.e., the Sniffer problem of the virtual machine. Virtualization technology can be applied on rapid allocation of various resources. Theoretically speaking, virtual machine escape means that an attacker breaks through a hypervisor, exposes the vulnerability of the hypervisor itself, or the users of the virtual machine launch malicious attacks that cause the most serious threats. Hypervisor, as the core of this layer, should focus on ensuring its security. Virtualized firewall, access control, and vulnerability scanning are generally used as protection mechanisms.

NaaS security: In the cloud environment, one should consider network security as a service. The key management points are a unified access mechanism, such as effective identity management, password and authentication management, online authorization, auditing, identity and online management AP [9]; network transmission security mechanism in the cloud environment includes IPsec (IP Security), GRE (Generic Routing Encapsulation), encryption and decryption authentication technology, key exchange technology, and access control technology; network traffic monitoring needs to use deep packet inspection (DPI) and deep flow inspection (DFI) for network traffic auditing.

PaaS security: Server, memory, and network constitute the basic structure of PaaS and also help provide middleware, development tools, business intelligence (BI) services, database management system, and other projects. PaaS can be constructed on a IaaS virtualization resource pool or directly on the physical infrastructure of a data center [10]. It needs to focus on platform security, interface security, application security, non-relational database security, etc.

SaaS security: SaaS is physically a multi-tenant sharing hardware infrastructure, but logically an exclusive service. Its security mainly considers physical deployment security, multi-user isolation, and business authorization links [11].
Data security: The ownership and management rights of data in traditional IT systems are unified and both belong to users themselves [12]. However, in the cloud environment, the ownership and management rights of data are separated. Therefore, during the process of storage, use, and deletion of cloud data, new security requirements may arise, such as the basic requirements of CIA (confidentiality, Integrity, Availability). There thus must be appropriate norms and a legally binding service level agreement (SLA) running for the encryption, isolation, backup, deletion etc. of cloud data [13]..

B. *Cloud user domain security*

Cloud users' terminal devices are not only the access entity of cloud computing, but also the link between users and cloud computing platforms [14]. The security of these terminal devices is an important link of cloud computing security and a key point of information security under a network environment. There are inevitable security vulnerabilities when users download applications from application stores and the Internet. Therefore, cloud service providers should take necessary precaution measures such as utilizing cloud terminal devices. Identity management of cloud terminal users, single sign-on (SSO), multi-factor authentication scheme, biometric identification, and other technologies, combined with cryptography technology, can also be used to provide users with more secure services.

C. *Cloud management domain security*

The cloud management domain is mainly for cloud computing operation monitoring and management, including monitoring of traffic size, network bandwidth, CPU utilization, storage space, database management, software configuration, load management, software audit, update file management, notification, and warning [15]. Malicious actions must also be monitored, such as blocking service attacks and unlawfully decrypting codes, etc. Virtualization is a major feature of cloud computing. The rapid provision and flexible expansion of related virtual resources have made security management extremely difficult. Therefore, there must be a more profound security coordination mechanism to manage the virtualization security management coordination functions of various levels in the whole cloud computing system in order to ensure the privacy and security of all data in the platform [16].

IV. CLOUD COMPUTING IN TAIWAN

Taiwan’s Executive Yuan (2015) drew up five development strategies for the cloud computing industry under the principles of balancing the "application value" and "industrial and economic output value" [17]. They are also the five strategies for the development of smart cities in Taiwan.

A. *Promoting applications as needed by the public*

The focus is on the promotion of the application, as supported by the platform and infrastructure construction. The application layer should help Taiwan's application software industry achieve cloud service functions and synergy under service expansion and user segregation. In the platform layer and foundation layer, Taiwan's hardware and software R&D should help with the premise of multi-disciplinary trials and practical evaluation.

B. *Building the development power of innovative applications*

The industry should accumulate the energy of innovative application development, invest in platforms, and provide an environment for cloud development tests [16].

C. Laying the foundation of system software

The industry should develop basic cloud operating software, reduce the cost of importing cloud service, and expand software vendors at home and abroad. Emphasis is on the research and development of green and affordable cloud computing systems and open and secure software technologies for large-scale cloud operating systems by legal persons. The government strategy supports the mainframe and storage hardware industry in Taiwan to enter the large-scale data center market; on the other hand, it helps Taiwanese players of value-added software for cloud application to develop an application market for small and medium-sized enterprises.

D. Implementing cloud infrastructure construction

The government strategy encourages server hardware players to engage in R&D and the manufacturing of cloud-based equipment and to expand into domestic and foreign markets. The key work is to support the industry to invest in R&D and renewable energy technology, as well as software system value-added services; to develop and provide complete solutions based on the hardware manufacturing infrastructure; and to build and accumulate strength by participating in cloud-based application services for the government, with the goal to enter the global data center and other cloud computing markets.

E. Giving full play to green energy-saving efficiency

The goal is to reduce the energy consumption of Taiwan's overall information system by fully utilizing the scale of the cloud economy and integrating the system into the cloud environment. The key work is to promote measures to improve the energy efficiency of data centers and to build data centers, virtualization, and co-construction of a cloud data center [18].

V. INFORMATION SECURITY STATUS

According to Harvey Nash & KPMG Global Survey (2018) [19], most types of crimes threatening global information security are trending higher, as shown in Table I, among which organized crime is the most serious.

Cloud technology is now maturing and IT leaders are generally not worried about cloud security and resilience. Another factor contributing to the increased usage of cloud technology is the direct investment and management of IT by enterprise functions, as shown in Table II, among which medium- and large-scale investments account for 70%, showing that enterprises have paid more attention to the scale of cloud technology investment.

iThome (Taiwan) [20] also made a survey on cloud storage, focusing on the major concerns of enterprises about cloud storage applications, as shown in Table III, while the proportion of cloud storage in enterprises' data storage stations is shown in Table IV. From Table III, we see that the proportion of concerns about information security accounts for 40.6%, while only 0.6% of concerns are about technician skills. This shows that cloud technology has become more mature and cloud computing will be widely accepted as long as the concerns about information security are solved.

TABLE I. LIST OF CRIME TYPES THREATENING INFORMATION SECURITY

Crime type	2018	2017	2016
Organized crime	77 %	71 %	69 %
Amateur cyber crime	56 %	52 %	48 %
Internal staff	49 %	48 %	40 %
Spammer	44 %	39 %	37 %
Foreign forces	33 %	28 %	27 %
Competitor	19 %	19 %	16 %

TABLE II. PROPORTION OF ENTERPRISE INVESTMENT IN CLOUD TECHNOLOGY

Investment Scale	Cloud Technology Investment
Large scale	34 %
Medium scale	36 %
Small scale	18 %
In planning	8 %
No investment plan	4 %

TABLE III. MAJOR CONCERNS OF ENTERPRISES ABOUT CLOUD STORAGE APPLICATIONS (TAIWAN)

Reasons for concern	Proportion of concern
Data security	40.6 %
Others	24.3 %
Cost	16.7 %
Management complexity	6.5%
Interoperability	5.9%
Regulatory compliance	5.5%
Technician skill	0.6%

TABLE IV. PROPORTION OF CLOUD STORAGE IN ENTERPRISES' STORAGE

Year	2019 (estimated)	2018	2017
Proportion of cloud storage	21.7 %	14 %	9 %

From the proportion of cloud storage in Table IV, we can see that enterprises are using more cloud computing technology year by year. Although the proportion is not high at present, its annual growth rate is as high as 50%. This corresponds to Table 4. As long as data security concerns are eliminated, cloud computing development can be optimistically expected.

VI. CONCLUSION AND SUGGESTIONS

After many years of development, Taiwan's ICT industry has grown to be an important supply base of hardware and information products around the world, with a solid industrial foundation. Cloud computing applications make the computing resources of computers available in the form of services, which can be directly obtained through the Internet. This will reshape the supply chain of the information industry and is bound to reshuffle the global information industry, triggering a new wave of competition [21]. In the course of developing the cloud computing industry and the operation of smart cities, there must be a strict information security mechanism and requirements for legal compliance, so that all businesses of enterprises are positively oriented to the construction and development of a cloud environment. During their operation, smart cities must realize that network attacks will break through the defense line successfully sooner or later. In the era of rapid growth, expansion, and popularization of cloud technology, information security is an important issue that all scales of enterprises, government,

and medical and school authorities must formally face and cautiously handle.

ACKNOWLEDGMENT

We hereby would like to express my gratitude to Azion Group (Taiwan) for its support in providing source materials and financial support during the composition of this paper.

REFERENCES

[1] S.A. Aljawarneh and M.O.B. Yassein, (2016). A conceptual security framework for cloud computing issues. *International Journal of Intelligent Information Technologies (IJIIT)*,2016, *12*(2), pp.12-24.

[2] M. Choi, Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. Sustainability, July 2016.

[3] A. Cardoso, F, Moreira, and P. Simões, A Support Framework for the Migration of E-Government Services to the Cloud. In *Cloud Computing Technologies for Connected Government* , IGI Global, 2016, pp. 124-162.

[4] S. M. Wu, T. Chen, Y. J. Wu and L. Miltiadis, Smart Cities in Taiwan: A Perspective on Big Data Applications. Sustainability 2018, 10, 106; doi:10.3390/su10010106

[5] Ministry of Economic Affairs Industry Bureau, 2015.

[6] CSA. The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. 2017.

[7] I-Long Lin. 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. MOJ, Essays on Criminal Policy and Crime Research, 2017, (20): 289-330.

[8] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds. *IEEE Transactions on Cloud Computing*, 2017, *5*(3), pp. 523-536.

[9] C. S. Mower, M. A. Palmer and S. C. Mayhew, *U.S. Patent No. 8,347,355*. Washington, DC: U.S. Patent and Trademark Office, 2013.

[10] V. S. Sharma, S. Sengupta and A. K. Mohamedrasheed, . *U.S. Patent No. 9,635,088*. Washington, DC: U.S. Patent and Trademark Office, 2013.

[11] R. Seethamraju, Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs). *Information systems frontiers*, 2015, *17*(3), pp. 475-492.

[12] P. K. Tiwari and S. Joshi, Data security for software as a service. In *Web-Based Services: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2016, pp. 864-880.

[13] D. Flint, Storms Ahead for Cloud Service Providers. *Business Law Review*, 2017, *38*(3), pp. 125-126.

[14] S. Rani and A. Gangal, Cloud security with encryption using hybrid algorithm and secured endpoints. *International journal of computer science and information technologies*,2012, *3*, pp. 4302-4304.

[15] M. Ali, S. U.Khan and A. V. Vasilakos, Security in cloud computing: Opportunities and challenges. *Information sciences*, 2015, *305*, pp. 357-383.

[16] S. M. Wu, D. Guo, Y. J. Wu and Y. C. Wu, Future Development of Taiwan's Smart Cities from an Information Security Perspective. *Sustainability*, 2018, *10*(12), 4520.

[17] NDC. Digital Country Innovative Economic Development Program 2017–2025. National Development Committee: Taipei, Taiwan, 2017; pp. 1–428.

[18] S. F. Piraghaj, A. V. Dastjerdi, R. N. Calheiros and R. Buyya, R. ContainerCloudSim: An environment for modeling and simulation of containers in cloud data centers. *Software: Practice and Experience*, 2017, *47*(4), pp. 505-521.

[19] A. Ellis and L. Heneghan, Harvey Nash & KPMG 2018 CIO Survey.

[20] iThome. Ithome 2018 Taiwan Enterprise Storage Survey: Emerging Storage Applications. 2018.

[21] Y. C. Wu, Y. J. Wu and S. M. Wu,Development and Challenges of Social Enterprises in Taiwan—From the Perspective of Community Development. *Sustainability*, 2018, *10*(6), pp. 1-17.