ICIC Express Letters
Part B: Applications
Volume **7**, Number **8**, August **2016**

ICIC International ©2016 ISSN 2185-2766
pp. 1813–1819

APPLICATION A NEW DEMATEL TO EXPLORE KEY FACTORS OF CHINA'S SECURITY RISKS OF CLOUD COMPUTING FOR E-GOVERNMENT

Kuang-Hua Hu[1] and Fu-Hsiang Chen[2]

[1]Accounting School
Nanfang College of Sun Yat-sen University
No. 882, Wenquan Avenue, Conghua District, Guangzhou 510970, P. R. China
khhu0622@gmail.com

[2]Department of Accounting
Chinese Culture University
No. 55, Hwa-Kang Road, Yang-Ming-Shan, Taipei 11114, Taiwan
chenfuhsiang1@gmail.com

Received February 2016; accepted May 2016

Abstract. *Cloud computing platform is a huge data center. In the establishment of E-government based on cloud computing, lots of government data are stored on the cloud, and under complicated network environment, huge hidden troubles and risks of information security have been brought about. Therefore, when deploying the E-government in the cloud computing environment, it is required to analyze and evaluate the possible risks thereof. In this study, DEMATEL technology is adopted to build the total influence relationship matrix of perspectives and criteria, aiming at building the influential network relation map to solve the problems in the real world, as well as to confirm the influence effects from different perspectives/criteria, to attempt to find out the important E-government cloud computing security risk factors, and to give the improvement strategies. The empirical results show that, based on the degree of network relationship influenced by perspectives, the improved priority shall be Integrity, Access, Availability, and Infrastructure.*

Keywords: Cloud computing, Risk, E-government, MADM, DEMATEL

1. **Introduction.** In the establishment of E-government cloud, lots of government data are stored on the cloud, and under complicated network environment, huge hidden troubles and risks of information security have been brought about. The technical security guide issued by National Institute of Standards and Technology (NIST) of USA is focused on continuous monitoring of cloud computing solutions, in which, risk management architecture is included. According to the Federal Risk and Authorization Management Program (FedRAMP) of NIST, a government-wide risk management standardization program on use of products and services based on cloud computing has been provided, including security evaluation, authorization and continuous supervision [1]. With the implementation of these measures, the user's trust and confidence to cloud computing environment will be increased. Therefore, when deploying the E-government system in cloud computing environment, it is required to analyze and evaluate the possible risks, so as to guarantee the safe and smooth operation of E-government under cloud computing environment. In this paper, China is taken as an example to determine the important factors of E-government cloud security risks, so as to create safe E-government cloud environment. As the risk element perspective of E-government, cloud is very huge and includes many sub-factors; if the E-government cloud security risk perspectives and criteria can be built, the influencing degree of criteria in each perspective can be understood as well as the mutual influence relationship between sub-factors and other sub-factors, and the priority

improvement strategy for improving the E-government cloud will be built, to serve as reference by the competent authority when making decisions. However, the risk criteria of E-government cloud are not independent in practice, and there may be mutual influence between the perspectives and criteria, so, this paper plans to adopt the DEMATEL (Decision Making Trial and Evaluation Laboratory) of Multiple Attribute Decision Making (MADM) on the mutual influence between the factors and sub-factors to solve the problem [2].

2. **Literature Review.** E-government cloud computing may bring about tangible risks and intangible risks, and these risks will be reflected together with the functions and advantages provided by cloud application. Therefore, to properly evaluate the security risks of E-government cloud, according to the literature and the results of depth interview with experts, the following four major risk perspectives and criteria are summarized in this study, specified as below.

2.1. **Access.** The information security risk of cloud computing firstly needs to face the problem of access control. In the perspective of Access, E-government government cloud security risks mainly include identity authentication, intrusion detection and control, and service level agreement (SLA). In complicated cloud environment, proper authentication and authorization mechanism will be very important [3]. Due to the distributed characteristics of cloud computing environment, according to Kaufman [4], the suppliers shall use encryption scheme for the data stored in the equipment and implement good control to prevent the unauthorized access. In addition, through the signing of SLAs between the cloud computing service suppliers and customers, it is able to guarantee the service quality to reach a certain level [5].

2.2. **Availability.** Outages, back-up mechanisms, malicious attacks, and portability of data and resources, four criteria are the main risk factors in the aspect of availability. Cloud computing service has a high availability; however, when the service demands skyrocket, the cloud server and storage equipment will have their loads increased suddenly, and cloud service is likely to have availability failure or interruption risk [6]. Gmail, Amazon's S3 and EC2 once conducted the widely known service interruption, which caused a serious impact on customers, showing the importance of regular data backup and emergency plans [4]. In addition, as cloud suppliers enjoy the privilege, the malicious insiders like system supervisors have more threats than ordinary customers, so the government shall consider when adopting cloud computing [7]. NIST has listed the transportability and interoperability of data between the cloud suppliers as the important items of cloud management, which is an important reference for customers to select suppliers.

2.3. **Infrastructure.** In infrastructure perspective, E-government cloud security risks mainly include flexible and scalable, interoperability, and system security, three criteria. In order to realize safe and useful cloud storage service, scalability management scheme can validly solve security risk problem [8]. Su and Dan [9] established E-government cloud corruption risks prevention system, to improve the system flexibility and scalability, therefore, preventing the occurrence of corruption risks at source. Clemons and Chen [10] pointed out the risk in interoperability of cloud computing. When customers are locked in a specific cloud service provider and cannot change to the others from one service provider, interoperability will be lacking between the existing in-house infrastructure and cloud service.

2.4. **Integrity.** The data integrity maintenance mainly includes data security and privacy, data recovery and contract language. The cloud suppliers provide the data access service, so that the data owners will lose the right to control the entire data; therefore, potential security risk may be caused. However, as IT disasters are hard to avoid, Edarat

Group has adopted advanced project management techniques to conduct various cloud disaster recovery services, to guarantee the online service quality and enhance the security of cloud-based environment. It is also pointed out by Velev and Zlateva [11] that, through virtual environment, data backup and migration are conducted to keep the service from interruption, to keep the continuity and availability of use by users. Contract language can reflect the government's needs and demands, so as to guarantee that the service providers can understand their responsibilities when providing the services [12]. This study constructed a general security risks framework of cloud computing for E-government. The 13 criteria constituted the preliminary questionnaire for assessing the key factors of China's security risks of cloud computing for E-government.

3. **Building a New Decision Model for E-Government Cloud Computing Security Risk.**

3.1. **DEMATEL technique for building an influential network relation map.**

The DEMATEL technique was developed for the purpose of showing a network relation diagram, a structural model for understanding specific societal problems. The DEMATEL technique involves three steps [2].

Step 1: *Calculate the direct influence-relation average matrix.* Assume that experts pairwise comparisons between any two factors are denoted and indicate the degree that each factor/criterion i affects each factor/criterion j. The answers by each expert form an $n \times n$ non-negative matrix $\boldsymbol{X}^h = \left[x_{ij}^h\right]$, $1 \leq h \leq H$, where $\boldsymbol{X}^1, \ldots, \boldsymbol{X}^h, \ldots, \boldsymbol{X}^H$ are the answer matrices by the H experts, and the elements of $\boldsymbol{X}^h$ are denoted by x_{ij}^h by expert h. Thus, we can construct an $n \times n$ average matrix $\boldsymbol{A}$ of all experts given by Equation (1):

$$\boldsymbol{A} = \begin{bmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{bmatrix} \tag{1}$$

The average scores of the H experts are $a_{ij} = \frac{1}{H}\sum_{h=1}^{H} x_{ij}^h$, which indicates the degree of influence with a factor by exerting on another as well as degree of influence it receives from the others.

Step 2: *Normalize the direct-influence average matrix.* The normalized initial direct influence-relation matrix $\boldsymbol{G}$ is obtained by normalizing the average matrix $\boldsymbol{A}$. The matrix $\boldsymbol{G}$ is easily derived from Equations (2) and (3) whereby all principal diagonal criteria are equal to zero:

$$\boldsymbol{G} = s \cdot \boldsymbol{A} \tag{2}$$

$$s = \min\left(1/\max_{1\leq i\leq n}\sum_{j=1}^{n} a_{ij}, 1/\max_{1\leq j\leq n}\sum_{i=1}^{n} a_{ij}\right) \tag{3}$$

Step 3: *Derive the total-influence matrix.* A continuous decrease of the indirect effects of problems moves along with the powers of the matrix $\boldsymbol{G}$, e.g., $\boldsymbol{G}^2, \boldsymbol{G}^3, \ldots, \boldsymbol{G}^\infty$, and $\lim_{q\to\infty} \boldsymbol{G}^q = [0]_{n\times n}$, for $\lim_{q\to\infty}\left(\boldsymbol{I} + \boldsymbol{G} + \boldsymbol{G}^2 + \ldots + \boldsymbol{G}^q\right) = (\boldsymbol{I} - \boldsymbol{G})^{-1}$, where $\boldsymbol{I}$ is an $n \times n$ unit matrix. The total-influence matrix $\boldsymbol{T}$ is an $n \times n$ matrix and is defined by $\boldsymbol{T} = [t_{ij}]_{n\times n}$, $i, j = 1, 2, \ldots, n$ as in Equation (4).

$$\begin{aligned} \boldsymbol{T} &= \boldsymbol{G} + \boldsymbol{G}^2 + \ldots + \boldsymbol{G}^q \\ &= \boldsymbol{G}\left(\boldsymbol{I} + \boldsymbol{G} + \boldsymbol{G}^2 + \ldots + \boldsymbol{G}^{q-1}\right) \\ &= \boldsymbol{G}\left(\boldsymbol{I} + \boldsymbol{G} + \boldsymbol{G}^2 + \ldots + \boldsymbol{G}^{q-1}\right)(1 - \boldsymbol{G})(1 - \boldsymbol{G})^{-1} \end{aligned}$$

$$= \boldsymbol{G}(\boldsymbol{I}-\boldsymbol{G})^{-1}, \text{ when } \lim_{q\to\infty}\boldsymbol{G}^q = [0]_{n\times n} \tag{4}$$

The total influence-relation matrix $\boldsymbol{T}$ of INRM (influential network relation map) can be obtained by Equation (4). Equations (5) and (6) are used to obtain each row sum and column sum in the matrix $\boldsymbol{T}$, respectively.

$$\boldsymbol{d} = (d_i)_{n\times 1} = \left[\sum_{j=1}^{n} t_{ij}\right]_{n\times 1} = (d_1,\ldots,d_2,\ldots,d_n)' \tag{5}$$

$$\boldsymbol{r} = (r_j)_{n\times 1} = (r_j)'_{1\times n} = \left[\sum_{i=1}^{n} t_{ij}\right]'_{1\times n} = (r_1,\ldots,r_2,\ldots,r_n)' \tag{6}$$

where d_i is the sum of a row in the total influence-relation matrix $\boldsymbol{T}$, which represents the total effects (both direct and indirect) of factor i on the other factors. Similarly, r_j is the column sum in the total influence-relation matrix $\boldsymbol{T}$, which represents the total effects (both direct and indirect) of factor j received from the other factors. Thus, when $i = j$, $(d_i + r_i)$ provides an index of the strength of the total influences given and received, $(d_i - r_i)$ provides an index of the degree of the cause of total influences [1].

4. An Empirical Result.

4.1. Data collection. In this study, there are 40 experts from the people's government of Guangdong province, including the senior staff and supervisors of IT department. The expert questionnaire, which assessed the mutual influence among the various criteria, was scored on a scale of 0 to 4, with 0 representing no influence, and 4 representing very

Table 1. The sum of the influences given and received on the perspectives and criteria

Perspectives/Criteria	Row sum (d_i)	Column sum (r_i)	$d_i + r_i$	$d_i - r_i$
Access (A)	**1.005**	**0.967**	**1.972**	**0.038**
Identity authentication (a_1)	1.031	1.129	2.160	–0.023(3)
Intrusion detection and control (a_2)	1.210	1.111	2.231	0.099(2)
Service level agreement (SLA) (a_3)	0.988	0.875	1.863	0.113(1)
Availability (B)	**0.987**	**1.034**	**2.021**	**–0.047**
Outages (b_1)	0.991	0.897	1.888	0.094(2)
Back-up mechanisms (b_2)	1.113	1.009	2.122	0.104(1)
Malicious attacks (b_3)	0.898	0.996	1.894	–0.098(3)
Portability of data and resources (b_4)	0.989	1.115	2.104	–0.126(4)
Infrastructure (C)	**1.033**	**1.148**	**2.181**	**–0.115**
Flexible and scalable (c_1)	0.832	1.011	1.843	–0.179(3)
Interoperability (c_2)	0.875	1.003	1.878	–0.128(2)
System security (c_3)	0.967	0.913	1.880	0.054(1)
Integrity (D)	**1.239**	**1.153**	**2.392**	**0.086**
Data security and privacy (d_1)	1.348	1.196	2.544	0.152(1)
Data recovery (d_2)	1.114	1.103	2.217	0.011(2)
Contract language (d_3)	0.998	1.039	2.037	–0.041(3)

Note: This paper $\frac{1}{n(n-1)}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\left|a_{ij}^{H}-a_{ij}^{H-1}\right|}{a_{ij}^{H}} \times 100\% = 0.53\% < 1\%$, i.e., significant confidence is 99.47%, where $H = 40$ denotes the number of experts and a_{ij}^{H} is the average influence of i criterion on; and n denotes number of criteria; here $n = 13$ and $n \times n$ matrix.

strong influence. The respondents indicated the degree of direct impact of each dimension/criterion on another dimension/criterion. The questionnaire results were analyzed empirically according to the research methods described in this study.

4.2. **An improvement plan for China's E-government cloud computing security risk.** Table 1 shows the perspectives to identify the inter-relationships between all perspectives and indicates that *Integrity* (D) would be the dimension with the most influential compared to others (with the highest $d_i - r_i = 0.086$). On the other hand, *Infrastructure* (C) exhibited the least significant impact (with the lowest $d_i - r_i = -0.115$). Figure 1 shows the perspectives and criteria measured in this study for the decline of China's Security Risks of Cloud Computing for E-government illustrated by the INRM. Based on the degree of the effect, improvement should be made according to the following order: ⌜Integrity (D)⌟ ﹣ ⌜Access (A)⌟ ﹣ ⌜Availability (B)⌟ ﹣ ⌜Infrastructure (C)⌟.

Therefore, the optimal strategy for reducing China's security risks of cloud computing for E-government is to strengthen integrity of data. In terms of criteria, compared to other criteria, Data security and privacy (d_1) is the most influential ($d_i - r_i = 0.152$); in contrast, Flexible and scalable (c_1) is the least influential ($d_i - r_i = -0.179$). All participating professionals held the same view, that more efforts should be devoted to integrity, because this perspective has immediate network effects on the other perspectives, and can help

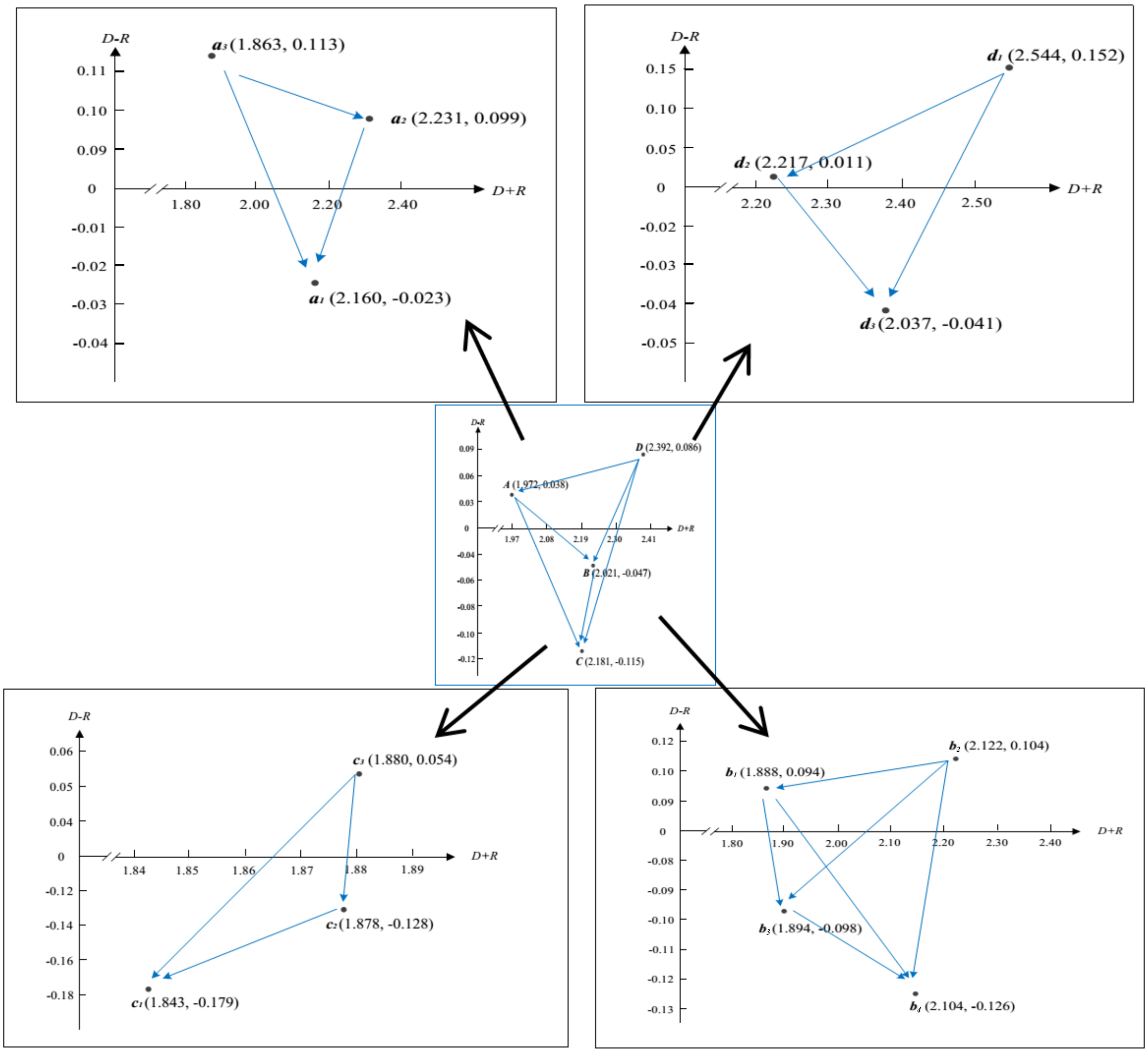

FIGURE 1. The INRM of total influence relationships for China's security risks of cloud computing for E-government

resolve multiple problems at the same time. Within an individual dimension, the influence network relationship of certain criteria also has the same effects. These are service level agreement (SLA) (a_3), back-up mechanisms (b_2), system security (c_3) and data security and privacy (d_1). These are the major influential factors within each perspective.

The findings indicate that when cloud computing for E-government constructed and adopted by the government the system security is the most important criterion. Using a set of appropriate control measures ensures that the cloud computing system is properly protected, and maintains the normal operation of the infrastructure. Obviously, the issue of data security and privacy is the hesitant reason for the government to utilize cloud computing nowadays. In order to increase the confidence of users in the cloud computing for E-government, the data security and privacy have to be intensified to retain the integrity of the data and reach the purpose of alleviating China's security risks of cloud computing for E-government. Decision-makers can consider the relationship between multiple solutions and formulate improved orders (see Table 2).

Table 2. The China's E-government cloud computing security risk implementation improvement plan

Items	Strategy (Sequence of improvement priority)
F1: Influential network of dimensions (based on DEMATEL)	$D \_ A \_ B \_ C$
F2: Influential network of criteria within individual dimensions	D: $(d_1) \_ (d_2) \_ (d_3)$ A: $(a_3) \_ (a_2) \_ (a_1)$ B: $(b_2) \_ (b_1) \_ (b_3) \_ (b_4)$ C: $(c_3) \_ (c_2) \_ (c_1)$

5. Conclusions.

This research proposes a strategy for improvement strategy of China's E-government cloud computing security risk, which may serve as reference for the government to evaluate development of the E-government cloud computing. A new decision model is constructed by the DEMATEL methods, to illustrate the inter-relationship between the influential factors. Based on the degree of the effect, consideration should be given as follows: integrity, access, availability and infrastructure. The datasets used in this research were tested by the consensus of experts. The research methodology discussed herein is capable of dealing with complex issues related to the assessment of the E-government cloud computing security risk. Not only does this research has profound implications for the responsible authorities, but, even more importantly, it also proposes a feasible and adequate modernization strategy for the E-government cloud computing security risk, which can assist the government in its improvement of both quality and quantity of the E-government cloud computing.

However, cloud computing has a high energy consumption of data center and leads high carbon emission. Green cloud computing can be used to improve this problem. Hence, application of green cloud computing for security risk for E-government has become a critical issue for future research. In addition, other approaches, such as longitudinal studies, can be used to identify other potential factors/criteria, and a larger expert sample can raise the reliability and generalizability of the results.

Acknowledgment. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] FedRAMP, *Federal Risk and Authorization Management Program*, http://www.gsa.gov/graphics/staffoffices/FedRAMP_1-20-12_Agency_Day_FINAL.pdf, 2012.

[2] F. H. Chen, G. H. Tzeng and C. C. Chang, Evaluating the enhancement of corporate social responsibility websites quality based on a new hybrid MADM model, *International Journal of Information Technology & Decision Making*, vol.14, no.3, pp.697-724, 2015.

[3] N. K. Sehgal, S. Sohoni, Y. Xiong, D. Fritz, W. Mulia and J. M. Acken, A cross section of the issues and research activities related to both information security and cloud computing, *IETE Technical Review*, vol.28, no.4, pp.279-291, 2011.

[4] L. M. Kaufman, Data security in the world of cloud computing, *Security & Privacy*, vol.7, no.4, pp.61-64, 2009.

[5] V. Ghazaryan and R.Tamošiūnaitė, Cloud computing development in Armenia, *Social Technologies*, vol.4, no.1, pp.118-138, 2014.

[6] J. O. Oredo and J. M. Njihia, Mindfulness and quality of innovation in cloud computing adoption, *International Journal of Business and Management*, vol.10, no.1, pp.144-159, 2015.

[7] M. Adineh and N. Hariri, Risks identification and ranking in information technology projects based on cloud computing, *Kuwait Chapter of the Arabian Journal of Business and Management Review*, vol.3, no.12A, pp.216-227, 2014.

[8] P. Deivendran and E. R. Naganathan, Scalability services in cloud computing using Eyeos, *Journal of Computer Science*, vol.11, no.1, pp.254-261, 2015.

[9] J. Su and S. Dan, Research on framework of corruption risks prevention system based on cloud computing, *The 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation*, pp.141-144, 2013.

[10] E. K. Clemons and Y. Chen, Making the decision to contract for cloud services: Managing the risk of an extreme form of IT outsourcing, *The 44th Hawaii International Conference on System Sciences*, pp.1-10, 2011.

[11] D. Velev and P. Zlateva, A feasibility analysis of emergency management with cloud computing integration, *International Journal of Innovation, Management and Technology*, vol.3, no.2, pp.188-193, 2012.

[12] S. Paquette, P. T. Jaeger and S. C. Wilson, Identifying the security risks associated with governmental use of cloud computing, *Government Information Quarterly*, vol.27, pp.245-253, 2010.