Application of a fuzzy Analytic Hierarchy Process to Select the Level of a Cyber Resilient Capability Maturity Model in Digital Supply Chain Systems

Naris Uraipan[1], Prasong Praneetpolgrang[2], and Tharinee Manisri[3]

ABSTRACT: Cyber resilience has emerged over the past few years because traditional cybersecurity measures are no longer enough to protect organizations from persistent attacks. The cyber-resilient capability maturity model is a crucial element within an effective digital supply chain with six components: identify, protect, detect, respond, recover, and continuity, which affect the cybersecurity of the organization. To measure the maturity level requires a holistic approach, the analytic hierarchy process (AHP) method, which allows both for using multiple criteria and also for simultaneous evaluation. Generally, the factors affecting cyber resilience in digital supply chains have non-physical structures. Therefore, the real problem is represented in a better way by using fuzzy numbers instead of constant numbers to evaluate these factors. In this study, a fuzzy AHP approach is proposed to determine the cyber resilient capability maturity level in the digital supply chain. The proposed method is applied in 9 SME companies to test the assessments. In the application, factors are weighted with fuzzy triangular numbers in pairwise comparisons. The result indicates that the weight factors from comparing the relationship of all factors put the importance of the identify factors first, followed by protect, detect, respond, recover, and continuity, respectively.

Keywords: Analytic Hierarchy Process, Cyber Resilient Capability Maturity Model, Digital Supply Chain

DOI: 10.37936/ecti-cit.2021152.240631

Article history: received June 1, 2020; revised July 28, 2020; accepted December 10, 2020; available online April 24, 2021

1. INTRODUCTION

Cyberattacks and cybercrime are a part of cyber risk that is evident for today [1], [2]. As a result of the use of advanced information and communication technology, especially the danger that comes from communicating through the Internet, various forms of cyber threats have also increased. The severity and complexity of these attacks have serious business consequences [3], [4], [5], [6], [7].

It is necessary to standardize business processes through the activities that occur in the supply chain under the digital infrastructure, including the need to increase communication between them [8]. The result of this operation causes risks to the supply chain [9]. The risks which most often occur are threats, vulnerabilities, impacts, and the likelihood that one of these will occur in the entire supply chain. The attacks come from corrupt persons who exploit a vulnerability or weaknesses in the system when attacking. The organization must also be robust, agile, and able to continue to work despite experiencing unexpected cyber threats. It needs guidelines for preparing the organization to be able to prevent, resist, detect, and respond to intrusion, espionage, or deception that could damage the organization. Here, it is called cyber resilience. So, the cyber resilience of the digital supply chain can be used to avoid, or at least reduce cyber risks and maintain the continuous and sustainable operations of business organizations.

In recent years, a variety of security maturity mod-

[1,3] The authors are with College of Logistics and Supply Chain, Sripatum University, Thailand., E-mail: naris080515@yahoo.com and tharinee@spu.ac.th

[2] The author is with School of Information Technology, Sripatum University, Thailand., E-mail: prasongspu@gmail.com

els have been proposed for overall security management. These come in the form of a maturity model. In 1989, Humphrey presented a maturity model for software quality evaluation [10]. Subsequently, this model was adopted as a basis and modified to be used for more cybersecurity work for many reasons: 1) This security capability maturity model is used effectively in many fields such as information technology and business; 2) The maturity model has a complete management process to manage a business for cybersecurity; and 3) This capability maturity model can be extended to cover all aspects of the security domain. In addition, we can see that the maturity model also is used in crucial traditional cybersecurity environments such as e-Government, e-Commerce, e-Education, and health. It is also especially important for critical national infrastructures such as electricity, water supply, oil, and transportation [11]. However, there are few people who are interested in cyber resilience for the digital supply chain [12], [13].

The Cyber Resilient Capability Maturity Model in Digital Supply Chain Systems presented by the researchers aims to find a way to deal with the threats to digital supply chains. The model was developed based on the NIST Cyber Security Framework with identify, protect, detect, respond, recover, and continuity to prepare organizations to respond to new cyber threats that can occur all the time. Effectiveness is measured with the development of indicators, assessment criteria, and assessment tools used for evaluation to help the organization conduct a self-assessment. But each evaluation process has different concepts and methods of measurement, with personal conditions and reasons. Therefore, the researcher uses the Analytic Hierarchy Process (AHP) technique for multi-criteria decision making.

Another limitation is the difficulty in assessing the capability maturity level of each indicator that will affect the overall maturity level. This assessment causes the results of the measurement process to be unable to measure the results with an accurate and neutral indicator [14], [15], [16]. A fuzzy logic approach using approximate reasoning should be adopted. It differs from the logical thinking of right/wrong, yes/no, used by classical logic in order to simulate the assessor's decisions that can solve complex problems.

Thus, the objectives of this paper are threefold. First, to apply the capability maturity model assessment to SMEs. Second, to evaluate the level of the cyber resilient capability maturity model of the digital supply chain in SMEs. Finally, to use the fuzzy AHP approach to determine the cyber resilient capability maturity level in the digital supply chain in the case of non-physical structures and to address the real problem factors that affect SMEs.

2. LITERATURE REVIEW

2.1 Analytic Hierarchy Process: AHP

AHP is a method used to determine important weights developed by Thomas L. Saaty in the 1970s as a technique for choosing or sorting alternatives for a multi-criteria decision problem. AHP creates a decision model with a hierarchical structure using the information obtained from experts' opinions to analyze and summarize suitable alternatives. The process of the AHP method consists of three steps which are described next.

1. Decomposition is in the form of a hierarchical structure (Hierarchy Structure). Each level consists of the criteria for making decisions related to that problem. The top-level is called the goal, and overall, there is only one factor. Level 2 is called the criteria. It may have many factors, depending on how many levels of the chart there are. Most importantly, the elements at the same level must be equally important. If they are of very different importance, the less essential factors should be separated to place them on the next level. An example of an AHP structure chart is shown in Fig.1

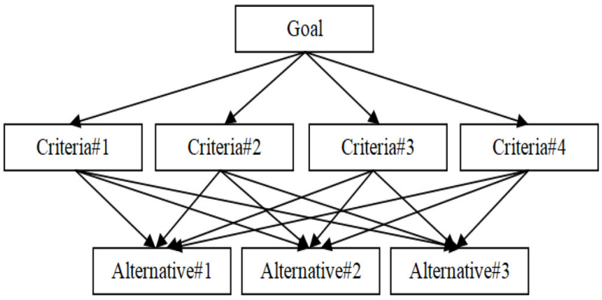

Fig.1: *Hierarchy Structure.*
Source:Boonsita Kitisrivorapot [17]

2. Prioritization is done by comparing the relationships one by one based on structural factors using the principle of hierarchic composition method. The diagnosis is expressed in the form of a numeric satisfaction level (ranging from 1 to 9) in the matrix table. The matrix table is the most suitable tool to compare pairs of factors. In addition to helping explain the comparison, the matrix table can also test the consistency of the diagnosis. It can be used to analyze the sensitivity of the priority when the diagnosis is changed.

3. Synthesis is done by considering all priorities from the comparison of chosen alternatives. It begins by analyzing the matrix and mean with mathematical methods.

2.2 Fuzzy Set Theory

Fuzzy set theory is a mathematical science that has become more active in the field of computer research and has been employed in many applications, such as medical, military, business, industrial, etc. [18]

1. Fuzzy Logic Concept

Fuzzy logic is a tool that helps you make subjective decisions under data instability by allowing for flexibility. This is accomplished by using logic that is similar to mimicking the convoluted thinking of humans. Fuzzy logic is different from Boolean logic. Fuzzy logic has an extension of partially true. In contrast, Boolean logic only has true and false, as shown in Fig.2.

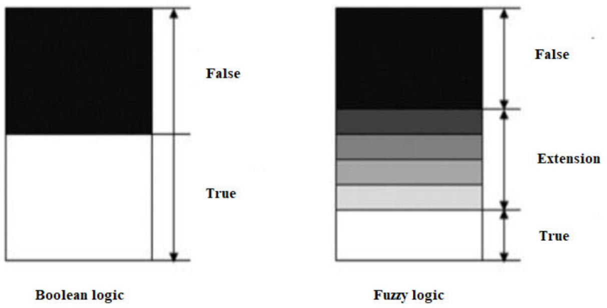

Fig.2: *Boolean logic and Fuzzy logic.*
Source: Phayung Meesad [18]

2. Membership Function The membership function is a function that determines the membership level of the variable that one needs to use. It starts by replacing it with an agent that is unclear, unpredictable, and ambiguous. This is an integral part of fuzzy's features or operations because the shape of the membership function is essential to the processes of thinking and problem-solving. The member functions can be asymmetric or symmetric in all respects. For this study, the triangular membership function was selected, with triangular membership numbers that have to be converted and the rating of the assessors averaged according to the Triangular Fuzzy Number function. In this paper, [19] [20] methods are used. Table 1 shows the triangular membership numbers.

Table 1: *Triangular Fuzzy Number.*

Fuzzy Number	Triangular Fuzzy Number
1	(1,1,1)
2	(1,2,3)
3	(2,3,4)
4	(3,4,5)
5	(4,5,6)
6	(5,6,7)
7	(6,7,8)
8	(7,8,9)
9	(8,9,9)

2.3 Fuzzy AHP Analysis

In this study, the research uses Chang's extent analysis method because the steps of this approach are more comfortable than the other fuzzy AHP approaches [21] [22].The definition of the triangular fuzzy number and the steps of Chang's extent analysis method are given next.

2.3.1 The description of the triangular fuzzy number and the operation laws of the triangular fuzzy number [20]

The membership function $\tilde{M}(x) : R \rightarrow [0,1]$ of triangular Fuzzy number $\tilde{M}(x) = (l,m,u)$ defined on R is equal to

$$\tilde{M}(x) = \begin{cases} \dfrac{x}{m-l} - \dfrac{l}{m-l}, & x \in [l,m], \\ \dfrac{x}{m-u} - \dfrac{u}{m-u}, & x \in [m,u], \\ 0, Otherwise, & \end{cases} \qquad (1)$$

where $l \leq m \leq u$, m is the possible value of the fuzzy number $\tilde{M}$, and l and u are the lower and upper bounds, respectively. According to Zadeh's extension principle, given two fuzzy triangular numbers $\tilde{M}_1 = (l_1, m_1, u_1)$ and $\tilde{M}_2 = (l_2, m_2, u_2)$,($l_2$ and $l_2 \geq 0$), the operators can be defined with Equations 2, 3 and 4.

1.The extended addition defined as

$$\tilde{M}_1 \oplus \tilde{M}_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2). \qquad (2)$$

2.The extended multiplication defined as

$$\tilde{M}_1 \oplus \tilde{M}_2 = (l_1 l_2, m_1 m_2, u_1 u_2). \qquad (3)$$

3. The inverse of a triangular fuzzy number defined as

$$\tilde{M}_1^{-1} \approx (\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}). \qquad (4)$$

2.3.2 Chang's fuzzy AHP Method

Let $\boldsymbol{X} = \{\boldsymbol{o_1}, \boldsymbol{o_2}, \ldots, \boldsymbol{o_n}\}$ be an object set, and let $\boldsymbol{U} = \{\boldsymbol{g_1}, \boldsymbol{g_2}, \ldots, \boldsymbol{g_m}\}$ be a goal set. According to the method of Chang's extent analysis, each object is considered one by one, and for each object, the analysis is carried out for each of the possible goals, g_i. Therefore, m extent analysis values for each object are obtained and shown in equation 5.

$$\tilde{M}^1_{gi},\ \tilde{M}^2_{gi}, \ldots, \tilde{M}^m_{gi}, \quad i = 1, 2, \ldots, n \qquad (5)$$

All of the $\tilde{M}^j_{gi} (j = 1, 2, \ldots, m)$ are all fuzzy triangular numbers. The membership function of the triangular fuzzy number is dented by $\tilde{M}(x)$. The steps of Chang's extent analysis are given next.

Step 1: The value of fuzzy synthetic extent concerning the i^{th} object is defined as

$$S_i \approx \sum\nolimits_{j=1}^{m} \tilde{M}_{gi}^{j} \otimes \left[\sum\nolimits_{i=1}^{n} \sum\nolimits_{j=1}^{m} \tilde{M}_{gi}^{j}\right]^{-1} \tag{6}$$

where $\otimes$ denotes the extended multiplication of two fuzzy numbers. To obtain $\sum_{j=1}^{m} \tilde{M}_{gi}^{j}$ perform the fuzzy addition operation of m extent analysis values for a particular matrix such that

$$\sum\nolimits_{j=1}^{m} \tilde{M}_{gi}^{j} = \left(\sum\nolimits_{j=1}^{m} l_j, \sum\nolimits_{j=1}^{m} m_j, \sum\nolimits_{j=1}^{m} u_j\right). \tag{7}$$

To obtain $[\sum_{j=1}^{m} \sum_{j=1}^{m} \tilde{M}_{gi}^{j}]^{-1}$, perform the fuzzy addition operation of $\tilde{M}_{gi}^{j}(j = 1, 2, \ldots, m)$ values such that

$$\sum\nolimits_{i=1}^{n} \sum\nolimits_{j=1}^{m} \tilde{M}_{gi}^{j} = \left(\sum\nolimits_{i=1}^{n} l_i, \sum\nolimits_{i=1}^{n} m_i, \sum\nolimits_{i=1}^{n} u_i\right) \tag{8}$$

and then compute the inverse of the vector in Eq.(7) such that

$$\left[\sum\nolimits_{i=1}^{n} \sum\nolimits_{j=1}^{m} \tilde{M}_{gi}^{j}\right]^{-1} = \left(\frac{1}{\sum_{i=1}^{m} u_i}, \frac{1}{\sum_{i=1}^{m} m_i}, \frac{1}{\sum_{i=1}^{m} l_i}\right). \tag{9}$$

Step 2: The degree of possibility of $\tilde{M}_2 = (l_2, m_2, u_2) \geq \tilde{M}_1(l_1, m_1, u_1)$ is defined as

$$V(\tilde{M}_2 \geq \tilde{M}_1) = sup\left[\min(\tilde{M}_1(x), \tilde{M}_2(y))\right] \tag{10}$$

and can be equivalently expressed as follows:

$$\begin{aligned} V(\tilde{M}_2 \geq \tilde{M}_1) &= hgt(\tilde{M}_1 \cap \tilde{M}_2) \\ &= \tilde{M}_2(d) \\ &= \begin{cases} 1 \\ 0 \\ \frac{l_2 - u_2}{(m_2 - u_2) - (m_1 - l_1)}. \end{cases} \end{aligned} \tag{11}$$

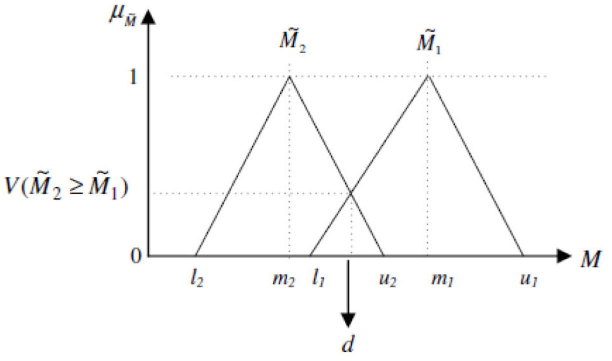

Fig.3: *The intersection between $\tilde{M}_1$ and $\tilde{M}_2$.*

Fig. 3 illustrates $V(\tilde{M}_2 \geq \tilde{M}_1)$, for the case $m_2 < l_1 < u_2 < m_1$, where d is the abscissa value corresponding to the highest crossover point D between $\tilde{M}_1$ and $\tilde{M}_2$. To compare $\tilde{M}_1$ and $\tilde{M}_2$, we need both of the values $V(\tilde{M}_1 \geq \tilde{M}_2)$ and $V(\tilde{M}_2 \geq \tilde{M}_1)$.

Step 3: The degree possibility for a convex fuzzy number to be higher than kconvex fuzzy numbers $\tilde{M}_i(i = 1, 2, \ldots, k)$ can be defined by Equation 12.

$$V(\tilde{M} \geq \tilde{M}_1, \tilde{M}_2, \ldots, \tilde{M}_k) = \min V(\tilde{M} \geq \tilde{M}_i) \quad i = 1, 2, \ldots, k. \tag{12}$$

Step 4: Finally,

$$W = (\min V(S_1 \geq S_k), \min V(S_2 \geq S_k), \ldots, V(S_n \geq S_k))^T$$

is the weight vector for $k = 1, 2, \ldots, n$.

3. METHODOLOGY

3.1 Study of Cyber resilient model in the digital supply chain for digital business continuity management

To study the cyber resilient capability maturity model in digital supply chain systems for managing digital business continuity management, the researchers conducted a study based on the cybersecurity framework of the United States National Institute of Standards and Technology (NIST), consisting of 5 main functions and 23 categories [23]. Each of the main functions is divided into smaller functions which are described in reference documents such as CIS CSC, COBIT 5, ISA 62443-2- 1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013 and NIST SP 800-53 Rev. 4. Researchers have studied and used these concepts to create the cyber-resilient capability maturity model in digital supply chain systems for managing digital business continuity management.

3.2 Component analysis of cyber resilient model for the digital supply chain for digital business continuity management

In this research, the researchers conducted a study of additional standards for enabling the development of a cyber resilient model for digital supply chain systems for digital business continuity management. Those standards consist of:

1. The ISO/IEC 27001:2013 information security management system (ISMS) is the standard for information security management. [24],[25]

2. The ISO/IEC 27002:2013 is the practical means for supporting ISO 2700. It specifies best practices for initiating, developing, and maintaining ISMS. [26]

3. The ISO/IEC 27005:2018 contains cyber risk management standards, which consist of information technology, security techniques, and information security management systems. [27]

4. The ISO22301:2012 business continuity management systems are the standards that enable orga-

nizations to plan and respond to disasters, especially cyber-attacks, systematically. [28],[29],[30]

5. The ISO/IEC 27032:2012 is an extension of ISO 27001 that is involved in confidentiality, integrity, and availability of assets such as hardware, software, information, and services, including virtual assets such as reputation, etc. [31]

6. The ISO/IEC 28000 is a standard that defines the requirements of the supply chain security management system and provides the management model for the organization that wants to implement this system. The objective is to effectively manage risks by organizing the security activities of the digital supply chain organization under the same system as other management systems [32] [33] [34].

7. The ISO 31000:2009 provides standards for enterprise risk management [35] [36].

These standards used in this study are international standards used for cybersecurity systems. They are necessary to develop the cyber-resilient model for the digital supply chain, as shown in Fig 4. Moreover, using them results in the organization's work process under the digital supply chain. It enables a business to work safely in the current digital environment by working with clear procedures and allows them to be ready with effective cybersecurity in the digital supply chain [37] [38]. It can build trust with partners under the digital supply chain.

From the study of the above information, the researchers can present a cyber-resilient model for the digital supply chain that has been developed, as shown in Fig.4.

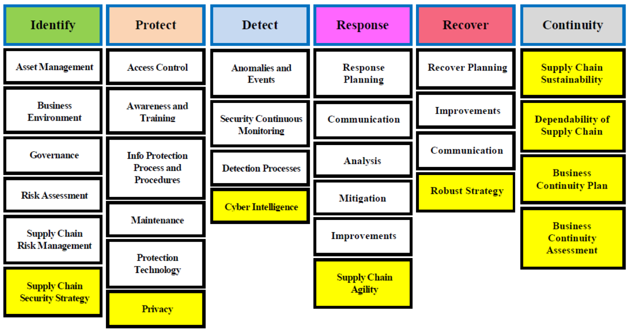

Fig.4: *Cyber Resilience Model for Digital Supply Chain.*
Source: Naris and Prasong [39]

The details of the cyber-resilient model for digital supply chain can divided into 6 functions and 32 categories. We can explain the main functions as follows:

1. Identify: It identifies and understands the various contexts of supply chain cyber risk management, which has added a new category, supply chain security strategy, based on ISO 28000 and ISO 31000.

2. Protect: It sets standards and controls to protect the organization's systems against the cyber risk of the digital supply chain, which added a new category, privacy, based on ISO 27001, ISO 27002, and ISO 27032.

3. Detect: It defines procedures and processes to detect abnormal situations, which added a new category cyber intelligence, based on ISO 27001, ISO 27002, and ISO 27005.

4. Respond: It describes methods and processes to deal with unusual situations that occur, which added a new category, supply chain agility [39].

5. Recover: It determines the steps and processes to restore the system to normal, which added a new category, robust strategy [39].

6. Continuity: It implements the various stages and procedures to enable the business to continue, which is a new function based on ISO 22301, including 4 categories: supply chain sustainability, dependability of supply chain, business continuity plan, and business continuity assessment.

From the development of the cyber-resilient model for the digital supply chain, the researchers developed the hierarchical structure of the AHP process used in this study, as shown in Fig. 5.

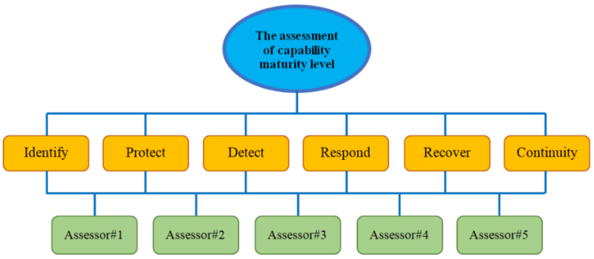

Fig.5: *Hierarchical structure of the assessmentof capability maturity level of the assessor.*

3.3 Questionnaire developed and data collection

After obtaining the components that will be used to assess the cyber resilient capability maturity model for the digital supply chain, the researchers created a questionnaire following the criteria and gave it to the assessor for an option. The researchers invited 9 SME companies to test the cyber-resilient capability maturity model in digital supply chain with a convenient sampling methodology. The researchers also explained and checked the understanding of the assessors about how to answer the questionnaire at their offices. The 12 assessors from 9 SME companies are shown in Table 2.

***Table 2:** List of 12 assessors from 9 companies.*

No	Company	Position
1	1	Managing Director
2	2	Digital Marketing Manager
3	3	IT Senior Officer
4	4	Senior IT Support
5	5	Assistant IT Section Manager
6	6	IT Manager
7	7	Operation Merchandising Parcel Support Manager
8	8	Human Resource Manager
9	9	Account Manager
10	9	Senior Programmer
11	9	Application Support Manager
12	9	Programmer

The researchers used Kappa statistics to assess the conformity of assessors, to learn whether the assessors agree. As there were more than 3 evaluators, the researcher used Fleiss's Kappa statistics as a test to confirm the consistency of the data obtained Fleiss, (1971) [40]. Fleiss's Kappa statistic ($\hat{K}_{\mathrm{F}}$) can be calculated by

$$\hat{K}_{\mathrm{F}} = \frac{\bar{P}_a - \bar{P}_e}{1 - \bar{P}_e} \tag{13}$$

when $\bar{P}_a = \frac{1}{r}\sum_{i=1}^{r} z_j$, $\bar{P}_a = \frac{1}{q}\sum_{k=1}^{r} p_j^2$
where $z_j = \frac{1}{m(m-1)}\left(\sum_{k=1}^{q} n_{ij}^2 - \sum_{k=1}^{q}\right)$ and $p_j = \frac{1}{rm}\sum_{i=1}^{r} n_{ij}$

Based on the data obtained from the survey of 12 assessors, it is possible to calculate the Kappa statistic with a value of 0.848. From the criteria for determining the degree of conformity of the Kappa statistic according to Fleiss Levin and Paik guidelines [41], the appraisal was found to the practically acceptable.

In this research, AHP using fuzzy logic was applied to define the weight of each assessor's opinion. All criteria were considered with a pairwise comparison matrix. In place of a numeric value, the Fuzzy AHP is a range of values that are combined to evaluate the weight of criteria [42]. The fuzzy prioritization method uses this scale in Parkash's study [43]. The fuzzy conversion scale is presented in Table 3.

***Table 3:** Triangular fuzzy scale (TFS).*

Importance Intensity	TFS	Importance Intensity	TFS
1	(1,1,1)	1/1	(1,1,1)
2	(1,2,3)	1/2	(1/3,1/2,1/1)
3	(2,3,4)	1/3	(1/4,1/3,1/2)
4	(3,4,5)	1/4	(1/5,1/4,1/3)
5	(4,5,6)	1/5	(1/6,1/5,1/4)
6	(5,6,7)	1/6	(1/7,1/6,1/5)
7	(6,7,8)	1/7	(1/8,1/7,1/6)
8	(7,8,9)	1/8	(1/9,1/8,1/7)
9	(9,9,9)	1/9	(1/9,1/9,1/9)

The researchers determined that respondents choose to evaluate the weight of the factors. It must be compared in pairs for all elements, starting from the top and going to the bottom of the chart. The number of pairs used for comparison is equal to:

$$\text{Number of pairs in comparison} = \frac{n^2 - n}{2} \tag{14}$$

where n = number of factors to compare.

In this research, we know from the hierarchical structure of the assessment of the maturity level of the assessors that there are a total of 6 factors, so the number can be found in the comparison as follows:

$$\begin{aligned}\text{Number of pairs in comparison} &= \frac{6^2 - 6}{2}\\ &= 15\text{Pairs.}\end{aligned}$$

4. RESULTS

4.1 Application of Fuzzy AHP techniques to create evaluation models for cyber-resilient capability maturity model in digital supply chain

After collecting the information, the researchers took the data from the questionnaire to analyze the weight of factors that influence the assessment of the cyber resilient capability maturity model for digital supply chain for managing digital business continuity management according to the Fuzzy AHP technique for decision-making processes, and the researchers performed an analysis with the following steps:

Step 1: Change actual numbers into ambiguity numbers.

Step 2: Put fuzzy numbers in the matrix using the Pairwise Comparison.

Step 3: Calculate the weight for each rule according to Chang's extent analysis.

Step 4: Calculate the weight of alternatives from the weighted values of each criterion for the best assessment of the cyber-resilient capability maturity levels of the assessors.

From the steps mentioned above, the researchers created the Pairwise Comparison Matrix shown in Table 4.

With a pairwise comparison of each factor, we can calculate the weight of the factors using the principles of Chang's extentanalysis. The values can be calculated as follows:

S_{IF}=(9.49,12.16,13.18)⊕(1/54.95, 1/48.12, 1/40.48)
≈ (0.17,0.26,0.33),

S_{PF} =(10.33,12.10,14.22) ⊕(1/54.95, 1/48.12, 1/40.48)
≈ (0.19,0.25,0.35),

S_{DF} = (6.69,8.12,9.48) ⊕ (1/54.95, 1/48.12, 1/40.48)
≈ (0.12,0.17,0.23),

S_{R1F} = (5.97,6.94,9.22) ⊕ (1/54.95, 1/48.12, 1/40.48)
≈ (0.11,0.14,0.23),

S_{R2F} = (3.92,4.30,4.87) ⊕ (1/54.95, 1/48.12, 1/40.48)
≈ (0.07,0.09,0.12),

Table 4: *Pairwise Comparison Matrix of Factors.*

	Identify	**Protect**	**Detect**	**Respond**	**Recover**	**Continuity**
Identify	(1,1,1)	(1.58,2.83,2.42)	(3.08,3.67,4.25)	(1.33,1.75,2.17)	(1.75,2.08,2.42)	(0.75,0.83,0.92)
Protect	(0.41,0.35,0.63)	(1,1,1)	(2.00,2.33,2.67)	(0.92,1.17,1.42)	(3.17,4.00,4.83)	(2.83,3.25,3.67)
Detect	(0.24,0.27,0.32)	(0.37,0.43,0.50)	(1,1,1)	(1.25,1.67,2.08)	(2.00,2.50,3.00)	(1.83,2.25,2.58)
Respond	(0.46,0.57,0.75)	(0.70,0.85,1.09)	(0.48,0.60,0.80)	(1,1,1)	(2.50,2.92,3.33)	(0.83,1.00,1.17)
Recover	(0.41,0.48,0.57)	(0.21,0.25,0.32)	(0.33,0.40,0.50)	(0.39,0.34,0.40)	(1,1,1)	(1.58,1.83,2.08)
Continuity	(1.09,1.20,1.33)	(0.27,0.31,0.35)	(0.39,0.44,0.55)	(0.85,1.00,1.20)	(0.48,0.55,0.63)	(1,1,1)

$\mathrm{S_{CF}} = (4.08,4.50,5.06) \oplus (1/54.95,\ 1/48.12,\ 1/40.48)$
$\approx(0.07,0.10,0.13)$.

Using these vectors,

$\mathrm{V(S_{IF} \geq S_{PF})} = 1.00$, $\mathrm{V(S_{IF} \geq S_{DF})} = 1.00$,
$\mathrm{V(S_{IF} \geq S_{R1F})} = 1.00$, $\mathrm{V(S_{IF} \geq S_{R2F}} = 1.00$,
$\mathrm{V(S_{IF} \geq S_{CF})} = 1.00$,
$\mathrm{Min\ V(S_{IF} \geq S_{IF},S_{DF},S_{R1F},S_{R2F},S_{CF})=1.00}$

$\mathrm{V(S_{PF} \geq S_{IF})} = 0.95$, $\mathrm{V(S_{PF} \geq S_{DF})} = 1.00$,
$\mathrm{V(S_{PF} \geq S_{R1F})} = 1.00$, $\mathrm{V(S_{PF} \geq S_{R2F}} = 1.00$,
$\mathrm{V(S_{PF} \geq S_{CF})} = 1.00$,
$\mathrm{Min\ V(S_{PF} \geq S_{IF},S_{DF},S_{R1F},S_{R2F},S_{CF})=0.95}$

$\mathrm{V(S_{DF} \geq S_{IF})} = 0.40$, $\mathrm{V(S_{DF} \geq S_{PF})} = 0.33$,
$\mathrm{V(S_{DF} \geq S_{R1F})} = 1.00$, $\mathrm{V(S_{DF} \geq S_{R2F}} = 1.00$,
$\mathrm{V(S_{DF} \geq S_{CF})} = 1.00$,
$\mathrm{Min\ V(S_{DF} \geq S_{IF},S_{DF},S_{R1F},S_{R2F},S_{CF})=0.33}$

$\mathrm{V(S_{R1F} \geq S_{IF})} = 0.33$, $\mathrm{V(S_{R1F} \geq S_{PF})} = 0.27$,
$\mathrm{V(S_{R1F} \geq S_{DF})} = 0.79$, $\mathrm{V(S_{R1F} \geq S_{R2F}} = 1.00$,
$\mathrm{V(S_{R1F} \geq S_{CF})} = 1.00$,
$\mathrm{Min\ V(S_{R1F} \geq S_{IF},S_{PF},S_{DF},S_{R2F},S_{CF})=0.27}$

$\mathrm{V(S_{R2F} \geq S_{IF})} = 0.56$, $\mathrm{V(S_{R2F} \geq S_{PF})} = 0.33$,
$\mathrm{V(S_{R2F} \geq S_{DF})} = 0.67$, $\mathrm{V(S_{R2F} \geq S_{R1F}} = 0.17$,
$\mathrm{V(S_{R2F} \geq S_{CF})} = 0.83$,
$\mathrm{Min\ V(S_{R2F} \geq S_{IF},S_{PF},S_{DF},S_{R1F},S_{CF})=0.17}$

$\mathrm{V(S_{CF} \geq S_{IF})} = 0.33$, $\mathrm{V(S_{CF} \geq S_{PF})} = 0.40$,
$\mathrm{V(S_{CF} \geq S_{DF})} = 0.13$, $\mathrm{V(S_{CF} \geq S_{R1F}} = 0.33$,
$\mathrm{V(S_{CF} \geq S_{CF})} = 1.00$,
$\mathrm{Min\ V(S_{CF} \geq S_{IF},S_{PF},S_{DF},S_{R1F},S_{CF})=0.13}$

are obtained. Thus, the weight vector from Table 4 is calculated as:

$\mathrm{W} = (1.00,0.95,0.33,0.27,0.17,0.13)^T$
$\mathrm{W_{Factors}} = (0.35,0.33,0.12,0.09,0.06,0.05)$.

4.2 Weight factor for the importance of key criteria

The result from the analysis of the factors/criteria that affect the evaluation of the cyber-resilient capability maturity model in digital supply chain is the weight of factors for importance criteria. Once the weight of factors of importance has been obtained, a model could be selected to find the outcome of the cyber-resilient capability maturity assessment in digital supply chain.

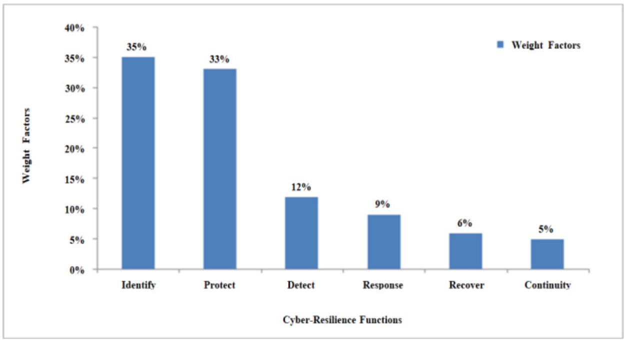

Fig.6: *Weight factors for the importance of key criteria.*

From Fig. 6, by using the fuzzy AHP technique, the results of weight factors comparing the relationship of all 6 factors from 12 respondents show that the importance of Identify factors was the highest, followed by Protect, Detect, Respond, Recover and Continuity with weight factors of 35%, 33%, 12%, 9%, 6%, and 5%, respectively

5. PRACTICAL APPLICATION

The results of the study were used by the researchers to assess the cyberresilient capability maturity model in digital supply chain. There will be cases where the assessment system will be used for evaluation in the company. The management of that organization may require an assessment as follows:

1. There is only one assessor, and the company will get 1 evaluation result.
2. There are many assessors, and the company will get many evaluation results.
3. There is a group of assessors, and the company will get 1 evaluation result.

There is no problem with the evaluation result in cases no. 1 and no. 3, but a problem exists for case no. 2. The management wants to get the best evaluation result from the assessors. Therefore, the researchers adopted the result from section 4 (weight factor for the importance of key criteria) to evaluate the best selection in the case of many assessors.

In the 9th SME company, there are 4 assessors with various positions as follows:

Assessor♯1	Account Manager
Assessor♯2	Senior Programmer
Assessor♯3	Application Support Manager
Assessor♯4	Programmer

The result of the evaluation is shown in Tables 5 and Fig. 7.

Table 5: *Assessment result from 4 assessors.*

Aspect	Maturity Score			
	♯1	♯2	♯3	♯4
Identify	3.69	3.98	3.16	2.72
Protect	2.93	2.70	2.64	2.70
Detect	2.83	2.84	2.72	2.93
Respond	3.16	2.95	2.89	2.92
Recover	3.21	3.39	2.87	3.21
Continuity	1.84	2.54	2.26	2.72

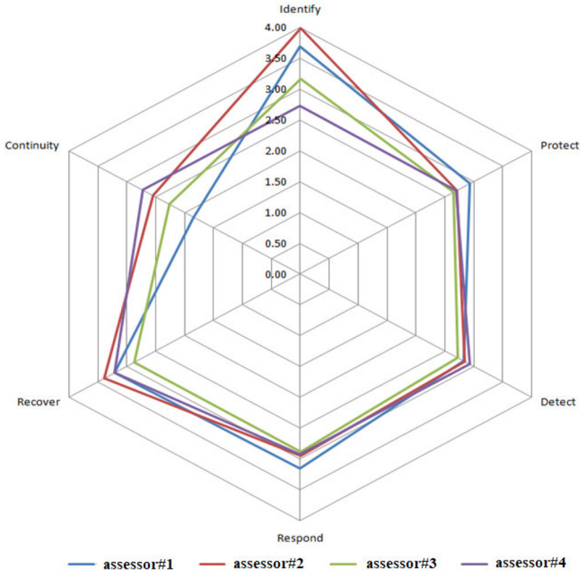

Fig.7: *(Maturity level from 4 assessors.*

From the weight factors of important criteria found in section 4, the assessment can be calculated. Results were chosen according to the assessors and are displayed in Tables 6 – 7.

Table 6: *Weight factors for the importance of key criteria .*

Criteria	**Weight Factor**
Identify	0.351
Protect	0.332
Detect	0.116
Respond	0.095
Recover	0.060
Continuity	0.046

Table 7: *The result of evaluating the maturity level from the assessor from the weight factor.*

Aspect	Maturity Score			
	♯1	♯2	♯3	♯4
Identify	(3.69×0.351) =1.295	(3.98×0.351) =1.397	(3.16×0.351) =1.109	(2.72×0.351) =0.955
Protect	(2.93×0.332) =1.028	(2.70×0.332) =0.948	(2.64×0.332) =0.927	(2.72×0.332) =0.948
Detect	(2.83×0.116) =0.993	(2.84×0.116) =0.997	(2.72×0.116) =0.955	(2.93×0.116) =1.028
Respond	(3.16×0.095) =1.109	(2.95×0.095) =1.035	(2.89×0.095) =1.014	(2.92×0.095) =1.025
Recover	(3.21×0.060) =1.127	(3.39×0.060) =1.190	(2.87×0.060) =1.007	(3.21×0.060) =1.127
Continuity	(1.84×0.046) =1.127	(2.54×0.046) =1.190	(2.26×0.046) =1.007	(2.72×0.046) =1.127
Total	**6.199**	**6.458**	**5.806**	**6.037**

As shown in Table 7, the 2nd assessor of this company has the highest maturity score of 6.458, which is followed by the 1st, 4th, and 3rd assessors with maturity scores of 6.199, 6.037, and 5.806, respectively. Therefore, it is possible to select the assessment from the 2nd assessor because it has the highest maturity score. This company can use this cyber-resilient capability maturity level in digital supply chain to be a guideline for further development of the company's cyber attack protection system

6. CONCLUSION

In this study, a model was developed to determine the cyber-resilient capability maturity model in digital supply chains. This model is based on learning the most crucial factors that may cause cyber risk in the company and taking precautions to correct these factors. In this study, a fuzzy AHP method is used to determine the degree of importance of the factors in the model. Chang's extent analysis method which is used in this paper has proved to be simpler, less time consuming, and have lower computation expense compared to other existing fuzzy AHP methods. This method can capture the ambiguity of the human thinking style and effectively solve multi-criteria decision-making problems.

The proposed model allows the evaluation of the results of the functional point of view. With the factor weights found by using fuzzy AHP, it can be determined which factors cause more cyber risk in the digital supply chain. In addition, the cyber-resilient capability maturity level can be identified. Although the model was developed and tested for use in one particular company, it can also be used, with slight modification, in any company.

For further study, more methodological work is needed to determine how to apply the cyber resilient capability maturity model in digital supply chain for small and medium enterprises. The researchers have also modified the capability maturity assessment system for evaluating the level of the cyber-resilient capability maturity model of digital supply chain in actual practice.

ACKNOWLEDGMENT

The National Research Council of Thailand supports this work through the College of Logistics and Supply Chain, Sripatum University, Bangkok, Thailand.

References

[1] M. Warren, and W. Hutchinson, "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management*, vol. 30 Iss. 7/8, pp.710 -716, 2000.

[2] C.W. Zobel, and L. Khansa, "Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks," *Decision Sciences*, vol.43, no.4, pp.687-710, 2012.

[3] M. Levi, "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues," *Crime, Law and Social Change*, vol.67, no.1, pp.3-20, 2016.

[4] H.S. Brar, and G. Kumar, "Cybercrimes: A Proposed Taxonomy and Challenges," *Journal of Computer Networks and Communications*, 2018.

[5] T. Rusi, and M. Lehto, "Cyber threats mega trends in cyber space," In *ICMLG 2017 5th International Conference on Management Leadership and Governance. Academic Conferences and Publishing Limited*, pp. 323, 2017

[6] B. Gaudenzi, and G. Siciliano, "Managing IT and Cyber Risks in Supply Chains," *Supply Chain Risk Management*, pp. 85–96, 2017.

[7] S. Papastergiou, and N. Polemi, "MITIGATE: A dynamic supply chain cyber risk assessment methodology," In *Smart Trends in Systems, Security and Sustainability*, pp.1-9, Springer, Singapore, 2018.

[8] G. Büyüközkan, and F. Göçer, "Digital Supply Chain: Literature review and a proposed framework for future research," *Computers in Industry*, vol.97, pp.157–177, 2018.

[9] I. Dmitry, D. Alexandre, and S. Boris, "The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics," *International Journal of Production research*, vol.57, no. 3, pp.829-846, 2019.

[10] Humphrey, *Cmm, IEEE*, vol.1, 1989.

[11] P.D. Curtis, and N. Mehravari, "Evaluating and improving cybersecurity capabilities of the energy critical infrastructure," In *Technologies for Homeland Security (HST), 2015 IEEE International Symposium*, pp. 1–6, 2015.

[12] A. Ghadge, M. Weiß, N.D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: A review and research agenda," *Supply Chain Management: An International Journal*, 2019.

[13] C. Colicchia, A. Creazza, and D.A. Menachof, "Managing cyber and information risks in supply chains: insights from an exploratory analysis," *Supply Chain Management: An International Journal*, 2019.

[14] A. Wibowo, and J. Taufik, "Developing a self-assessment model of risk management maturity for client organizations of public construction projects: Indonesian context," *Procedia engineering*, Vol. 171, pp. 274-281, 2017.

[15] R. Brennan, J. Attard, and M. Helfert, "Management of data value chains, a value monitoring capability maturity model," 2018.

[16] C. Klötzer, and A. Pflaum, "Toward the development of a maturity model for digitalization within the manufacturing industry's supply chain," 2017.

[17] K. Boonsita Kitisrivorapot, "Selection of Logistics Service Providers for Hana Microelectronics Public Company Limited, the Northern Region Industrial Estate, by Applying Analytic Hierarchy Process and Fuzzy Set Theory for Decision Making," *Graduate School, Chiang mai University*, 2011.

[18] M. Phayung, "Fuzzy Systems and Neural Network," Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, 2011.

[19] Yasemin, and F.G. Wu, "Global supplier selection: a fuzzy-AHP approach," *International Journal of Production Research*, vol.46, pp.3825-3857, 2004.

[20] Y.C. Erensal, T. Ö zcan, and M.L. Demircan, "Determining key capabilities in technology management using fuzzy analytic hierarchy process: A case study of Turkey," *Information Sciences*, vol. 176, pp. 2755–2770, 2006.

[21] D.Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *European Journal of Operational Research*, vol.95, pp.649–655, 1996.

[22] D.Y. Chang, "Extent Analysis and Systematic Decision, Optimization Techniques and Application," *World Sciencific*, Singapore, p.352, 1992.

[23] Framework for Improving Critical Infrastructure Cybersecurity version 1.1. National Institute of Standards and Technology. Available at: `https://doi.org/10.6028/NIST.CSWP.04162018` [Accessed:25/11/19].

[24] J.W. Candra, O.C. Briliyant, and S.R. Tamba, "ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study : XYZ institute)," *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, 2017.

[25] M.I. Tariq, and S. Vito, "Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing," *International Conference on Information Systems Security and Privacy*, vol. 2. SCITEPRESS, 2016.

[26] J. Gutiérrez-Martínez, M. A. Núñez-Gaona, and H. Aguirre-Meneses, "Business Model for the

rity of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard," *Journal of Digital Imaging*, vol.28, no.4.

[27] E. Humphreys, "The Future Landscape of ISMS Standards," *Datenschutz und Datensicherheit-DuD*, vol. 42, no.7, pp. 421-423, 2018.

[28] S.V. Aleksandrova, M.A. Aleksandrov, and V.A. Vasiliev, "Business Continuity Management System," *2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)*, IEEE, 2018.

[29] Y. Muflihah, and P.S. Apol, "A basic element of it business continuity plan: systematic," *Jurnal Informatika*, vol.12, no.1, pp.-17-23, 2018.

[30] R. Koen, S. R. Von, and M. Gerber, "ICT Readiness for Business Continuity in local government," *2016 IST-Africa Week Conference*, 2016.

[31] J. Meszaros, and A. Buchalcevova, "Introducing OSSF: A framework for online service cybersecurity risk management," *Computers & Security*, vol.65, pp.300–31, 2017.

[32] M.F. Blos, S. L. Hoeflich, E.M. Dias, and H.-M. Wee, "A note on supply chain risk classification: discussion and proposal," *International Journal of Production Research*, vol.54, no.5, pp.1568–1569, 2015.

[33] S. Papastergiou, and N. Polemi, "MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology," *Smart Trends in Systems, Security and Sustainability*, pp.1–9, 2017.

[34] M.F. Blos, and S.L. Hoeflich, "Supply chain risk management framework for virtual enterprises: a theoretical approach," *Unisanta Science and Technology*, vol.5, no.3, pp.161-166, 2017.

[35] D. Proenca, J. Estevens, R. Vieira, and J. Borbinha, "Risk Management: A Maturity Model Based on ISO 31000," *2017 IEEE 19th Conference on Business Informatics (CBI)*, 2017.

[36] U.R. De Oliveira, F.A.S. Marins, H.M. Rocha, and V.A.P., Salomon, V. A. P., "The ISO 31000 standard in supply chain risk management," *Journal of Cleaner Production*, vol.151, pp.616–633, 2017.

[37] B. Massimino, J.V. Gray, and Y. Lan, "On the Inattention to Digital Confidentiality in Operations and Supply Chain Research," *Production and Operations Management*, vol. 27, no,,pp. 1492–1515, 2018.

[38] A. Yeboah-Ofori, and S. Islam, "Cyber Security Threat Modeling for Supply Chain Organizational Environments," *Future Internet*, vol.11, no.3, pp.1-25, 2019.

[39] U. Naris, P. Prasong, and M. Tharinee, "The development of cyber resilient capability maturity model of digital supply chains for managing the digital business continuity in small and medium-sized enterprises," Doctor of philosophy thesis, College of Logistics and supply chain, Sripatum University, 2019.

[40] J.L. Fleiss, "Measuring nominal scale agreement among many raters," Psychological Bulletin. 76, 378 – 382, 1971.

[41] J. L. Fleiss, B. Levin, and M. C. Paik, "Statistical Methods for Rates and Proportions," Third Edition. New Jersey: John Wiley & Sons, Inc, 2003.

[42] P. Ziemba, J. Watróbski, J. Jankowski, and M. Piwowarski, "Research on the Properties of the AHP in the Environment of Inaccurate Expert Evaluations," In Selected Issues in Experimental Economics; Springer: Cham, Switzerland, pp. 227–243, 2016.

[43] M.S. Shu, C.H. Cheng, and J.R. Chang, "Using intuitionistic fuzzy set for fault-tree analysis on printed circuit board assembly." Microelectron. Reliab. 46, 2139–2148 2006.

Naris Uraipan received his B.Eng. in Electrical Engineering from Mahanakorn University of Technology, Bangkok, Thailand, in 1994, and his M.B.A. in Money and Banking from Sripatum University, Bangkok, Thailand, in 1998. He currently is a Ph.D. in the Logistics and Supply Chain Management from Sripatum University. He has worked in the ERP software development industry for more than ten years as a system analyst, business analyst, and project manager with more than 30 companies and is also a lecturer at Western University, Thailand. His research interests include digital supply chain management and cyber-resilience. His current main research is focused on cyber-resilience in digital supply chain towards business continuity management for SMEs.

Prasong Praneetpolgrang received his B.Sc. 1st Hons in Electrical Engineering from the Royal Thai Air Force Academy, Bangkok, Thailand. He received his M.S. in Computer Engineering, his M.S. in Electrical Engineering, and his Ph.D. in Computer Engineering from the Florida Institute of Technology, Florida, USA. He currently has the rank of Professor at the School of Information Technology, Sripatum University, Thailand. His research interests are in the areas of Cybersecurity, Cloud Computing, IoT/Big Data Analytics, and Blockchain. Dr. Praneetpolgrang has more than 160 published articles in these areas. He has served on program committees of both national and international conferences on Computer Science and Engineering, Information Technology, and e-Business. He is also a member of IEEE and ACM.

Tharinee Manisri received her M.Eng. and her D.Eng in Industrial Engineering from Kasetsart University, Thailand, in 2003 and 2009, respectively. She is a Dean of the College of Logistics and Supply Chain at Sripatum University, Thailand. Her research interests are in the areas of developing algorithms for complex, real-world logistic problems using heuristics and metaheuristic techniques. She is also interested in simulation modeling and analysis. It is important to her that her research is directly applicable to practical problems. She currently is working in the areas of developing algorithms for the vehicle routing problem.