Towards Security Effectiveness Evaluation for Cloud Services Selection following a Risk-Driven Approach

Sarah Maroc[1], Jian Biao Zhang[2]
Beijing Key Laboratory of Trusted Computing
Faculty of Information Technology
Beijing University of Technology
Beijing, 100124, China

***Abstract*—Cloud computing is gaining a lot of popularity with an increasing number of services available in the market. This has rendered services selection and evaluation a difficult and challenging task, particularly for security-based evaluation. A key problem with much of the literature on cloud services security evaluation is that it fails to consider the overall evaluation context given the cloud characteristics and the underlying influence factors including threats, vulnerabilities, and security controls. In this paper, we propose a holistic risk-driven security evaluation approach for cloud services selection. We first use fuzzy DEMATEL method to jointly assess the likelihood and impact of threats with respect to the cloud service types, the exploitability of vulnerabilities to the identified threats, and the effectiveness of security controls in mitigating those vulnerabilities. Consequently, the overall diffusion of risk is captured via the relations across these concepts, which is leveraged to filter and prioritize the most critical security controls. The selected controls were then weighted using a combination of fuzzy DEMATEL and fuzzy ANP methods based on several factors, including their effectiveness in preventing the identified risks, user's preferences and level of control (i.e., responsibilities). The latter denotes how much control a cloud user is transferring to the cloud provider. To enhance the reliability of the results, the subjective weights were integrated with objective weights using the Entropy method. Finally, the TOPSIS method was employed for services ranking and the Improvement Gap Analysis (IGA) method was leveraged to provide more insights on the strength and weaknesses of the selected services. An illustrative example is given to demonstrate the application of the proposed framework.**

Keywords*—*Cloud computing; cloud services selection; decision-making; risk-driven assessment; security evaluation

I. Introduction

Cloud computing has become increasingly popular due to its cost-effective and resources efficient services. It is a "model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction" [1]. With the high number of cloud services available in the market, services selection and evaluation has become a significant challenge to users, particularly security evaluation.

The first and most critical step in any evaluation process is criteria identification. It describes the characteristics of the evaluation target that are of interest for the evaluation, thus it needs to be context specific. This is especially important in the cloud, given that the security threats, vulnerabilities, and controls differ from one service model to another. For example, IaaS suffers mainly from issues related to virtualization like hardening the host and securing inter-host communications. PaaS issues are more concerned with authentication and authorization. As for SaaS, the secure composition of the services is a critical area of concern [2]. Therefore, the selection of the critical security controls in the cloud needs to consider the overall dependencies between the vulnerabilities, threats, and the particular cloud services characteristics.

Various services selection methods have been proposed in the literature to support users in finding the most suitable services. However, in most of the available methods, the evaluation criteria were generally determined based on literature and experts' surveys (e.g., [3]–[8]). Other approaches have leveraged some recent standardization efforts such as the SMI framework [9] (e.g., [10], [11]), and CSA's CCM framework [12] (e.g., [13], [14]). Still, the evaluation criteria are generally specified in a rigid way for all cloud service models without considering the change in threats, and controls when applied to different cloud service models, rendering the evaluation process inefficient.

Indeed, an extensive list of criteria is important for a comprehensive evaluation. However, security evaluation is a challenging task that involves significant effort, in terms of both computational and human resources. Therefore, a minimal and representative set of evaluation criteria is more critical in a given context. This permits to focus on the situation and eliminate unnecessary tasks. Restricting the list of evaluation criteria will also help in the criteria weighting process. Most available weighting techniques such as AHP [15] and ANP [16] do not scale well with a large set of evaluation criteria, because of the large number of pairwise comparisons to be performed. For example, in the case of 20 evaluation criteria, 190 pairwise comparisons need to be performed using AHP method, which is both time consuming and a cumbersome task. The SMI framework [9] and CCM framework [12], which are widely used as evaluation criteria for cloud services selection, contain in total 51 attributes and 133 sub-controls, respectively. Thus, due to scalability issues, there is a need for a mechanism in place to first prioritize and select the most critical criteria given the evaluation context.

There exist several security standards on risk management such as NIST CRMF [17], which serve as good references for the selection of the baseline security controls. However, in these frameworks, the selection of the critical security controls is conducted in a purely qualitative way mostly relying on the expertise of the decision makers. With this challenge in mind, in this paper, we focus on selecting and prioritizing the critical security services in the cloud environment in a quantitative way following a risk management approach.

Following a risk-driven approach for cloud services selection helps in assessing the effectiveness of the security controls. Current cloud services evaluation and selection methods are mostly targeting the sufficiency and efficiency of the security controls, which focus on determining whether the security service performances meet customer's requirements. However, the presence of the security controls within the cloud service system does not necessarily mean it is always secure. Effectiveness measurement can only be appraised with sufficient knowledge about the threats and vulnerabilities [18]. Thus, adopting a risk-driven approach in selecting the evaluation criteria considering the relevant vulnerabilities and threats likelihoods, would consequently enable measurement of the effectiveness of the security controls. We further assess the extent of the effectiveness of the implemented security controls by analyzing their performance gaps against an assumed ideal using improvement gap analysis (IGA) method [19].

Another essential step related to the evaluation process is the weighting of the criteria. Current weighting approaches are generally based on the subjective users' preferences, criteria dependencies, or on the objective analysis of the evaluation data. An important factor that is not considered but highly relevant in the cloud context is the cloud users' varying degree of control over the implementation and management of the security services. In the cloud, the security responsibilities are shared among the cloud actors and depend on the cloud deployment model (i.e., public or private), service model (i.e., IaaS, PaaS, and SaaS), and the security control type. In the IaaS, the consumer is mostly responsible for securing the virtualized resources, application and data, while the cloud provider is responsible for securing the physical infrastructure. Contrary, in the SaaS, most of the security responsibilities are shifted to the provider side, leaving the consumer only responsible for the data and some minimal application management [17]. Accordingly, more importance should be assigned to the particular security control when the cloud user loses more control over its management to emphasis the responsibility for the associated security risks.

To summarize, the main contributions of this paper are:

1) Context-aware and risk-driven criteria selection. We benefit from our earlier work [20] on criteria selection for cloud services evaluation, with enhancements on the approach to address the scalability issues and account for the uncertainty and subjectivity of the process. In this paper, Fuzzy DEMATEL [21] method is used to identify the causal relationships between the cloud service types, threats and vulnerabilities, and the security controls. Fuzzy DEMATEL requires less comparisons compared to other dependency-aware techniques like ANP or AHP ($n(n-1)/2$). The goal is not to blindly use all the criteria that exist in the literature, but instead to identify those that are most critical to the context of the evaluation considering the characteristics of cloud service types and the overall evaluation context. This allows to reduce the effort required in the evaluation.

2) Criteria weighting considering more comprehensive set of factors. The proposed approach is distinguished from other existing methods in that it considers multiple factors in the weighting of criteria, namely user's preferences, criteria interdependencies, in addition to the user's level of control (i.e., responsibilities). The user's level of control reflects the degree of loss of control over the management and implementation of the security services, which represent one of the novelties of the proposed approach. Criteria weighting was performed using fuzzy DEMATEL and fuzzy ANP methods. The resultant subjective weights were further combined with objective weights based on Entropy method to obtain more accurate and less sensitive results to user's preferences or unreasonable criteria prioritization.

3) Effectiveness-driven evaluation following a risk-driven approach and gap analysis for performance improvement. The proposed framework attempts, on one hand, to enhance the efficiency of the evaluation process by reducing the set of evaluation criteria to the core attributes. On the other hand, it drives for an effectiveness-based evaluation of security services by assessing the effectiveness of the security controls in mitigating the potential threats and vulnerabilities, thus the risks prevented. Furthermore, the extent of the effectiveness of the implemented security controls are assessed using the improvement gap analysis (IGA) method [19].

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 presents the proposed framework. Section 4 demonstrates the effectiveness of the proposed approach through a case study. Section 5 concludes the paper.

II. Related Work

In this section, we will review the related work on cloud services evaluation with the focus on security-driven studies and dependency-aware cloud services selection approaches.

A. Cloud Services Security-based Evaluation

Security evaluation, in our context, aims to provide a quantification of the security level of cloud services in a way to enable comparison between different services offerings. Cloud services evaluation has mostly targeted measurable attributes such as performance and availability, with less focus on security [22], [23]. Although security is mentioned in almost every study on cloud services evaluation, most of the studies do not of focus on security related attributes and influence factors.

Among the few works focused on security, Mouratidis et al. [24] proposed a holistic framework starting from the elicitation of the security and privacy requirements to the selection of cloud services providers. Luna et al. [13] presented

two evaluation techniques, namely Quantitative Policy Trees (QPT) and Quantitative Hierarchy Tree (QHP) for assessing the security level of cloud providers as per the claimed SLAs with respect to users' requirements. The QPT weighted the criteria and aggregated alternatives performances in an ad-hoc manner, whereas QHP employed the AHP technique for criteria weighting and ranking of alternatives. Modic et al. [14] proposed a cloud security assessment technique called Moving Intervals Process (MIP) that aimed at decreasing the time complexity of the assessment algorithm by separating scores for services providers that can fulfill users' needs from scores of those that are under-provisioning. Halabi and Bellaiche [8] proposed a security self-evaluation methodology for cloud providers using a variety of security metrics. In another work from the same authors [3], the security level of cloud service providers was quantified with respect to the traditional security attributes (CIA triad), namely: confidentiality, integrity, and availability. The best solution was then obtained using a linear multi-objective optimization technique that aims at minimizing the dissatisfaction factors. Alabool and Mahmood [25] proposed a framework for ranking IaaS cloud providers and used the IPA method for ranking the unimproved gaps to provide insights on how to better improve the cloud services.

In the above studies and most available cloud services evaluation approaches, an extensive list of criteria is employed in the evaluation, either identified through literature and experts survey, or by leveraging existing frameworks such as the SMI framework [9] or CCM framework [12]. However, these frameworks target cloud services in general and do not consider the change in threats and measures when applied to different cloud deployment models and service types. Besides, the long list of criteria (e.g., CCM framework includes 16 control domains with more than 130 security sub-controls) renders the weighting process a tedious task. Furthermore, security evaluation constitutes only a part of the overall trustworthiness evaluation of cloud services. A variety of other evaluation criteria including financial and performance attributes are of interest. Thus, prioritizing and filtering the criteria to a minimum and representative set is important for practical and efficient evaluation.

There exists some general security frameworks and guidelines for selecting baseline security controls such as NIST cloud-adapted risk management framework (CRMF) [17]. However, existing standards lack a quantitative and systematic method of how controls should be selected. In [26], the authors proposed a quantitative framework for prioritizing the security controls with respect to the identified vulnerabilities and threats given the severity and cost of the remediation effort. Nevertheless, the proposed framework targets the security information domain in general and thus fails to consider the specific characteristic of the cloud environment including the influences of cloud service models on the potential threats and vulnerabilities, as well as the shared responsibility of cloud users in the process. In the next section, we will discuss some of the works addressing dependency relations in cloud security evaluation literature.

B. Dependency-Aware Cloud Security Evaluation Methods

The relationships between the evaluation concepts are often neglected in existing cloud evaluation studies. To address this lack, Sun et al. [27] applied fuzzy measure and Choquet integral to measure and aggregate non-linear relations between criteria. Taha et al. [28] proposed a framework for measuring the structural dependencies between cloud security services, which were then used as weights for the evaluation criteria. However, the proposed approach only considered the relations between the services in a hierarchical structure. In [29], The influences of attributes on the overall quality of services were integrated with the user's preferences in order to calculate the final weights of attributes using the ANP method to allow for a flexible network-like structure representation. In [30], the authors employed fuzzy-ANP to calculate criteria weights for cloud services evaluation. In [31], the authors examined the causal relationships between the criteria using fuzzy DEMATEL-based ANP technique to determine the influence and the weights of the criteria. VIKOR method was then employed to rank the alternatives and identify the weaknesses to help improve service performances. Several other works have combined DEMATEL and ANP to handle the dependencies between the evaluation criteria in the cloud such as [32] and [33]. However, the above-reviewed methods do not consider the dependencies between criteria from a risk perspective.

In [34], the authors applied DEMATEL-based ANP to account for the dependencies between the security controls, which were identified following risk assessment procedure. Also, in [35], a method was proposed for evaluating the risk levels of information security. DEMATEL was first used to analyze the interrelations among security control areas. The risk likelihood ratings were then obtained using the ANP method. Still, these frameworks only considered the dependencies between the security controls directly. That is, the influence of threats and vulnerabilities were not jointly included in the quantitative analysis. Besides, the above methods were applied to security information in general, and hence lack the specific characteristic of the cloud environment. That is the change in threats, vulnerabilities, and controls when applied to different cloud deployment and service models types.

Overall, while some researchers have considered the dependencies between the evaluation criteria, they have ignored the characteristics of cloud service model types, as well as the underlying risk factors (threat likelihood, vulnerability relevance, and control effectiveness). Besides, the dependencies between criteria, when considered, were only addressed as part of the weighting process. In contrast, in this paper, we leverage the causal relationships between the cloud service types, threats vulnerabilities and security controls to extract the minimum and critical set of the evaluation criteria. The dependency values were then integrated with users' preferences and their level of control (i.e., responsibilities) to obtain the total subjective weights, which were then combined with objective weights to improve the reliability and accuracy of the approach. The proposed framework attempts to enhance the efficiency of the evaluation process by reducing the set of evaluation criteria to the core factors, and drive for effectiveness-based evaluation by understanding the extent of the effectiveness of the implemented security controls in preventing the risks.

III. Proposed Framework

The proposed framework, as shown in Fig. 1, consists of five main phases: context establishment, criteria selection, criteria weighting, services ranking, and finally performance improvement and gap analysis. The detailed description of the steps at each phase is described in the following sections.

A. Context Building and Criteria Selection

The concepts model follows a risk perspective by modeling the threats, vulnerabilities, and security controls, while considering the characteristics of the cloud service types. The problem can be formally modeled as follows. Let $S = \{s_1, s_2, \dots, s_w\}$ be the cloud service model types of the evaluation target, $T = \{t_1, t_2, \dots, t_p\}$ the threats, $V = \{v_1, v_2, \dots, v_q\}$ the vulnerabilities, and $C = \{c_1, c_2, \dots, c_n\}$ the security controls representing the evaluation criteria.

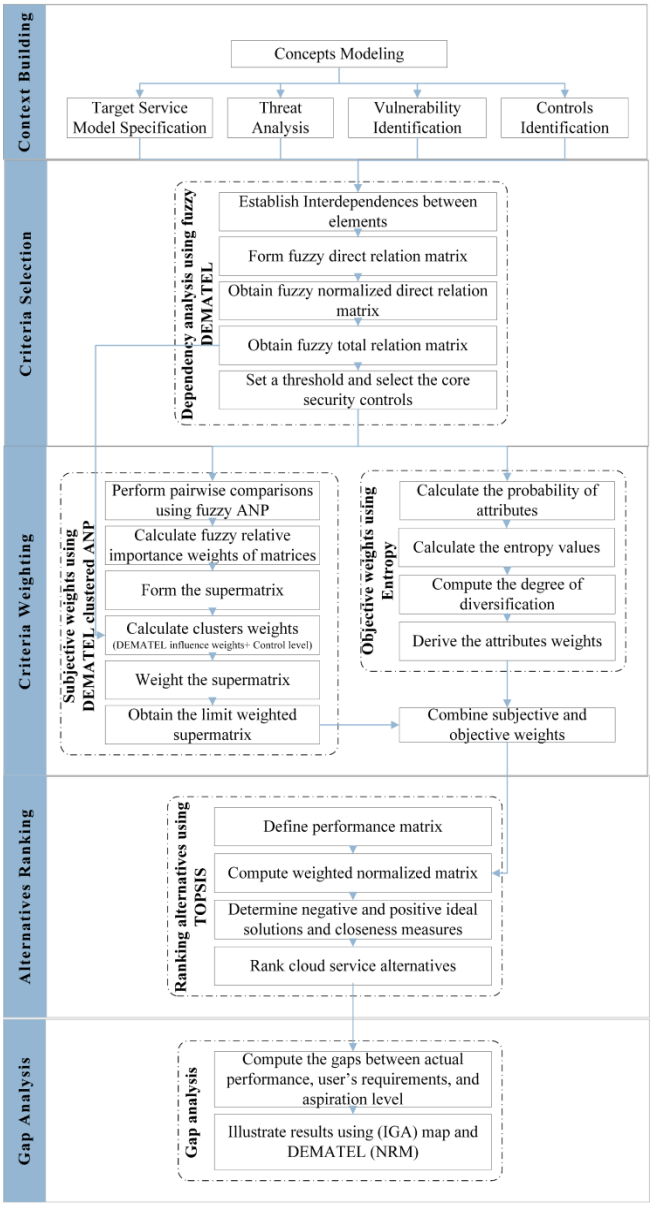

Fig. 1. The Conceptual Model of the Proposed Framework.

For criteria selection, DEMATEL [21] method is used to analyze the dependencies (direct and indirect) between the service model, potential threats, exploited vulnerabilities, and the appropriate security controls. This way, we can jointly assess the likelihood of threats given the service type, the relevance of various vulnerabilities to the identified threats, and the effectiveness of the security controls in mitigating the vulnerabilities. Consequently, the overall diffusion of risk is captured via the relations and dependencies across these concepts, which will be used to filter and prioritize the critical security controls that contribute the most to the evaluation. To cope with the fact that human judgment is often uncertain and hard to estimate by exact numerical values. fuzzy theory [36] is applied to the DEMATEL method. The output at this stage is a list of the minimal and critical security controls judged necessary and sufficient for an effective and efficient evaluation of cloud services. The steps are as follows.

Step 1. Establishing the dependencies between elements and forming the fuzzy direct-relation matrix. The direct-relation matrix $\tilde{Z}$ is constructed through pairwise comparison among the elements in which $\tilde{z}_{ij} = (l_{ij}, m_{ij}, u_{ij})$ indicates the degree to which the element i affects element j as ascertain by experts. It is assumed that a consensus of opinions exists among experts in the evaluation process.

$$\tilde{Z} = \begin{array}{c} \\ S \\ \\ \\ T \\ \\ \\ \\ V \\ \\ \\ C \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccccccc} S & & & T & & & V & & & C & & \end{array} \\ \begin{array}{cccccccccccc} s_1 & \cdots & s_w & t_1 & \cdots & t_p & v_1 & \cdots & v_q & c_1 & \cdots & c_n \end{array} \\ \begin{bmatrix} 0 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \tilde{z}_{ij} \\ \vdots & & & & & & & & & & & \cdot \\ \tilde{z}_{ij} & & & & & & & & & & & \cdot \\ \cdot & & & \cdot & & & & & & & & \cdot \\ \cdot & & & & \cdot & & & & & & & \cdot \\ \cdot & & & & & \cdot & & & & & & \cdot \\ \cdot & & & & & & \cdot & & & & & \cdot \\ \cdot & & & & & & & \cdot & & & & \cdot \\ \cdot & & & & & & & & \cdot & & & \cdot \\ \cdot & & & & & & & & & \cdot & & \cdot \\ \cdot & & & & & & & & & & & \cdot \\ \tilde{z}_{ij} & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix} \end{array} \quad (1)$$

Fig. 2 illustrates the graphical structure of the concepts and their relations.

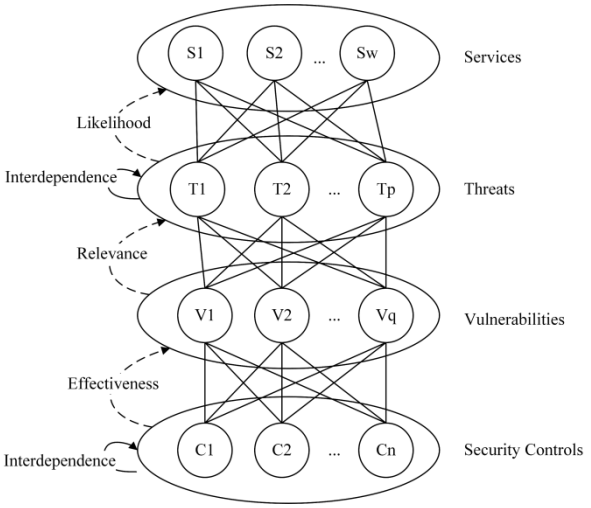

Fig. 2. Criteria Selection Problem Structure of the underlying Factors and Relations.

TABLE. I. INFLUENCE MEASURES USING LINGUISTIC TERMS.

Linguistic terms	Linguistic values
No influence (N)	(0, 0, 0.25)
Low influence (L)	(0, 0.25, 0.5)
Medium influence (M)	(0.25, 0.5, 0.75)
High influence (H)	(0.5, 0.75, 1)
Very high influence (VH)	(0.75, 1, 1)

The fuzzy linguistic scale is used for measuring the influence degree with its equivalent triangular membership function, as shown for example in Table I.

Step 2. Calculating the normalized fuzzy direct-relation matrix. On the base of the direct-relation matrix $\tilde{Z}$, the normalized direct-relation matrix $\tilde{X}$ can be obtained as follows.

$$\tilde{z}_{ij} = (l_{ij}, m_{ij}, u_{ij}) \text{ and } s = \frac{1}{\max\limits_{1\le i\le m} \sum_{j=1}^{m} u_{ij}}, \text{ then} \quad (2)$$

$\tilde{X} = \tilde{Z} \times s$, where

$$\tilde{X} = [\tilde{x}_{ij}]_{m\times m} = \tilde{z}_{ij} \times s = (l_{ij} \times s, m_{ij} \times s, u_{ij} \times s)$$

Step 3. Calculating the fuzzy total-relation matrix. The fuzzy direct/indirect relation matrix, known as the total relation matrix can be obtained as follows.

$$\tilde{T} = \lim_{k\to\infty} (\tilde{X} + \tilde{X}^2 + \cdots + \tilde{X}^k) = \tilde{X}(I - \tilde{X})^{-1} \quad (3)$$

$\tilde{T} = [\tilde{t}_{ij}]_{m\times m}$, $\tilde{t}_{ij} = (\grave{l}_{ij}, \grave{m}_{ij}, \grave{u}_{ij})$, where

$[\grave{l}_{ij}] = \tilde{X}_l(I - \tilde{X}_l)^{-1}$, $[\grave{m}_{ij}] = \tilde{X}_m(I - \tilde{X}_m)^{-1}$, $[\grave{u}_{ij}] = \tilde{X}_u(I - \tilde{X}_u)^{-1}$

Where I is the identity matrix.

Step 4. Setting a threshold value and selecting the critical security controls. A threshold value α is set to filter minor effects and reduce the complexity of the decision process. Only elements whose influence value in the total matrix is higher than the threshold value can be chosen. The influence values in matrix $\tilde{T}$ is reset to zero if its values are less than α. The new matrix is called the α-cut total-influence matrix $\tilde{T}_\alpha$. Based on this idea, we exclude the security controls with negligible effects and select the controls with the most influence relationships. The threshold value can be decided by experts or using analytical methods such as the mean value of the total influence matrix. To simplify the calculation, we first defuzzify the total fuzzy relation matrix $\tilde{T}$. Several defuzzification methods exist, we chose the center of area (CoA) method, as it is the most commonly used method. The formula is as follows.

$$t_{ij} = \frac{(\grave{u}_{ij} - \grave{l}_{ij} + \grave{m}_{ij} - \grave{l}_{ij})}{3} + \grave{l}_{ij} \quad (4)$$

The sum of rows R_i denotes the sum of direct and indirect effects of element i on the other elements. Whereas, the sum of columns D_j denotes the sum of direct and indirect effects that element j has received from the other elements. Consequently, $R_i + D_i$ denotes the strength of influences given and received, which represents the degree of the central role that element i plays in the decision-making process. If $R_i - D_i$ is positive than element i is affecting other elements (cause group), if negative, it is being influenced by the other elements (effect group). Furthermore, a visual causal diagram can be depicted by arranging $R_i + D_i$ values in x-axis and $R_i - D_i$ values on the y-axis.

B. Criteria Weighting

The selected security controls from the previous stage represent the top-level evaluation criteria (dimensions or clusters). These criteria are further divided into more fine-grained sub-criteria. The weights of criteria are calculated using subjective and objective methods. The subjective weights are determined based on the influence degree of the criteria, level of control, and their importance to the users. Fuzzy ANP method is used to assign the importance weights to the criteria through pairwise comparisons. However, contrary to the assumption of equal cluster's weight in traditional ANP, we use fuzzy DEMATEL influence degrees obtained previously combined with the level of control degree to weight the clusters. The obtained subjective weighs are further adjusted with objective weights using the entropy method to obtain more reliable results. The steps for weighting the criteria are described below.

Step 1. Performing pairwise comparison and obtaining priority vectors. The ANP method [16] combined with fuzzy set theory is employed to derive the subjective weights. The relations between clusters (i.e., dependence relations between security controls) are determined based on the previous results from the DEMATEL network relation map (NRM). Once the relations between criteria and sub-criteria are identified, users are asked to perform pairwise comparison between criteria. The importance values are assigned using triangular fuzzy numbers based on a 9-point scale (from equally important to extremely important) The priority vectors for each pairwise comparison matrix can be calculated using the eigenvalue method [16]. Then, the weighs are defuzzified in the same way as in Eq. (4). A consistency ratio of the pair-wise comparisons is calculated and should be less than 0.10 for the comparison to be acceptable. Otherwise, it is necessary to adjust the results. The priorities are gathered into the appropriate columns to build the supermatrix. The form of the supermatrix is as follows.

$$W = \begin{array}{c} \\ C_1 \\ \\ C_i \\ \\ C_n \\ \end{array} \begin{array}{c} \begin{array}{cccccc} C_1 & & C_j & & C_n \end{array} \\ \begin{array}{cccccc} c_{11} \cdots c_{1m_1} & & c_{1j} \cdots c_{jm_j} & & c_{1n} \cdots c_{nm_n} \end{array} \\ \begin{bmatrix} W_{11} & \cdots & W_{1j} & \cdots & W_{1n} \\ \vdots & & \vdots & & \vdots \\ W_{i1} & \cdots & W_{ij} & \cdots & W_{in} \\ \vdots & & \vdots & & \vdots \\ W_{n1} & \cdots & W_{nj} & \cdots & W_{nn} \end{bmatrix} \end{array} \quad (5)$$

Step 2. Obtaining the weights of clusters. In the traditional ANP, the weights of elements are divided by the number of clusters. This normalization method implies that the clusters are of equal weights (in our context the high-level security controls). However, in reality, the effect of each cluster on the

other clusters is different, and have been determined in the previous step using fuzzy DEMATEL method. Hence, these influence values are used in weighting the clusters, in addition to another factor, which is the level of control.

Step 2.1. Obtaining the influence degree of the clusters. The interdependencies between the clusters are already determined previously using DEMATEL, hence can be directly derived from the total influence matrix. Let $T^{\alpha SC}$ be the α-cut total-influence matrix for security controls. $t_{ij}^{\alpha SC}$ represents the degree of influence that the cluster i (i.e., security control) exerts on the cluster j.

Step 2.2. Determining the user's level of control degree. The degree of control (w^{cont}) denotes how much control a consumer is transferring to the cloud provider. Accordingly, more importance should be assigned to the particular security control when the cloud user loses more control over its management, as oppose to when the user has full control for its management. In NIST security reference architecture [17], the responsibility of the cloud user for each security component given the cloud deployment model and service type was defined as follows:

- Full responsibility. Meaning the user has full control over the management of the security control and thus, less importance value should be assigned to the security control. In this case ($w^{cont} = 0.25$).
- Shared responsibility. Meaning both the cloud user and provider share responsibility for managing the particular security control. In this case ($w^{cont} = 0.5$).
- Least responsibility. Meaning the provider has full control over the management of the security control. The consumer needs to negotiate with the provider to ensure that the requirements are met. Therefore, more importance value is assigned to the security control since the consumer loses the ability to implement it and manage it. In this case ($w^{cont} = 1$).

For example, the responsibility for the security component "Data Governance >Secure Disposal of Data" is a shared responsibility between the consumer and provider in the IaaS model ($w^{cont} = 0.5$), but needs to be implemented by the cloud provider in all other service models ($w^{cont} = 1$).

Step 2.3. Obtaining the total weights of the clusters. The weight of the cluster w^{cl} is the product of its influence degree $T^{\alpha SC}$ and level of control w^{cont}.

$$w_{ij}^{cl} = w_i^{cont} \times t_{ij}^{\alpha SC} \tag{6}$$

The clusters' weights are then normalized as follows.

$$w_{ij}^{cl} = \frac{w_{ij}^{cl}}{\sum_{j=1}^{n} w_{ij}^{cl}} \tag{7}$$

Step 3. Obtaining the weighted supermatrix. By combining the weights of the clusters with the unweighted supermatrix as defined in [37], we obtain the weighted supermatrix as follows.

$$W^s = w^{cl}W = \begin{array}{c} \\ C_1 \\ \\ C_i \\ \\ C_n \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} C_1 & & C_j & & C_n \\ c_{11} \cdots c_{1m_1} & & c_{1j} \cdots c_{jm_j} & & c_{1n} \cdots c_{nm_n} \end{array} \\ \begin{bmatrix} w_{11}^{cl} \times W_{11} & \dots & w_{j1}^{cl} \times W_{1j} & \dots & w_{n1}^{cl} \times W_{1n} \\ \vdots & & \vdots & & \vdots \\ w_{1i}^{cl} \times W_{i1} & \dots & w_{ji}^{cl} \times W_{ij} & \dots & w_{ni}^{cl} \times W_{in} \\ \vdots & & \vdots & & \vdots \\ w_{1n}^{cl} \times W_{n1} & \dots & w_{jn}^{cl} \times W_{nj} & \dots & w_{nn}^{cl} \times W_{nn} \end{bmatrix} \end{array} \begin{array}{l} \\ c_{11} \\ \vdots \\ c_{1m_1} \\ c_{i1} \\ \vdots \\ c_{im_1} \\ c_{n1} \\ \vdots \\ c_{nm_n} \end{array} \tag{8}$$

Step 4. Obtaining the limit weighted supermatrix. To obtain the global priorities, the weighted supermatrix is raised to the limiting powers $\lim_{k\to\infty} W_s^k$, where k is the number of powers.

Step 5. Calculating the objective weights. In the previous steps, criteria weights were calculated using subjective approaches and based on subjective factors that rely heavenly on decision-makers' opinions. To adjust the weights and help achieve more reliable results, we measure the weights using objective method, namely, the entropy method [38]. The entropy method determines the criterion's weight based on the information transmitted by that criterion. That is, if a particular criterion has similar values for all the alternatives, then this criterion has little importance in the decision-making. In contrast, the criterion that alternatives are most dissimilar should have the highest importance weight since it transmits more information and helps to differentiate between the different alternatives.

The projected outcomes P_{ij} of a criterion c_j is defined as:

$$P_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \tag{9}$$

x_{ij} is the performance of alternative i on criterion j.

The entropy is calculated as follows:

$$ET_j = -\left(\frac{1}{\ln m}\right) \sum_{i=1}^{m} P_{ij} \ln P_{ij} \tag{10}$$

The degree of diversification of the information provided by the criterion j is

$$d_j = 1 - ET_j \tag{11}$$

The entropy weight is then:

$$w_j^o = \frac{d_j}{\sum_{j=1}^{n} dj} \tag{12}$$

Step 6. Compute the final criteria weights. The final criteria weights are obtained by combing the subjective and objective weights as follows.

$$w_j = \alpha {w_j}^o + \beta {w_j}^s, \text{ where } \alpha + \beta = 1 \tag{13}$$

α and β can be adjusted accordingly to reflect the influence of subjective and objective weights on the decision-making.

C. Services Ranking

After weighing the criteria, the ranking of the best cloud service provider is performed using TOPSIS [39] method. TOPSIS method is based on the distance measure of an alternative from the ideal solution, taking into account both the closeness distance from the positive ideal solution (PIS) and the farthest distance from the negative ideal solution (NIS). TOPSIS was chosen as it best reflects the risk attitudes of decision-makers. The smaller the distance measure from PIS, the higher alternative preference to profit; whereas the larger the distance measure from NIS, the higher the alternative preference to avoid risk [39]. This approach is suitable for a security-based evaluation of cloud services as a risk avoider strategy. Due to space limitations, the steps of TOPSIS method can be found in [39].

D. Performance Improvement and Gap Analysis

Most existing cloud services evaluation studies have limited the evaluation process to the ranking of cloud services alternatives. However, the evaluation process also aims to help cloud service providers in improving their service performances. Few studies have attempted to identify what should be improved. Work in this direction was proposed by Alabool et al. [4]. They used the importance-performance analysis (IPA) [40] method to identify and rank the unimproved gaps. IPA is one of the most used methods to identify the strength and weaknesses of service performances. However, IPA has some limitations concerning the nonlinearity between the performance of attributes and customer satisfaction [19]. Aiming to overcome these problems, Tontini and Picolo [19] proposed the improvement gap analysis (IGA) method. IPA method compares the performance of the criteria with respect to their importance. In contrast, the IGA method compares the expected customer dissatisfaction if an attribute has a low performance with the expected customer satisfaction if the attribute is improved [19].

In traditional IGA, customers are asked to estimate their expected satisfaction and dissatisfaction with respect to each attribute and the actual attribute performance. The improvement gap (IG) for each attribute is calculated as the difference between the expected and the actual performance ($IG = EP - AP$) . The dissatisfaction is stated directly according to the expected impact on customer dissatisfaction if an attribute has low performance. In this paper, we calculate the improvement gap as the difference between the best available performance among all alternatives (BP_j) and the actual performance of the particular service AP_{ij} (Eq. 14). The value of the gap represents the scope of improvement needed in order to achieve high market competition. The best performance can also be replaced by the aspirational levels instead of the minimum-maximum values.

$$IG_{ij} = BP_j - AP_{ij} \text{ where} \quad (14)$$

$$BP_j = (\max(y_{ij}) | \, j \in Benefit, \min(y_{ij}) \, | \, j \in Cost))$$

y_{ij} represents the performance of alternative i on criteria j.

As for the dissatisfaction value (DP_{ij}), it is calculated based on its importance and the difference between user's requirements (RQ_j) and the actual service performance.

$$DP_{ij} = w_j * (RQ_j - AP_{ij}) \quad (15)$$

We plot the performance of alternatives into a two-dimensional graph as defined in the IGA method (see Fig. 3), showing each criterion's expected dissatisfaction on the y-axis with respect to the improvement gap on the x-axis. Attributes are classified into four categories: (1) critical for improvement, (2) keep as it is, (3) attractive, and (4), neutral [19].

An attribute is classified as critical to improve if its performance is lower than its competitors and doesn't satisfy the customer's requirements. It is classified as keep as it is when its performance is higher than the competition but not fully satisfying customers' requirements. Employing more resources to improve this attribute when its performance is already higher and deemed sufficient than the market, will not necessarily bring superior satisfaction to costumers, which may lead to a waste of resources. It is classified as attractive attribute if there is no strong dissatisfaction with its performance but there is still a high gap to the market, which if improved can bring superior customer satisfaction. It is classified as neutral when more improvement in this attribute will neither bring strong market differentiation nor superior customer satisfaction.

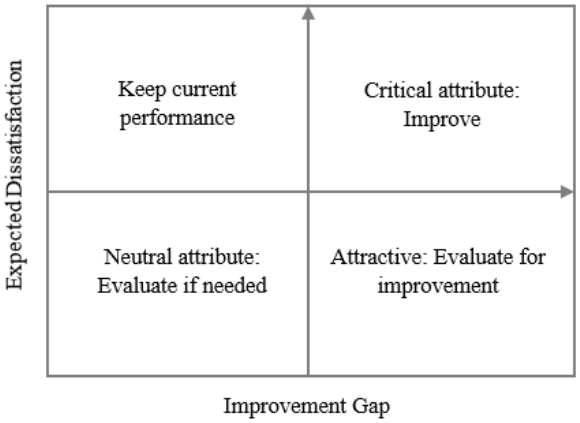

Fig. 3. Adapted Importance-Performance Analysis (IGA) Map [19].

IV. Case Study

To demonstrate the applicability of the proposed framework, we present an example of an evaluation for a SaaS service using data extracted from NIST security reference architecture [17] and CSA STAR repository, which is a public registry that documents the security controls provided by popular cloud computing. Following the proposed framework, the first phase involves establishment of the evaluation context, including the modeling of the target's service model, potential threats, vulnerabilities, and available security controls. For simplicity and without loss of generality, we consider the list of possible threats, vulnerabilities, and security controls presented in Table II. The next phase involves the selection of the critical security controls from the derived list of controls.

TABLE. II. EVALUATION CONCEPTS

(List of threats, vulnerabilities, and controls)	
	Designation
T1	Denial of service
T2	Data leakage
T3	Account or service hijacking
T4	Malicious insiders
T5	Cross VM attacks
T6	Sniffing /spoofing virtual networks
T7	Insecure VM migration
V1	Unlimited allocation of resources
V2	Incomplete data removal
V3	Authentication & authorization vulnerabilities
V4	VM co-residence
V5	Data collocation with weak separation
V6	Insecure interfaces and APIs
V7	Communication encryption vulnerabilities
C1	Application security
C2	Data security
C3	Identity & access management
C4	Human resources
C5	Virtualization security
C6	Security monitoring services
C7	Information system regulatory mapping

The initial fuzzy direct relation matrix of DEMATEL is shown in Table III using linguistic values from Table I. It depicts the different dependencies between the cloud service type, threats, vulnerabilities, and security controls considering several factors: the likelihood of a threat on SaaS service type, its impact, the relevance degree of the vulnerabilities to the identified threats, the effectiveness of controls on mitigating those vulnerabilities, and the interdependencies between the security controls. Following steps 2-4 (Section 3.1), we obtain the defuzzified total influence matrix, as shown in Table IV. The resultant security controls submatrix is depicted in bold in Table IV. We set a threshold value of (0.068); influence values less than the threshold are reset to zero. From the results, it can be concluded that criterion (C4) have less impact and relevance on the overall evaluation in this case study, thus it is excluded from the evaluation process. The resulting network relation (NRM) structure between the selected security controls (C1, C2, C3, C5, C6, and C7) is shown in Fig. 4.

After the selection of the critical security controls and establishing the network structure, we proceed to the next phase, criteria weighting. The control criteria are divided into more fine-grained sub-criteria. Table V presents the performance of alternatives with respect to the criteria. After performing the pairwise comparisons between each node in the cluster and the nodes in the related clusters as per the network structure, we obtain the initial supermatrix (step 1, section 3.2), as shown in Table VI.

TABLE. III. THE INITIAL FUZZY RELATION MATRIX

	SaaS	***T1***	***T2***	***T3***	***T4***	***T5***	***T6***	***T7***	***V1***	***V2***	***V3***	***V4***	***V5***	***V6***	***V7***	***C1***	***C2***	***C3***	***C4***	***C5***	***C6***	***C7***
SaaS	0	M	M	L	M	M	M	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T1	H	0	M		L	M	M	L	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T2	H	L	0	M	L	M	M	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T3	H	M	H	0	L	M	M	L	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T4	H	L	H	H	0	M	M	L	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T5	H	M	H	H	L	0	M	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T6	H	M	H	M	L	M	0	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
T7	H	L	H	M	L	M	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V1	0	H	M	M	L	L	L	L	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V2	0	M	M	L	L	L	L	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V3	0	H	H	H	H	H	H	H	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V4	0	M	H	H	L	H	M	H	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V5	0	L	H	H	L	H	M	M	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V6	0	H	M	M	H	M	H	H	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V7	0	M	M	M	H	M	H	H	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C1	0	0	0	0	0	0	0	0	H	H	M	M	H	H	M	0	L	H	L	M	M	L
C2	0	0	0	0	0	0	0	0	L	M	H	H	H	H	H	H	0	H	H	H	L	M
C3	0	0	0	0	0	0	0	0	M	H	M	M	M	H	M	H	H	0	H	H	L	M
C4	0	0	0	0	0	0	0	0	L	L	L	M	L	L	L	L	M	M	0	L	L	M
C5	0	0	0	0	0	0	0	0	L	H	H	H	H	M	H	H	H	M	M	0	M	M
C6	0	0	0	0	0	0	0	0	L	L	M	H	M	M	M	M	L	L	M	M	0	H
C7	0	0	0	0	0	0	0	0	L	M	M	M	M	M	M	L	L	M	H	M	M	0

TABLE. IV. THE DEFUZZIFIED TOTAL RELATION MATRIX

	SaaS	***T1***	***T2***	***T3***	***T4***	***T5***	***T6***	***T7***	***V1***	***V2***	***V3***	***V4***	***V5***	***V6***	***V7***	***C1***	***C2***	***C3***	***C4***	***C5***	***C6***	***C7***
SaaS	0.0393	0.0696	0.0799	0.0573	0.0646	0.0731	0.0730	0.0706	0.0225	0.0261	0.0261	0.0270	0.0265	0.0265	0.0261	0.0252	0.0244	0.0252	0.0256	0.0252	0.0234	0.0247
T1	0.0917	0.0346	0.0795	0.0739	0.0474	0.0730	0.0730	0.0533	0.0225	0.0261	0.0261	0.0270	0.0265	0.0265	0.0261	0.0252	0.0243	0.0252	0.0256	0.0252	0.0234	0.0247
T2	0.0917	0.0526	0.0444	0.0739	0.0474	0.0730	0.0730	0.0709	0.0225	0.0261	0.0261	0.0270	0.0265	0.0265	0.0261	0.0252	0.0243	0.0252	0.0256	0.0252	0.0234	0.0247
T3	0.0933	0.0711	0.0982	0.0397	0.0482	0.0743	0.0743	0.0546	0.0229	0.0266	0.0265	0.0274	0.0270	0.0270	0.0265	0.0256	0.0248	0.0256	0.0260	0.0256	0.0238	0.0251
T4	0.0950	0.0548	0.1003	0.0941	0.0311	0.0757	0.0757	0.0556	0.0233	0.0271	0.0270	0.0279	0.0275	0.0275	0.0270	0.0261	0.0252	0.0261	0.0265	0.0261	0.0243	0.0256
T5	0.0966	0.0733	0.1017	0.0951	0.0499	0.0414	0.0769	0.0740	0.0237	0.0275	0.0275	0.0284	0.0279	0.0279	0.0275	0.0265	0.0256	0.0265	0.0270	0.0265	0.0247	0.0260
T6	0.0949	0.0720	0.0999	0.0765	0.0490	0.0756	0.0401	0.0731	0.0233	0.0270	0.0270	0.0279	0.0275	0.0275	0.0270	0.0261	0.0252	0.0261	0.0265	0.0261	0.0243	0.0256
T7	0.0933	0.0535	0.0985	0.0752	0.0482	0.0743	0.0743	0.0366	0.0229	0.0266	0.0265	0.0274	0.0270	0.0270	0.0265	0.0256	0.0248	0.0256	0.0261	0.0256	0.0238	0.0252
V1	0.0418	0.0853	0.0758	0.0716	0.0447	0.0525	0.0525	0.0498	0.0156	0.0251	0.0251	0.0259	0.0255	0.0255	0.0251	0.0242	0.0234	0.0242	0.0246	0.0242	0.0225	0.0238
V2	0.0401	0.0659	0.0744	0.0525	0.0439	0.0511	0.0511	0.0669	0.0212	0.0186	0.0246	0.0254	0.0250	0.0250	0.0246	0.0238	0.0230	0.0238	0.0242	0.0237	0.0221	0.0233
V3	0.0591	0.0968	0.1115	0.1045	0.0898	0.1017	0.1017	0.0976	0.0258	0.0300	0.0239	0.0310	0.0305	0.0305	0.0300	0.0289	0.0280	0.0290	0.0294	0.0289	0.0269	0.0284
V4	0.0522	0.0744	0.1045	0.0983	0.0501	0.0963	0.0785	0.0933	0.0242	0.0281	0.0280	0.0229	0.0285	0.0285	0.0280	0.0270	0.0262	0.0271	0.0275	0.0270	0.0252	0.0266
V5	0.0488	0.0544	0.1013	0.0956	0.0483	0.0936	0.0758	0.0733	0.0233	0.0271	0.0271	0.0280	0.0215	0.0275	0.0271	0.0261	0.0253	0.0262	0.0266	0.0261	0.0243	0.0256
V6	0.0539	0.0932	0.0886	0.0823	0.0871	0.0799	0.0976	0.0940	0.0246	0.0286	0.0285	0.0295	0.0290	0.0230	0.0285	0.0275	0.0266	0.0276	0.0280	0.0275	0.0256	0.0270
V7	0.0522	0.0742	0.0872	0.0810	0.0863	0.0785	0.0963	0.0930	0.0242	0.0281	0.0280	0.0290	0.0285	0.0285	0.0220	0.0271	0.0262	0.0271	0.0275	0.0271	0.0252	0.0266
C1	0.0473	0.0560	0.0665	0.0609	0.0500	0.0593	0.0592	0.0592	0.0328	0.0896	0.0711	0.0733	0.0902	0.0905	0.0711	**0.0339**	**0.0498**	**0.0858**	**0.0524**	**0.0690**	**0.0642**	**0.0502**
C2	0.0543	0.0654	0.0775	0.0715	0.0583	0.0693	0.0693	0.0690	0.0496	0.0801	0.0968	0.0995	0.0985	0.0985	0.0968	**0.0939**	**0.0390**	**0.0943**	**0.0949**	**0.0936**	**0.0532**	**0.0743**
C3	0.0520	0.0628	0.0731	0.0670	0.0551	0.0647	0.0649	0.0648	0.0661	0.0965	0.0782	0.0809	0.0799	0.0974	0.0782	**0.0929**	**0.0904**	**0.0408**	**0.0939**	**0.0925**	**0.0522**	**0.0733**
C4	0.0400	0.0455	0.0534	0.0493	0.0402	0.0477	0.0474	0.0471	0.0406	0.0483	0.0482	0.0679	0.0491	0.0494	0.0482	**0.0465**	**0.0623**	**0.0642**	**0.0300**	**0.0468**	**0.0424**	**0.0629**
C5	0.0533	0.0639	0.0762	0.0700	0.0568	0.0679	0.0675	0.0676	0.0484	0.0959	0.0957	0.0984	0.0974	0.0797	0.0957	**0.0926**	**0.0895**	**0.0758**	**0.0764**	**0.0399**	**0.0695**	**0.0734**
C6	0.0462	0.0542	0.0642	0.0594	0.0482	0.0576	0.0572	0.0569	0.0437	0.0532	0.0708	0.0910	0.0720	0.0717	0.0708	**0.0678**	**0.0486**	**0.0513**	**0.0697**	**0.0681**	**0.0291**	**0.0848**
C7	0.0459	0.0540	0.0636	0.0585	0.0480	0.0567	0.0567	0.0564	0.0442	0.0706	0.0705	0.0732	0.0714	0.0714	0.0705	**0.0509**	**0.0495**	**0.0682**	**0.0872**	**0.0681**	**0.0639**	**0.0323**

TABLE. V. THE PERFORMANCES OF ALTERNATIVES WITH RESPECT TO THE CRITERIA

	C11	**C12**	**C13**	**C21**	**C22**	**C23**	**C31**	**C32**	**C33**	**C51**	**C52**	**C53**	**C61**	**C62**	**C63**	**C71**	**C72**	**C73**
A1	0.9	0.3	1	1	2	1	3	1	2	2	3	0	2	180	2	1	2	{HIPAA, ISO 27001}
A2	2	0..5	1	1	3	0	2	0	3	3	2	1	3	230	3	1	2	{HIPAA, ISO 27001}
A3	1	0.6	1	1	3	1	4	1	3	1	4	1	3	356	3	1	3	{HIPAA, ISO 27001, SOC, PCI}
A4	0.9	0.1	1	1	3	1	4	0	3	1	4	1	2	365	4	1	4	{HIPAA, ISO 27001, SOC, PCI}
A5	1	0.5	1	1	2	1	3	1	2	2	3	0	2	230	2	1	3	{HIPAA, ISO 27001, SOC}

TABLE. VI. THE SUPERMATRIX

	Goal	C11	C12	C13	C21	C22	C23	C31	C32	C33	C51	C52	C53	C61	C62	C63	C71	C72	C73
Goal	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C11	0.614	0	0.667	0.667	0.493	0.333	0.333	0.26	0.26	0.26	0.311	0.311	0.345	0	0	0	0	0	0
C12	0.117	0.667	0	0.333	0.196	0.333	0.333	0.328	0.328	0.328	0.196	0.196	0.109	0	0	0	0	0	0
C13	0.268	0.333	0.333	0	0.311	0.333	0.333	0.413	0.413	0.413	0.493	0.493	0.547	0	0	0	0	0	0
C21	0.345	0	0	0	0	0.75	0.667	0.493	0.493	0.493	0.249	0.249	0.359	0	0	0	0	0	0
C22	0.109	0	0	0	0.75	0	0.333	0.311	0.311	0.311	0.157	0.157	0.124	0	0	0	0	0	0
C23	0.547	0	0	0	0.25	0.25	0	0.196	0.196	0.196	0.594	0.594	0.517	0	0	0	0	0	0
C31	0.568	0.577	0.368	0.493	0.559	0.345	0.345	0	0.5	0.5	0.627	0.627	0.588	0	0	0	0.493	0.493	0.493
C32	0.075	0.081	0.082	0.311	0.089	0.109	0.109	0.8	0	0.5	0.094	0.094	0.089	0	0	0	0.311	0.311	0.311
C33	0.358	0.342	0.55	0.196	0.352	0.547	0.547	0.2	0.5	0	0.28	0.28	0.323	0	0	0	0.196	0.196	0.196
C51	0.311	0.493	0.333	0.493	0.4	0.196	0.493	0.594	0.594	0.594	0	0.5	0.5	0.493	0.493	0.493	0.493	0.493	0.493
C52	0.196	0.311	0.333	0.311	0.2	0.311	0.196	0.249	0.249	0.249	0.333	0	0.5	0.311	0.311	0.311	0.311	0.311	0.311
C53	0.493	0.196	0.333	0.196	0.4	0.493	0.311	0.157	0.157	0.157	0.667	0.5	0	0.196	0.196	0.196	0.196	0.196	0.196
C61	0.226	0	0	0	0	0	0	0	0	0	0.493	0.493	0.109	0	0.5	0.5	0	0	0
C62	0.101	0	0	0	0	0	0	0	0	0	0.311	0.311	0.163	0.5	0	0.5	0	0	0
C63	0.674	0	0	0	0	0	0	0	0	0	0.196	0.196	0.729	0.5	0.5	0	0	0	0
C71	0.14	0	0	0	0.14	0.196	0.169	0.328	0.328	0.328	0.126	0.126	0.493	0.379	0.493	0.493	0	0.5	0.25
C72	0.528	0	0	0	0.528	0.311	0.443	0.26	0.26	0.26	0.416	0.416	0.311	0.331	0.311	0.311	0.5	0	0.75
C73	0.333	0	0	0	0.333	0.493	0.387	0.413	0.413	0.413	0.458	0.458	0.196	0.289	0.196	0.196	0.5	0.5	0

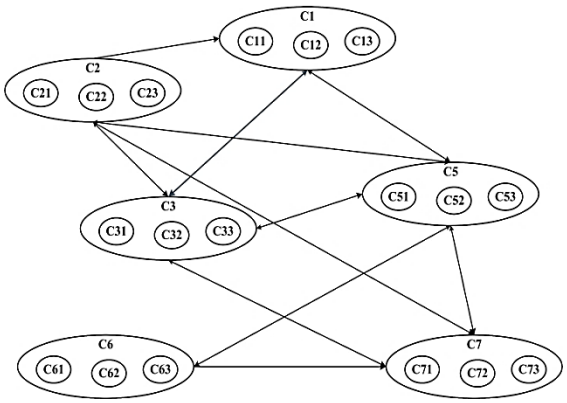

Fig. 4. Security Controls Network Structure based on Fuzzy DEMATEL Analysis.

Next, we calculate the weights of the control criteria to obtain the weighted supermatrix. As discussed in (step 2, section 3.2), the weight of a control criterion is the combination of its influence weight and the level of control granted to the user over its management. The influence weights of the control criteria are the α-cut total-influence sub-matrix for security controls. The level of control the user has over the criteria are defined as follows: $w_1^{cont} = 1, w_2^{cont} = 1, w_3^{cont} = 0.5, w_5^{cont} = 1,\ w_6^{cont} = 1, w_7^{cont} = 1$. The total weight of the cluster is the product of its influence degree and level of control. The clusters weights are used to calculate the weighted supermatrix and obtain the limit supermatrix to derive the total subjective weights of criteria. The subjective criteria weights are combined with objective weights following (steps 5-6, section 3.2). The coefficients are set to (α=β=0.5). The results are shown in Table VII.

TABLE. VII. THE OBJECTIVE, SUBJECTIVE, AND TOTAL CRITERIA WEIGHTS

Criteria		Subjective Weights	Objective Weights	Total Weights
Incident resolution	C11	0.0498	0.0326	0.0412
Incident response	C12	0.0418	0.0679	0.0548
Malware detection	C13	0.0691	0	0.0346
Data leakage prevention techniques	C21	0.0481	0	0.0241
Data deletion type	C22	0.0290	0.0103	0.0196
Encryption techniques	C23	0.0470	0.1255	0.0863
Authentication level	C31	0.1264	0.0161	0.0712
Third party authentication	C32	0.0478	0.2874	0.1676
Authentication mechanisms	C33	0.0748	0.0103	0.0425
VM encryption	C51	0.1320	0.0487	0.0903
Cryptographic hardware module protection level	C52	0.0766	0.0161	0.0463
Hypervisor access control policy	C53	0.0586	0.2874	0.1730
Log access availability	C61	0.0190	0.0115	0.0152
Logs retention period	C62	0.0129	0.021	0.0169
Network penetration tests	C63	0.0145	0.0199	0.0172
Independent audits	C71	0.0429	0	0.0215
Audit planning	C72	0.0525	0.0199	0.0362
Compliances	C73	0.0573	0.0255	0.0414

Next, we perform the ranking of alternatives following the TOPSIS method. The final results regarding the closeness distance to the ideal solution, and the final ranking are shown in Table VIII. The best alternative according to the results is (A3).

In the final phase, we perform the gap analysis for the best-selected alternative (A3) as discussed in section 3.4. The IGA map is shown in Fig. 5. We can further leverage the characteristics of DEMATEL to understand the cause-effect relationship between the different attributes based on the prominence level $(R_i + D_i)$ and relation level $(R_i - D_i)$ as discussed in (step 4, section 3.1). The relation level for the control criteria are as follows: $(R_i - D_i$: C1= -0.125, C2= 0.271, C3=0.119, C5=0.086, C6=0.153, C7=-0.083), calculated from the security control total influence matrix (Table IV). Both criteria C1 and C7 have a negative relation level, which means that they are effect criteria. The remaining criteria (C2, C3, C5, and C6) are cause criteria, representing the driving factors of the core problem. We plot the cause attributes into the IGA map following Eq. 14-15 (Section 3.4), as shown in Fig. 5. Most of the attributes fall into the "keep as it is" quadrant, while criterion C32 is considered a "neutral" attribute, and criteria C51 and C63 "critical" to improve. For example, the criterion C63 being a critical attribute, while most of the attributes being influenced fall into the "keep as it is". Then, the improvements towards this attribute should begin immediately along with the performance of the other attributes.

TABLE. VIII. THE DISTANCE MEASURES TO THE BEST IDEAL SOLUTION (**S+**), WORST SOLUTION (**S-**), CLOSENESS, AND THE FINAL RANKING OF ALTERNATIVES

	S+	S-	Closeness	Ranking
A1	0.1071	0.1091	0.5047	5
A2	0.1099	0.112	0.5047	4
A3	0.0445	0.151	0.7724	1
A4	0.1102	0.1129	0.5061	3
A5	0.1047	0.1112	0.5149	2

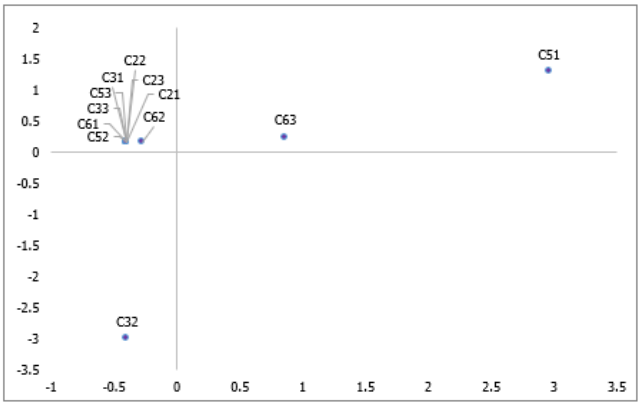

Fig. 5. The IGA Map based on the cause Attributes from DEMATEL for Best-Selected Alternative (A3).

V. CONCLUSION

In this paper, we proposed a holistic risk-driven security evaluation approach for cloud services selection. We addressed three main issues, namely, (1) lack of a systematic and quantitative approach for the selection of the minimal and representative criteria for cloud services security evaluation considering the dependency relations between cloud service models, the potential threats and vulnerabilities, and the effectiveness of the security controls; (2) lack of comprehensive criteria weighting approach considering the dependencies between control criteria and cloud stockholder's varying degree of control for implementing and managing the security services; and (3) lack of effectiveness-based evaluation for cloud services. The proposed method first builds the evaluation context and selects the core security controls (i.e., evaluation criteria) considering several factors, namely threat likelihood, vulnerability relevance, and controls effectiveness given the cloud service models using fuzzy DEMATEL method. Next, the weights of criteria were calculated based on the dependencies between the security controls, cloud user's level of control given the cloud service model and security control type, as well as user preferences using a combination of fuzzy DEMATEL and fuzzy ANP methods. Furthermore, subjective weights were combined with objective weights to obtain more reliable results. Finally, the TOPSIS method was employed for services ranking and the improvement gap analysis (IGA) method was leveraged to provide more insights on the strength and weaknesses of the selected services. The proposed method facilitates a systematic

selection and prioritization of security controls for evaluation following a risk-driven approach, which drives for more efficient and effective services evaluation.

REFERENCES

[1] L. Badger, R. Patt-corner, and J. Voas, "NIST cloud computing synopsis and recommendations," Nist Spec. Publ., vol. 800, no. 146, p. 81, 2012.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.

[3] T. Halabi and M. Bellaiche, "A broker-based framework for standardization and management of Cloud Security-SLAs," Comput. Secur., vol. 75, pp. 59–71, 2018.

[4] H. Mohammad, A. Ahmad, and K. Bin, "A novel evaluation framework for improving trust level of Infrastructure as a Service," Cluster Comput., vol. 19, no. 1, pp. 389–410, 2016.

[5] J. Sidhu and S. Singh, "Improved TOPSIS method based trust evaluation framework for determining trustworthiness of cloud service providers," J. Grid Comput., vol. 15, no. 1, pp. 81–105, 2017.

[6] R. Krishankumar and K. S. Ravichandran, "Solving cloud vendor selection problem using intuitionistic fuzzy decision framework," Neural Comput. Appl., vol. 1, 2020.

[7] Z. Ma, R. Jiang, M. Yang, T. Li, and Q. Zhang, "Research on the measurement and evaluation of trusted cloud service," Soft Comput., vol. 22, no. 4, pp. 1247–1262, 2018.

[8] T. Halabi and M. Bellaiche, "Towards quantification and evaluation of security of Cloud Service Providers," J. Inf. Secur. Appl., vol. 33, pp. 55–65, 2017.

[9] The Cloud Service Measurement Initiative Consortium (CSMIC), "Service measurement index introducing the service measurement index (SMI)," pp. 1–8, 2011.

[10] R. Ranjan, K. Siba, and M. Chiranjeev, "A novel framework for cloud service evaluation and selection using hybrid MCDM methods," Arab. J. Sci. Eng., 2017.

[11] S. K. Garg, S. Versteeg, R. Buyya, "A framework for ranking of cloud computing services," Futur. Gener. Comput. Syst., vol. 29, no. 4, pp. 1012–1023, 2013.

[12] CSA. "Cloud Controls Matrix.". https://cloudsecurityalliance.org/group/cloud-controls-matrix.

[13] J. Luna, A. Taha, R. Trapero, and N. Suri, "Quantitative reasoning about cloud security using service level agreements," IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 457–471, 2017.

[14] J. Modic, R. Trapero, A. Taha, J. Luna, M. Stopar, and N. Suri, "Novel efficient techniques for real-time cloud security assessment," Comput. Secur., vol. 62, pp. 1–18, 2016.

[15] T.L. Saaty, "The analytic hierarchy process," McGraw-Hill, New York, (1980).

[16] T.L. Saaty, "The analytic network process," Pittsburgh: RWS, (1996).

[17] NIST, "NIST Cloud Computing security reference architecture," NIST Tech Beat, pp. 1–2, 2011.

[18] R. M. Savola and H. Pentikäinen, "Towards security effectiveness measurement utilizing risk-based security assurance," 2010 Inf. Secur. South Africa, pp. 1–8, 2010.

[19] G. Tontini and J. D. Picolo, "Improvement gap analysis," Manag. Serv. Qual., vol. 20, no. 6, pp. 565–584, 2010.

[20] S. Maroc and J. B. Zhang, "Risk-based and dependency-aware criteria specification for cloud services security evaluation," IEEE Inter. Conf. Comm. Soft and Netw. (ICCSN), 2019, pp. 731–735.

[21] E. Fontela, and A. Gabus, "DEMATEL innovative methods tech. report no. 2, structural analysis of the world problematique," NY: Battelle Geneva Resear. Inst., (1974).

[22] C. A. B. de Carvalho, R. M. de C. Andrade, M. F. de Castro, E. F. Coutinho, and N. Agoulmine, "State of the art and challenges of security SLA for cloud computing," Comput. Electr. Eng., vol. 59, pp. 141–152, 2017.

[23] H. Alabool, A. Kamil, N. Arshad, and D. Alarabiat, "Cloud service evaluation method-based Multi-Criteria Decision-Making: A systematic literature review," J. Syst. Softw., vol. 139, pp. 161–188, 2018.

[24] H. Mouratidis, S. Islam, C. Kalloniatis, and S. Gritzalis, "A framework to support selection of cloud providers based on security and privacy requirements," J. Syst. Softw., vol. 86, no. 9, pp. 2276–2293, 2013.

[25] H. M. Alabool et al., "A novel evaluation model for improving trust level of infrastructure as a service," 2015 Int. Symp. Math. Sci. Comput. Res. iSMSC 2015 - Proc., vol. 19, no. 1, pp. 162–167, 2016.

[26] N. Al-safwani, Y. Fazea, and H. Ibrahim, "ISCP : In-depth model for selecting critical," Comput. Secur., vol. 77, pp. 565–577, 2018.

[27] L. Sun, H. Dong, O. K. Hussain, F. K. Hussain, and A. X. Liu, "A framework of cloud service selection with criteria interactions," Futur. Gener. Comput. Syst., vol. 94, pp. 749–764, 2019.

[28] A. Taha, P. Metzler, R. Trapero, J. Luna, and N. Suri, "Identifying and utilizing dependencies across cloud security services," ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur., pp. 329–340, 2016.

[29] C. Choi and H. Jeong, "Quality evaluation and best service choice for cloud," pp. 245–270, 2014.

[30] T. Subramanian and N. Savarimuthu, "Cloud service evaluation and selection using fuzzy hybrid mcdm approach in marketplace," vol. 5, no. 2, 2016.

[31] C. H. Su, G. H. Tzeng, and H. L. Tseng, "Improving cloud computing service in fuzzy environment - Combining fuzzy DANP and fuzzy VIKOR with a new hybrid FMCDM model," 2012 Int. Conf. Fuzzy Theory Its Appl. iFUZZY 2012, pp. 30–35, 2012.

[32] V. Ghafori and R. Manouchehri Sarhadi, "Best cloud provider selection using integrated ANP-DEMATEL and prioritizing SMI attributes," Int. J. Comput. Appl., vol. 71, no. 16, pp. 18–25, 2013.

[33] B. Alexandru, D. Mihaela, and D. Mihail, "A decision making framework for weighting and ranking criteria for Cloud provider selection," 2016.

[34] Y. O. Yang, H. Shieh, and G. Tzeng, "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment," Inf. Sci. (Ny)., vol. 232, pp. 482–500, 2013.

[35] C. C. Lo and W. J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," Expert Syst. Appl., vol. 39, no. 1, pp. 247–257, 2012.

[36] L.A. Zadeh, "Fuzzy set theory," Inf. and Contr. vol. 8, pp. 338–353, 1965.

[37] L. E. Quezada, H. A. López-ospina, P. I. Palominos, and A. M. Oddershede, "Identifying causal relationships in strategy maps using ANP and DEMATEL," Comput. Ind. Eng., vol. 118, no. January 2017, pp. 170–179, 2018.

[38] X.H. Xu, L.Y. Zhang, Q.F Wan, "A variation coefficient similarity measure and its application in emergency group decision-making," Syst. Eng. Proc. 5 119–124 (2012).

[39] K. Yoon, and C. L Hwang, "TOPSIS (Technique for order preference by similarity to ideal solution)-A multiple attribute decision making," (1980).

[40] J. A. Martilla and J. C. James, "Importance-Performance Analysis," J. Mark., vol. 41, no. 1, pp. 77–79, 1977.