Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# A DELPHI-BASED SECURITY RISK ASSESSMENT MODEL FOR CLOUD COMPUTING IN ENTERPRISES

[1,2] AHMED YOUSSEF

[1] College of Computer and Information Sciences, King Saud University, Riyadh, KSA

[2] Faculty of Engineering at Helwan, Helwan University, Cairo, Egypt

E-mail: ahyoussef@ksu.edu.sa

## ABSTRACT

Cloud computing (CC) reveals a remarkable potential to provide on-demand services to a wide variety of enterprises over the Internet with greater flexibility in a cost-effective manner. However, it presents an added level of security and privacy risks because essential services are often outsourced to a third party. Security risks are the most critical issue that hinders enterprises from adopting CC since they may result in loss of satisfaction for many business objectives. On the other hand, Cloud Service Providers (CSP) are struggling with the cloud platform security issues since the cloud model has a very complex architecture with many characteristics and different stakeholders' security requirements. Hence, there is an essential need for an in-depth assessment of cloud related security risks. Traditional risk assessment methods do not fit CC well due to its complex environment and the assumption by those methods that assets are owned and fully controlled by the enterprise itself. In this paper, we propose a Delphi-based Cloud Security Risk Assessment Model (DCSRAM) that identifies, analyzes, and evaluates security risks affecting CC adoption in enterprises. The proposed model supports a higher level of trust in cloud technologies from the side of enterprises and a cost-effective and reliable productivity from the side of CSP. The model has been tested for applicability and usability through a use case scenario.

**Keywords:** *Cloud Computing; Risk Assessment; Information Security; Data Privacy; Delphi Technique.*

## 1. INTRODUCTION

Cloud Computing (CC) represents a new paradigm shift in Internet services. It delivers highly scalable platforms in which computational resources are offered by Cloud Service Providers (CSP) to Cloud Services Consumers (CSC) in the form of on-demand, cost effective services. In the past few years, cloud technologies have experienced an exponential advancement and growth. Gartner projects cloud service industry to grow exponentially through 2022 (Table 1). According to Gartner's latest forecast published in April 2019, the worldwide public cloud services market is projected to grow 17.5 percent in 2019 to total $214.3 billion, up from $182.4 billion in 2018. The fastest-growing market segment will be infrastructure as a service (IaaS), which is forecast to grow 27.5 percent in 2019 to reach $38.9 billion, up from $30.5 billion in 2018 [37].

In spite of the rapid advancement and growth in cloud service market and the increasing number of cloud users, CC introduces new security risks that need to be assessed and mitigated [12,13]. These security risks are considered one of the top ranked issues regarding CC adoption in enterprises, as reported by IDC [34] (Figure 1). A reasonable justification of such increasing concerns about security in CC includes: 1) loss of control over cloud hosted assets; 2) lack of security guarantees in the Service Level Agreements (SLA) between CSP and CSC; and 3) sharing of resources with competitors or malicious users [3]. Accordingly, no matter how strongly CC is secured, CSC continue suffering from loss of control and lack of trust problems. On the other hand, CSP are struggling with the cloud platform security issues because Cloud has a very complex architecture with many characteristics and different stakeholders' security needs that must be considered when developing a holistic security model. In addition, CSP are not always aware of the security requirements that must be enforced on the services they host which leads to loss of security control over these services [3].

Journal of Theoretical and Applied Information Technology
15th January 2020. Vol.98. No 01

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Table 1: Worldwide Public Cloud Service Revenue Forecast (Billions of U.S. Dollars)*

| Services | 2018 | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| BPaaS | 45.8 | 49.3 | 53.1 | 57.0 | 61.1 |
| PaaS | 15.6 | 19.0 | 23.0 | 27.5 | 31.8 |
| SaaS | 80.0 | 94.8 | 110.5 | 126.7 | 143.7 |
| Security | 10.5 | 12.2 | 14.1 | 16.0 | 17.9 |
| IaaS | 30.5 | 38.9 | 49.1 | 61.9 | 76.6 |
| **Total Market** | **182.4** | **214.3** | **249.8** | **289.1** | **331.2** |

BPaaS = Business Process as a Service; IaaS = Infrastructure as a Service; PaaS = Platform as a Service; SaaS = Software as a Service

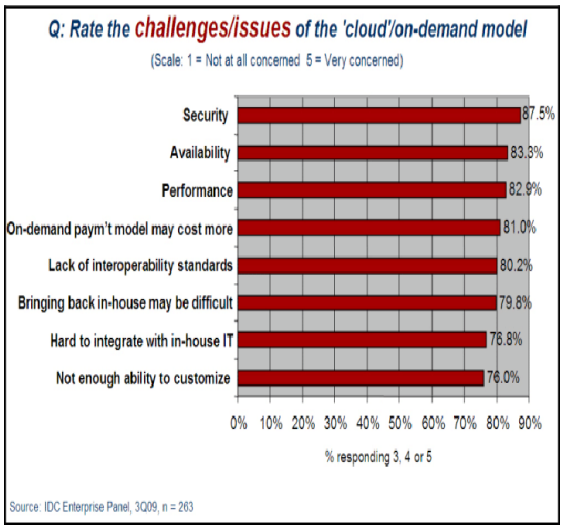


*Figure 1: Top ranked issues in CC*

The importance of security risk assessment for enterprises stems from the serious security issues associated with cloud technologies. The lack of adequate confidence in a cloud service in terms of the uncertainties associated with its level of quality may prevent several enterprises from adopting cloud technologies. In addition, security risks associated with CC may result in loss of satisfaction for many organizational objectives of the enterprise. Consequently, assessment of security risks in CC is essential [1,5,6,7,9]. Traditional risk assessment methods do not fit CC well due to its complex environment and the assumption by those methods that assets are owned and fully controlled by the enterprise itself.

This work proposes DCSRAM, a Delphi-based Security Risk Assessment Model that identifies, analyzes, and evaluates security risks affecting the adoption of CC in enterprises. The model is validated through a use-case scenario. Although the provision of zero-risk service is not practical, the proposed model may at least provide an adequate level of confidence in cloud technologies from the side of enterprises (i.e., successful fulfillment of SLA) and a cost-effective (e.g., making a certain amount of profit) and reliable productivity (e.g., efficient utilization of resources) from the side of CSP.

The rest of this paper is organized as follows: section 2 provides background information on CC paradigm, risk assessment and the Delphi method. In section 3, we review the previous work related to risk assessment models. In section 4, we describe the proposed CC **s**ecurity risk assessment model (DCSRAM) and present its fundamental concepts and theory. In section 5, we validate DCSRAM through a use-case scenario, and in section 6, we give our conclusions and a plan for future work.

## 2. BACKGROUND

### 2.1 Cloud Computing Paradigm

Nowadays, CC has become a popular topic for discussion in workshops, forums and social media [11]. Both individuals and enterprises show a significant interest in CC as it is essential to improve their businesses and operations. In addition, the emergence of technology trends, such as mobility, Big Data analytics, and social media is driving enterprises to optimize and innovate their business models through investment in CC. The National Institute of Standards and Technology (NIST) [33,35] defined cloud computing as *"A model for enabling ubiquitous, convenient, 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 service provider interaction"*. NIST categorized services offered by CC into three types: *Software as a Service (SaaS); Platform as a Service (PaaS); and Infrastructure as a Service (IaaS),* these are shown in figure 2.

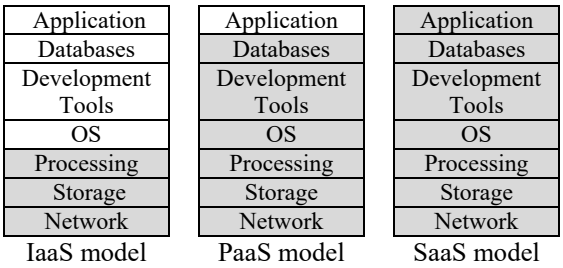


*Figure 2: NIST Cloud Service Models*

models; *public cloud*, *private cloud*, *community cloud* and *hybrid cloud*. In public cloud, the infrastructure and other cloud services are made available to the general public over the Internet. It

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

exists on the premises of the CSP. In private cloud, the infrastructure is deployed solely by a single enterprise, and it may exist on or off premises. In community cloud, infrastructure is deployed by several enterprises that have the same interest and security requirements, and it may exist on or off premises. Finally, in hybrid cloud, the cloud infrastructure consists of a combination of two or more public, private or community cloud components. NIST has also described five CC essential characteristics which are: on demand self-service; broad network access; resource pooling; rapid elasticity, and measured service.

### 2.2 Risk Assessment

Risk is unavoidable and present in every human situation, daily life, and public and private sector enterprises. There are many accepted definitions of risk in use depending on the context (i.e., security, insurance, stakeholders, etc.). The common concept in all definitions is uncertainty of outcomes, where they differ in how they characterize outcomes. Risk is often thought of as having only adverse or negative outcomes (consequences). However, risk is also associated with positive outcomes (opportunities) [10]. Risk itself is not bad, it is essential to progress, and failure is often a key part of learning. The issue is that we must learn how to balance the possible consequences of the risk against its potential opportunities [4].

Risk management [15] refers to a coordination set of processes including risk identification, risk analysis, risk evaluation, and risk treatment that is used to direct an enterprise and to control the many risks that can affect its ability to achieve its business objectives [4]. Risk assessment, which is a part of risk management, includes three phases: 1) identifying risks to a system, 2) analyzing the identified risks by estimating their probability of occurrence and the impact of its consequences, and 3) evaluating risk level. Risk assessment implies that as minimum, some form of quantitative or qualitative analysis is required for making decision concerning major risks to the achievement of organizational objectives [10]. In quantitative risk analysis, a numerical estimate is made of the probability that a defined harm will result from the occurrence of a particular risk event. This kind of analysis is performed on risk that have been prioritized. The impacts of these risks are analyzed and a numerical rating to those impacts are assigned. On the other hand, qualitative risk analysis is used in the cases where it is difficult to express numerical measure of risks. It is, for example, the occurrence without adequate numerical data. Such analysis can be used as an initial assessment to recognize risks. In many cases, risk analysis can be made partially quantitative and partially qualitative [2,4].

### 2.3 The Delphi Method

Delphi is a widely accepted consensus-based estimation method for identifying and prioritizing issues regarding decision-making [16,17]. It is a forecasting technique used to collect expert opinion in an objective way, and arrive to a consensus conclusion based on that. Delphi was originally developed by RAND Corporation in 1950-1960s for the military purpose [18]. It has since been applied to other domains such as technology, population sciences, and environmental risk assessment and has been proven to be a very effective estimation tool [19].

Three essential characteristics of Delphi method are: 1) structured and iterative information flow, 2) anonymity of the participants in order to alleviate peer pressure and other performance anxieties, and 3) iterative feedback of the participants. In this method, a moderator is used to control and facilitate information gathering from a selected group of Subject Matter Experts (SME) who are knowledgeable on the enterprise's particular type of business. During the Delphi process, each participant of the SME is asked to provide an answer to a question regarding decision-making issue. A form is designed such that the participant can easily provide a numerical answer to the questions. Following this step, the moderator merges the answers from all participants in anonymous presentation, shares and discusses the combined results with all participants. The participants are then encouraged to iteratively reconsider and modify their answers based on the feedback from previous discussion.

## 3. RELATED WORK

In literature, there are several models and frameworks with different approaches that help in information security risk assessment [3,5-9,14,20-32], however, these traditional risk management frameworks do not fit CC well due to its complex environment and the assumption by those frameworks that the assets are owned and fully managed by the enterprise itself. This section reviews the existing information security risk assessment models:

CORAS: is a UML model security risk analysis method developed for InfoSec. It defines a UML language for security concepts such as threat, asset, vulnerability, and scenario, which is applied to model unwanted incidents and risks [30]. In

CORAS, a security risk analysis is conducted in seven steps which are: introduction, high level analysis, approval, risk identification, risk estimation, risk evaluation, and risk treatment. The major weaknesses of CORAS are: 1) it is a generalized methodology; hence, there is still a need to develop or extend the methodology for particularly requirements phase, 2) quantitative risk assessment cannot be provided by CORAS, and 3) it is not clear how the severity of threats and vulnerabilities are mapped [23].

CRAMM: a risk analysis and management method that includes a comprehensive range of risk assessment tools that are fully complaint with ISO27001 and address tasks such as: asset dependency modeling, identifying and assessing threats and vulnerabilities, assessing risk levels, and identifying required controls [22,32]. It provides a staged and disciplined approach embracing both technical (e.g. hardware and software) and non-technical (e.g. physical and human) aspects of security. The major flaws in CRAMM are: 1) quantitative risk assessment cannot be provided. Hence, there is need to extend this methodology in this direction and 2) it does not clearly talk about the security attributes e.g. Confidentiality, Integrity, and Availability [23].

COBRA: a risk assessment model that consists of a range of risk analysis, consultative and security review tools which were developed largely in recognition of changing nature of IT and security, and the demands placed by business upon these areas [31].The default risk assessment process usually consists of three stages: questionnaire building, risk surveying, and report generation. The major weaknesses of COBRA are 1) risk assessment technique is not clearly mentioned; hence, there is need to extend this methodology in this direction and 2) threats and vulnerabilities play a very important role in the process of risk assessment; but how these are taken into consideration, is not clearly given in COBRA [23].

OCTAVE: a standard security framework for measuring risk level and planning defenses against cyber assaults [20,21,23]. The framework describes a methodology to depreciate exposure to possible threats, determine the permissible consequences of attacks and deal with attacks that succeed. One of the significant draw backs of OCTAVE is its complexity and it does not allow quantitative risk analysis.

NIST RMF: a general risk management framework that can be applied to any asset [20,23]. It covers a series of activities related to managing risk, however, it is not available with computer support, where templates could be used electronically, and reports could be created automatically for the vast number of data collected during the information risk assessment. It is used more as a guideline instead of methodology.

FAIR: a risk assessment framework for understanding, measuring and analyzing information risk for enabling well-informed decision making. It is established to approach the weaknesses of security concern. It assists in normalizing risks, applying risk assessment and viewing overall risks. However, the main deficiency of FAIR is the lack of information about methodology and examples of how it is applied [20].

Many Enterprise Risk Management (ERM) tools are available for use by enterprises [38]. RSA Archer Suite, a leader in the 2019 Gartner Magic Quadrant for integrated risk management, empowers enterprises of all sizes to manage multiple dimensions of risk on one configurable, integrated software platform. With RSA Archer, enterprises can quickly implement risk management processes based on industry standards and best practices leading to improved risk management maturity, more informed decision-making and enhanced business performance [39].

RiskSync, a leading company with more than 15 years of experience contributing to risk management within all types of enterprises, provides proven risk management solutions. Each solution identifies and analyses risks, discovers trends and facilitates continuous quality improvement. Together the applications form a complete risk management system tailored to the needs of the enterprise: secure, user-friendly, modular and integrated with existing systems. The information security solution is hosted on the RiskSync platform and includes all the built-in functionalities [40].

## 4. THE PROPOSED MODEL

### 4.1 An Overview of DCSRAM

We define the following terms in the context of CC security risk assessment in enterprises:

a. Risk: is an uncertain factor whose occurrence may result in loss of satisfaction of an enterprise's organizational objective.
b. Asset: is something to which enterprise assigns value and hence for which it requires protection such as VM, SLA and computational resources.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

c. Vulnerability: is a weakness, flaw or deficiency in CC that may be exploited to harm or reduce the value of an asset(s).
d. Threat: is a potential undesired event that exploit CC vulnerability to harm or reduce the value of an asset(s).
e. Consequence: is a potential loss of satisfaction of enterprise's objective(s) caused by a risk.

For each risk, $r_i$, where $i \in \{1,2,3, \dots\}$, we define the following elements which help express the risk in a structured format.

1. Threat ($t_i$): a security threat corresponds to $r_i$, each risk $r_i$ maps to a single threat $t_i$ and vise-versa ($r_i \leftrightarrow t_i$)
2. Vulnerabilities ($V_i$): a set of vulnerabilities that may be exploited by $t_i$.
3. Assets ($A_i$): a set of assets that may be harmed by $t_i$
4. Threat Likelihood $L(t_i)$: probability of occurrence of $t_i$
5. Consequences ($C_i$): a set of consequences caused by $t_i$ where
   $C_i = \{c_j: c_j \ a \ consequence \ of \ t_i\}$
   where: $j \in \{1,2,3, \dots\}$
6. Consequence Likelihood $L(c_j|t_i)$: probability of occurrence of $c_j$ when $t_i$ occurs.
7. Consequence Impact $I(c_j)$: the degree by which $c_j$ influences enterprise's objectives.
8. Risk Level $E(r_i)$: the severity of the risk, $r_i$, derived from $L(t_i)$, $L(c_j|t_i)$, and $I(c_j)$.

Figure 3 illustrates these elements and table 2 shows an example of risk profile in a structured format.

Risk assessment involves three phases: *risk identification, risk analysis,* and *risk evaluation*. In DCSRAM, risk identification phase comprises five processes; asset identification, vulnerability identification, threat identification, consequence identification, and risk mapping. On the other hand, risk analysis phase includes the estimate of threat likelihood $L(t_i)$, consequence likelihood $L(c_j|t_i)$, and consequence impact $I(c_j)$. Finally, in risk evaluation phase, risk level $E(r_i)$ is computed as a function in $L(t_i)$, $L(c_j|t_i)$, and $I(c_j)$. Figure 4 shows all phases of the proposed model DCSRAM.

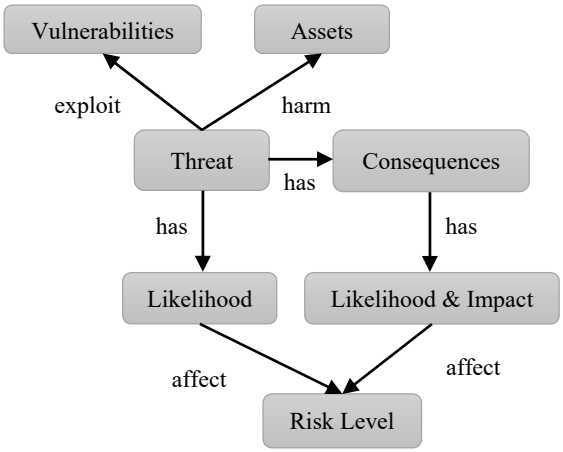


*Figure 3: Elements of risk and the relationships between them*

*Table 2: An example of risk profile in a structured format*

| Risk element | Description |
|---|---|
| threat | unauthorized access to sever |
| vulnerability | virus protection not updated |
| asset affected | servers |
| consequence | data confidentiality affected |
| threat likelihood | moderate |
| consequence likelihood | high |
| consequence impact | moderate |
| risk level | moderate |

### 4.2 Risk Identification Phase

The identification of security risks that are likely to affect cloud services, and consequently the achievement of the goals of enterprises that adopt CC technology, is the most critical step in risk assessment. The better identifying and understanding the risks, the more meaningful and effective will be the risk assessment process. The appropriate risk identification method will depend on the application area (i.e., nature of activities and the hazard groups), the nature of projects in the enterprise, resources available, regularity requirements and client requirements as to objectives, desired outcome and the required level of detail [10].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

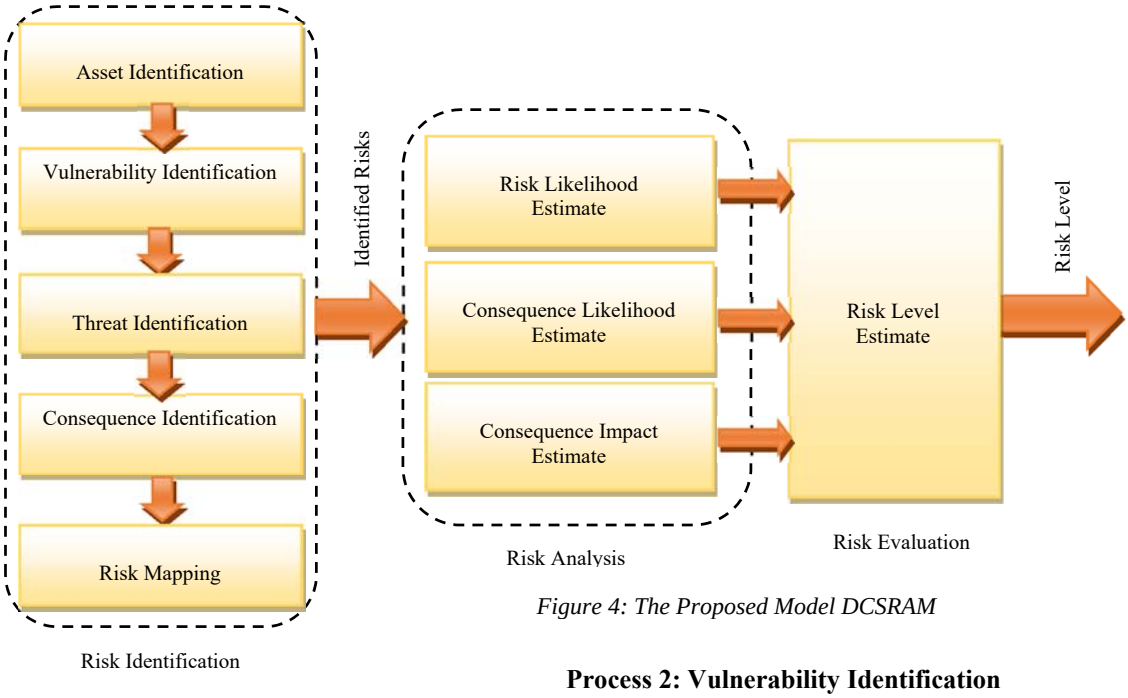


*Figure 4: The Proposed Model DCSRAM*

In DCSRAM, each process in risk identification is performed in a *"group session"* by a team that comprises a number of experts who are knowledgeable about CC security threats particular to the enterprise and a diverse group of stakeholders in the enterprise (e.g., manager, system analyst, sponsor, etc.). In the group session, the team identifies a set of assets (set A) of the enterprise and a set of vulnerabilities, (set V), in CC platform. Then, it recognizes a set of potential threats to CC (set T) that may exploit vulnerabilities in V to harm assets in A. Next, the team defines C, which is a set that gathers consequences of each threat in T. Finally, it maps each identified threat ($t_i$) to a subset of assets ($A_i$), vulnerability ($V_i$), and consequences ($C_i$). It is worthy to mention that the European Network and Information Security Agency (ENISA) [36] has provided generic lists of assets, vulnerabilities and threats for CC. However, these lists do not reflect the enterprise's organizational objectives nor they reveal a specific class of business applications.

**Process 1: Asset Identification**

In this step, the team identifies a set of assets (A) of the enterprise that may be affected by cloud security breaches. Examples of these assets are:

- Sensitive data
- Physical nodes and VM
- Intellectual property

**Process 2: Vulnerability Identification**

The goal of vulnerability identification step is to develop a set of cloud vulnerabilities (V) or security breaches in the cloud services. Examples of these vulnerabilities are:

- Authentication Authorization Accounting (AAA) vulnerabilities
- User provision vulnerabilities
- Lack of reputational isolation
- Inaccurate modelling of resources

**Process 3: Threat identification**

In threat identification, the team identifies a set of the potential threats (T) that may exploit vulnerabilities in set V to harm assets in set A. Examples of such threats are given below:

- Resource Exhaustion: over or under provision of cloud resources which leads to inadequate service or denial.
- Isolation Failure: failure in effectively separating storage, memory, and routing causes isolation failure.
- Malicious Insider: a CSP's employee maliciously alters or corrupts customer data.

ENISA provides 23 classes of assets that CSC assign value when adopting CC, lists 53 vulnerabilities, 31 are cloud specific and 22 are not cloud specific, and identifies 35 threats that fall in one of the following

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

four categories: policy and organization, technical, legal, and other threats not specific to CC.

**Process 4: Consequence Identification**

In this step, the team uses all information acquired in the previous three steps (A, V, and T) to identify the consequences of each threat in T. These consequences are gathered in set C. Examples of these consequences are:

- Loss of confidentiality which means the unauthorized disclosure of information
- Loss of integrity which means the unauthorized modification or destruction of information
- Loss of availability which means the disruption of access to information
- Loss of customers

**Process 5: Risk Mapping**

Now using the information acquired above, the team will define a set of risks (R), each risk ($r_i \in R$) corresponds to a threat ($t_i \in T$), which maps to a subset of assets ($A_i \subseteq A$), a subset of vulnerabilities ($V_i \subseteq V$), and a subset of consequences ($C_i \subseteq C$), this mapping is shown in figure 5. For example, a risk $r_i$, corresponds to a threat $t_i$="*account hijacking*" maps to a subset of assets $A_i$={storage resources, computational resources, customer's trust}, a subset of vulnerabilities $V_i$={insufficient input-data validation, weak credential, insufficient authorization check} and a subset of consequences $C_i$={loss of confidentiality, loss of availability, loss of customers}.

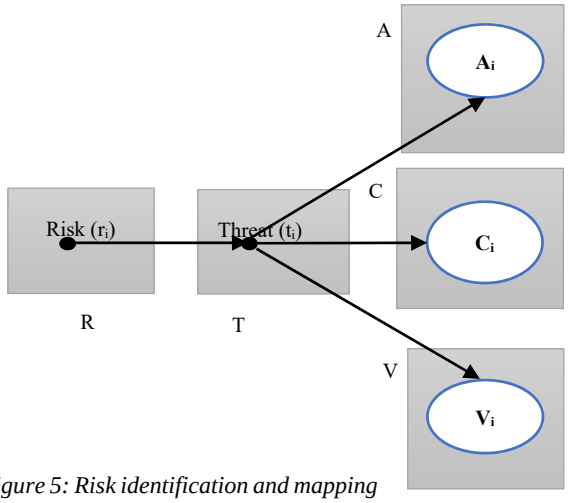


*Figure 5: Risk identification and mapping*

### 4.3 Risk Analysis Phase (Delphi Session)

Risk analysis usually encompasses the estimate of risk likelihood and consequence impact. Often qualitative and semi-quantitative techniques are employed using tools such as risk matrix which is a 2-dimentional matrix (risk likelihood and consequence impact). Qualitative analysis requires defining evaluation level for likelihood and impact. For example, an expert can define three levels for risk likelihood (unlikely, possible, likely) and three levels for consequence impact (minor, moderate, major). The final risk level assessment is based on expert opinion that takes the two factors into consideration and it may assume four levels (low, medium, high, very high). For example, risk due to vendor lock-in is assessed to be high, because its likelihood is likely, and its consequence impact is moderate [8]. Semi-quantitative approach, on the other hand, uses value ranges for the evaluation of both risk likelihood and consequence impact, but does not consider their combined influence in a quantitative manner. For instance, the previous example of qualitative approach may be modified to follow a semi-quantitative manner by defining scales for risk likelihood and consequence impact as shown in table 3. However, the final risk level assignment is still based on expert opinion as shown in table 4. Both approaches do not consider consequence likelihood.

*Table 3: Risk likelihood and consequence impact scale in semi-quantitative approach*

| risk likelihood scale | | consequence impact scale | |
|---|---|---|---|
| unlikely | 0-0.25 | minor | 0-3 |
| possible | -0.75 | moderate | 4-7 |
| likely | -1.0 | major | 8-10 |

*Table 4: Risk Matrix*

| Prob/Impact | minor (0-3) | moderate (4-7) | major (8-10) |
|---|---|---|---|
| unlikely (0-0.25) | Low | Medium | high |
| possible (-0.75) | medium | High | very high |
| likely(-1.0) | High | High | very high |

Estimate of probabilities of several security risks is a tedious task, due to the lack of historic data. For example, in case of risks due to spoofing attacks, critical data need is the frequency of occurrence of such attacks on all enterprise systems. While such data are not readily available, collaborative research among institutions collecting and analyzing security data will be very helpful in likelihood and impact estimation [8]. In DCSRAM, we adopted a fully quantitative risk analysis approach that further considers consequence likelihood and improves the previous approaches by enabling stakeholders comparatively evaluate risks using Delphi

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

technique. Delphi technique is used in DCSRAM for the estimate of threat likelihood $L(t_i)$, consequence likelihood $L(c_j|t_i)$, and consequence impact $I(c_j)$. This technique is shown in figure 6 and is described below:

1. **Select moderator and SME:** The technique begin by selecting a team consists of a moderator and a group of SME with 3 to 7 members. Picking qualified team is an important part of generating accurate estimates. Moderator should be familiar with the Delphi process, SME must be willing to estimate each task honestly, and should be comfortable working with each other. They should be knowledgeable about enterprise's goals and CC risks to make educated estimates about their likelihoods and consequences.
2. **Prepare for a kickoff meeting:** The first meeting during which estimation team creates a work breakdown structure and discusses assumptions. Moderator leads the meeting and give vision, scope and a goal statement for estimation session to SME before the meeting. The goal statement should be no more than a few sentences that describe the scope of the work that is to be estimated. For example, "Generate estimates for likelihoods and consequences of risks associated with the utilization of CC in the enterprise".
3. **Individual Estimate:** After the meeting, each expert in SME creates an effort estimate for each risk, $r_i$. SME individually provide their best numerical estimates for $L(t_i)$, $L(c_j|t_i)$ and $I(c_j)$ in a well prepared estimate form. The likelihood ranges between 0.0 and 1.0 and the impact is estimated on a scale from 0 to 10.
4. **Assemble Estimate:** Moderator collects all estimate forms. Estimates are compiled, shared, including summary statistics, and displayed on a whiteboard.
5. **Revise Estimate:** SME revise their individual estimates, moderator try to resolve issues or disagreements, remove redundancies and resolve remaining estimate differences. Any estimate with an especially wide discrepancy should be marked for further discussion.
6. **Check Convergence:** If all estimate values converge within an acceptable range (e.g. 5% variance), the moderator records the final estimates for each risk to use for risk evaluation, otherwise steps 3-5 are repeated.

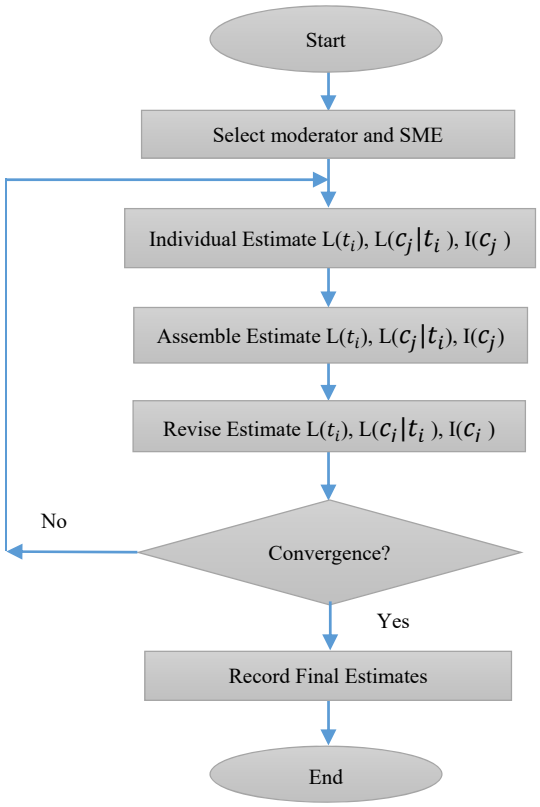


*Figure 6: The Delphi Risk Analysis Process*

### 4.4 Risk Evaluation Phase

After the SME converge on a consensus for the numerical values of $L(t_i)$, $L(c_j|t_i)$ and $I(c_j)$ for each risk $r_i \in R$, the risk level, $E(r_i)$, can be evaluated using these value as per Equation 1. The overall security risk level ($E_t$) for the given cloud application is the cumulative sum of risk levels, $E(r_i)$, for all n risks in R, and is given by Equation 2. The risk factor R.F for the enterprise can be estimated from Equation 3 ($0 \leq R.F \leq 1$). This equation is a normalization for $E_t$ since the maximum value of $E_t$ is 10mn.

$$E(r_i) = L(t_i) \sum_{j=1}^{m} L(c_j|t_i) I(c_j) \quad (1)$$

*m:* number of consequences in C

$$L(c_j|t_i) = 0 \; if \; c_j \notin C_i$$

$$E_t = \sum_{i=1}^{n} E(r_i) \quad (2)$$

*n:* number of risks in R

$$R.F = \frac{E_t}{10\,m\,n} \quad (3)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## 5. MODEL VALIDATION

To demonstrate the usability and the applicability of DCSRAM, we provide a step-by-step use-case scenario that shows how an enterprise adopting CC may use DCSRAM to assess security risks. Advanced Telecom (AT) is a leading telecommunications company that has a broad range of customers, whom it offers integrated communications services, through its state-of-the-art infrastructure. The company has heard about the cutting-edge CC technology and thought that it would probably be a good idea to adopt this technology and leverage its several benefits to improve the performance of its Enterprise Resource Planning (ERP) system. However, AT's top management is still reluctant to adopt CC due to its security risks. Our goal is to help AT company take a decision on the adoption of CC using our proposed CC security risk assessment model. Table 5 shows AT's profile which gives information concerning its business objectives and security requirements. These information are used to guide different processes in risk assessment phases.

*Table 5: Enterprise Profile*

| | |
|---|---|
| Enterprise name | Advanced Telecom. (AT) |
| Selected CC service (application) | ERP |
| Business Objectives | Gain and increase profitability from transaction broker<br>Provide perfect customer service<br>Enhance customer satisfaction |
| Security requirements | Confidentiality – medium<br>Integrity – high<br>Availability – high |

### Phase 1: Risk Identification (Group Session)

In this step, a team of seven members that comprises SME and a diverse group of stakeholders in the enterprise meet to identify potential risks and different elements of these risks using the information available in enterprise's profile. Each group session is structured in a way such that each participant has a clearly defined role (moderator, manager, user, developer, expert, etc.) and contributes to risk elaboration according to his/her role, towards reaching cooperation. The output of this phase are the sets R, T, A, V, and C. The team then provides mapping among these sets as per figure 5. Table 6 illustrates the output of group session phase.

### Phase 2: Risk Analysis (Delphi Session)

In Delphi session, each SME member provides his/her best numerical estimates for $L(t_i)$, $L(c_j|t_i)$, and $I(c_j)$ for each risk $r_i$, and consequence $c_j$ identified in phase 1. The likelihoods range between 0.0 and 1.0 and the impacts are estimated on a scale from 0 to 10. Moderator then collects all estimates, displays results to SME, allows them to revise their estimates and resolves conflicts. This process is repeated until results converge within 5% variance. The experts' final estimates are recorded in table 7 and are used for risk level estimate.

### Phase 3: Risk Evaluation

The final step is to estimate the level, $E(r_i)$, of each identified risk, as per Equation 1. The results are shown in the last column of table 7. The overall security risk level ($E_t$) for the given cloud application (ERP) is computed using Equation 2. The overall risk level for the enterprise has been estimated to be **22.2**, the risk factor (R.F) has been computed from equation 3 and found to be **0.123**. Finally, the SME should take a step back and view the process holistically. Have a conversation with the stakeholders about the R.F estimated and make a decision upon. The best strategy is often to try minimize the R.F by considering various techniques for risk treatment and mitigations.

## 6. CONCLUSION AND FUTURE WORK

The adoption of CC provides enormous operational and economic benefits for enterprises. Unfortunately, these benefits do not offer better security in terms of integrity, confidentiality, and availability. For this reason, developing a risk assessment model for CC is essential to enable CSP and enterprises to quantify risks based on the likelihood of their occurrence and the impact of their consequences. Moreover, developing a risk assessment model for CC in a complicated environment requires careful consideration of CC characteristics and main features of its security risks. In this paper, we proposed DCSRAM, a Delphi-based risk assessment model that identifies, analyzes and evaluates CC security risks that result in loss of satisfaction of business objectives in enterprises adopting CC technologies. This model leads to a higher level of trust in cloud technologies from the side of enterprises and a cost-effective and reliable productivity from the side of service providers. For the future work, there is a need to develop a comprehensive risk management framework that should be simple and clearly defines all risk management processes including risk treatment and countermeasure, monitoring and review, and risk acceptance by enterprises.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## REFERENCES


[1] Karim Djemame, Django Armstrong, Mariam Kiran, and Ming Jiang, "A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems", 2ndInternational Conference on Cloud Computing, GRIDs, and Virtualization, 2011.

[2] Karim Djemame, Django Armstrong ,Jordi Guitart, and Mario Macias, "A Risk Assessment Framework for Cloud Computing", IEEE Transactions on Cloud Computing, Vol. 4 , Issue. 3 , 2016.

[3] Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", IEEE 4th International Conference on Cloud Computing, Washington, DC, USA, 2011.

[4] Drissi S.,Houmani H. and Medromi H, "Survey: Risk Assessment for Cloud Computing", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 4, No. 12, 2013.

[5] Xuan Zhang , NattapongWuwong , Hao Li and Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", 10th IEEE International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July 2010.

[6] Rana Alosaimi and Mohamed Alnum,"A Proposed Risk Management Framework for Cloud Computing Environment", Inernational Journal of Computer Science and Information Security, Vol. 14, No.8, 2016.

[7] Rana Alosaimi and Mohamed Alnum, "Risk Management Framework for Cloud Computing: A Critical Review", International Journal of Computer Science and Information Technology, Vol.8, No. 4, 2016.

[8] Prasad Saripalli and Ben Walters, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security", IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, 5-10 July 2010.

[9] Erdal Cayirci, Alexandr Garaga, Anderson Santana de Oliveira and Yves Roudier, "A Risk Assessment Model for Selecting Cloud Service Providers", Journal of Cloud Computing: Advances, Systems and Applications, 5:14, 2016.

[10] Heinz-Peter Berg, "Risk Management: Procedures, Methodsand Experiences", RT&A, Vol. 1, No. 2(17), 2010.

[11] BlessonVarghese and RajkumarBuyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Vol. 79, Part 3,pp. 849-861, February 2018,

[12] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, 4:5, 2013.

[13] SaurabhSingh,Young-SikJeong, and Jong HyukPark, "A Survey on Cloud Computing Security: Issues, Threats, and Solutions", Journal of Network and Computer Applications, Vol. 75, pp. 200-222, 2016.

[14] J. Oriol Fitó ; Mario Macías ; Jordi Guitart, "Toward business-driven risk management for Cloud computing", International Conference on Network and Service Management, Niagara Falls, ON, Canada, 25-29 Oct. 2010.

[15] IRMcorporation, [online] Available: https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf, 2002.

[16] H.A. Linstone, The Delphi Method: Techniques and Applications, Addison-Wesley, 1975.

[17] L.M. Stuter, "The Delphi Technique: What is it?", Lynn's Educational and Research Network, March 1996.

[18] RAND Corporation, "A collection of RAND publications on the Delphi method", 2007.

[19] E. Teijlingen, E. Pitchfork, C. Bishop, E. Russell, "Delphi method and nominal group techniques in family planning and reproductive health research", Journal of Family Planning and Reproductive Health Care, Vol. 31, No. 2, pp. 132-135, 2005.

[20] Umesh Kumar Singh and Chanchala Joshi, "Comparative Study of Information Security Risk Assessment Frameworks", International Journal of Computer Application, Vol. 2, Issue 8, 2018.

[21] Filipe Macedo and Miguel Mira da Silva, "Comparative Study of Information Security Risk Assessment Models.

[22] Ahmad Amini and Norziana Jamil, "A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing", Journal of Physics: Conference Series, Volume 1018, 2018.

[23] S. K. Pandey and K. Mustafa, "A Comparative Study of Risk Assessment Methodologies for Information Systems", Bulletin of Electrical Engineering and Informatics, Vol.1, No.2, pp. 111-122, June 2012.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[24] Mohammed Alnuem, Hala Alrumaih and Halah Al-Alshaikh, "A Comparison Study of Information Security Risk Management Frameworks in Cloud Computing", The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization, CLOUD COMPUTING 2015.
[25] Neeta Shukla and Sachin Kumar, "A Comparative Study on Information Security Risk Analysis Practices" International Journal of Computer Applications, Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies, 2012.
[26] Mouna Jouinia, and Latifa Ben ArfaRabaia, "Comparative Study of Information Security Risk Assessment Models for Cloud Computing systems", The 6th International Symposium on Frontiers in Ambient and Mobile Systems, Procedia Computer Science 83, pp. 1084 – 1089, 2016.
[27] Vivek Agrawal, "A Comparative Study on Information Security Risk Analysis Methods", Journal of Computers, Vol. 12, No. 1, January 2017.
[28] Nada Mannane , Youssef Bencharhi, BrahimBoulafdour and BoubkerRe gragui, "Survey: Risk assessment models for cloud computing: Evaluation criteria", 3rd International Conference of Cloud Computing Technologies and Applications , Rabat, Morocco, 24-26 Oct. 2017.
[29] K.V.D.Kiran, SaikrishnaMukkamala, AnudeepKatragadda and L.S.S.Reddy, "Performance And Analysis Of Risk Assessment Methodologies In Information Security", International Journal of Computer Trends and Technology (IJCTT),Vol. 4, Issue 10, October 2013.
[30] CORAS: A Platform for risk analysis of Security Critical Systems. IST-2000-25031. 2000.
[31] COBRA: Introduction to Security Risk Analysis. Available on: http://www.security-risk-analysis.com/
[32] CRAMM: Information Security Risk Assessment Toolkit, http://www.cramm.com
[33] https://csrc.nist.gov/publications/fips
[34] https://www.idc.com/
[35] https://www.nist.gov/
[36] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
[37] https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g
[38] https://technologyadvice.com/erm-software/
[39] https://www.rsa.com/en-us/products/integrated-risk-management
[40] https://www.risksync.com/

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Table 6: Output Risk Identification Phase (Group Session), N=3, M=6*

| i | $r_i$ | $t_i$ | $A_i$ | $V_i$ | $C_i$ |
|---|---|---|---|---|---|
| 1 | $r_1$ | $t_1$:account or service hijacking | $A_1$={storage resources, computational resources, customer's trust} | $V_1$={insufficient input-data validation, weak credential, insufficient authorization check} | $C_1$={$c_1$,$c_2$,$c_3$}={loss of confidentiality, loss of availability, loss of customers} |
| 2 | $r_2$ | $t_2$:data leakage | $A_2$={VM, storage resources} | $V_2$={incomplete data deletion, data backup done by untrusted third party, data is often stored, processed, and transferred in clear plain text, uncontrolled placement of VM images in public repository, sharing of virtual bridges by several VM, uncontrolled copying of VM, uncontrolled migration of VM. uncontrolled allocation and deallocation of VM, the IP addresses of VM are visible to anyone} | $C_2$= ={$c_1$,$c_4$}={loss of confidentiality, loss of integrity} |
| 3 | $r_3$ | $t_3$:sniffing/spoofing virtual network | $A_3$={virtual networks} | $V_3$={sharing of virtual bridges by several VM} | $C_3$={$c_1$,$c_5$,$c_6$}={loss of confidentiality , loss of trust, loss of privacy} |
| T={$t_1$,$t_2$,$t_3$} = {account or service hijacking, data leakage, sniffing/spoofing virtual network } C={$c_1$,$c_2$,$c_3$,$c_4$,$c_5$,$c_6$}= {loss of confidentiality, loss of availability, loss of customers, loss of integrity, loss of trust, loss of privacy} | | | | | |

*Table 7: Output Of Delphi Session And Risk Evaluation Phases*

| i | $t_i$ | $L(t_i)$ | j | $c_j$ | $L(c_j \mid t_i)$ | $I(c_j)$ | $E(r_i)$ |
|---|---|---|---|---|---|---|---|
| 1 | $t_1$ account or service hijacking | 0.8 | 1 | loss of confidentiality | 0.9 | 5 | 11.28 |
| | | | 2 | loss of availability | 0.8 | 7 | |
| | | | 3 | loss of customers | 0.5 | 8 | |
| 2 | $t_2$ data leakage | 0.7 | 1 | loss of confidentiality | 0.8 | 5 | 5.32 |
| | | | 4 | loss of integrity | 0.6 | 6 | |
| 3 | $t_3$ sniffing/spoofing virtual network | 0.5 | 1 | loss of confidentiality | 0.7 | 5 | 5.6 |
| | | | 5 | loss of trust | 0.5 | 9 | |
| | | | 6 | loss of privacy | 0.8 | 4 | |
| Overall security risk for ERP application in *AT*, $E_t$ | | | | | | | 22.2 |
| Risk factor in *AT* (R.F) | | | | | | | **0.123** |