A Quantitative Methodology for Cloud Security Risk Assessment

Srijita Basu[1], Anirban Sengupta[1] and Chandan Mazumdar[2]
[1]*Centre for Distributed Computing, Jadavpur University, 188 Raja S. C. Mullick Road, Kolkata, India*
[2]*Department of Computer Science and Engineering, 188 Raja S. C. Mullick Road, Jadavpur University, Kolkata, India*

Keywords: Asset Dependency, Cloud Security, Cloud Service Provider, Risk Assessment, Security Concern.

Abstract: Assets of Cloud stakeholders (Service Providers, Consumers and Third Parties) are the essential elements required to carry out necessary functions / services of the cloud system. Assets usually contain vulnerabilities that may be exploited by threats to jeopardize the functioning of the cloud system. Therefore a proper risk assessment methodology is required to determine the asset-specific and stakeholder-specific risks so as to be able to control them. Existing methodologies fail to comprehensively evaluate various risk elements like asset value, vulnerabilities and threats. This paper is an attempt to quantitatively model all risk elements and devise a methodology to assess risks to assets and stakeholders of a cloud system.

1 INTRODUCTION

Advances in Cloud Computing technologies have resulted in rapid growth in the adoption of Cloud-based services by small and medium-sized business organizations. However, it has been discovered by the Cloud Security Alliance (CSA) (CSA 2014) that inadequate due diligence by such organizations is one of the top threats to cloud computing. Usually, a Cloud Service Customer (CSC) enters into an agreement with a Cloud Service Provider (CSP) before initiating the process of service provisioning; this is referred to as a Service Level Agreement (SLA). Proper insight of both the parties regarding security and compliance requirements of their organizational data is essential before signing the SLA. Such requirements can be identified by performing a correct assessment of security risks that may arise due to provisioning of a cloud service. Security risks may emanate from multiple sources. For example, presence of inherent vulnerabilities within the assets of CSP and / or CSC, combined with the existence of relevant threats, may give rise to risks in cloud services. Besides, legal and regulatory issues regarding cross-border transfer of sensitive data, encrypted storage etc. (Janson and Grance 2011) may also give rise to risks that need proper management. The situation gets further complicated when a third-party service provider (CTS) is involved. In some cases, CSP outsources certain tasks (like auditing, billing, etc.) to a third party. Therefore, identification and management of security risks associated with third parties is critical in such situations.

Though there have been some preliminary research regarding the above issues, there is a dearth of proper quantitative risk assessment methodologies that can address the security issues which are specific to cloud-based services. This paper attempts to address this research gap by proposing a quantitative Cloud risk assessment methodology. Some of the fundamental notations and constructs of this work have been derived from (Bhattacharjee, Sengupta and Mazumdar 2013). The proposed methodology identifies the Cloud assets and evaluates those considering inter-asset dependencies. The vulnerabilities within those assets are identified and their Severity and Exploitability values are calculated. Also, values of Likelihood of Occurrence (LoC) of relevant threats are computed. Finally, two categories of Risk Factors (Asset-specific and Stakeholder-specific) are determined by combining the above values. It may be noted that the Cloud Computing Reference Architecture (CCRA) (ISO/ lEC 17789:2014(E)) has been used in this work to describe the Cloud components (functional units and assets).

Rest of the paper is organized as follows. Section 2 presents a survey of related work. Section 3 describes the process of identification of Cloud assets and Section 4 presents their valuation considering various inter-dependencies. Section 5 details the process of computing vulnerabilities and

Basu, S., Sengupta, A. and Mazumdar, C.
A Quantitative Methodology for Cloud Security Risk Assessment.
DOI: 10.5220/0006294401200131
In *Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017)*, pages 92-103
ISBN: 978-989-758-243-1
Copyright © 2017 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

threats. Section 6 describes the computation of risk factors. Section 7 illustrates the proposed methodology with the help of a case study. Finally, Section 8 concludes the paper.

2 RELATED WORK

Cayirci et. al. (Cayirci Et. Al. 2014) proposed a “Cloud Adoption Risk Assessment Model” (CARAM). Here Cloud risk is classified under 3 heads viz. Security, Privacy and Service. The model assesses risks for a particular CSP-CSC pair based on Cloud Assessment Initiative Questionnaire (CAIQ) of Cloud Security Alliance. An algorithm has been designed that converts the answers of CAIQ to discrete values. The probability and impact factor of a Cloud-based incident, along with the CAIQ values, are used to map the risk values on a qualitative scale. Moreover a maximum acceptable value of risk (R_{max}) is calculated for each CSP which is later used to select the best CSP from a group of probable candidates whose risk values are less than R_{max}.

Djemame (Djemame Et. Al. 2016) proposed a “A Risk Assessment Framework for Cloud Computing” which assesses and even tries to lessen Cloud risks at various stages of a Service life-cycle of an Infrastructure Provider. The Risk Assessment methodology followed here may be summarized in six steps: 1) Preparation of Risk Inventory (elements of Risks for Virtual Machines, Physical Hosts, and SLA); 2) Vulnerability Identification (Using Vulnerability Vectors represented by binary values); 3) Threat Identification (represented by binary values); 4) Data Monitoring (Data requirement which needs support are identified with the help of Cloud Monitoring Infrastructure (Djemame Et. Al. 2016)); 5) Event Analysis (Likelihood of Occurrence of a threat acting over a vulnerability); and 6) Quantitative Risk Analysis (Based on Likelihood of an event and its impact).

ENISA (ENISA 2009) provides a list of 35 incident scenarios, 31 Cloud Specific Vulnerabilities and 23 classes of CSC assets that can be affected as a result of Cloud service adoption. It provides a method of predicting the levels of risk on the basis of likelihood of a risk scenario mapped against the estimated negative impact. This has been used in many works for determining the risk factor of an enterprise (Kaplan 1981)

Luna et. al. (Luna Et. Al. 2012) discussed Cloud Security Level Agreements (SecLA) and proposed a methodology to benchmark SecLA of CSPs with respect to CSCs’ requirements (Luna Et. Al. 2012). Both CSP SecLA necessities and user requirements are depicted using a specific data structure termed as Quantitative Policy Tree. It facilitates expressing controls with varied granularity: CCM control areas, control groups, and controls (corresponding to CAIQ answers). The proposed approach utilizes the Reference Evaluation Methodology (Casola Et. Al. 2005) as a technique to quantitatively evaluate security policies. The authors describe their scheme using data of several CSPs from Cloud Security Alliance’s Security, Trust & Assurance Registry (CSA STAR), by calculating security levels for respective controls and control groups.

All the above approaches assess Cloud risks either quantitatively or qualitatively. However, these approaches are too generic and fail to address asset dependencies. Besides, a comprehensive mathematical approach to model all relevant factors, namely Cloud asset values, vulnerabilities, threats, and risks are not present in any of the above methodologies. The proposed work tries to address these gaps by formulating a mathematical model to identify and assess Cloud-specific risks.

3 ASSETS AND THEIR RELATIONSHIPS

As mentioned in Section 1, realization of cloud-based services may involve three kinds of stakeholders / organizations:

i) Cloud Service Provider (CSP)
ii) Cloud Service Customer (CSC)
iii) Cloud Third-Party Service Provider (CTS)

A risk assessment procedure generally begins with the identification and evaluation of assets of each of these stakeholders. Assets can be classified into two major categories: Primary assets and Supporting assets (ISO/lEC 27005 2011). Primary assets are those that are absolutely critical for the existence of the Cloud stakeholder. They are of two types: (i) Cloud processes and activities, and (ii) Cloud information assets. For example, the Cloud business support systems process encompasses the set of business-related management capabilities dealing with customers and supporting processes (ISO/ lEC 17789 2014). On the other hand, information assets comprise of documents, records as well as user credentials necessary for running business operations, and maintaining information security and compliance requirements, of the CSP.

Supporting assets are those that help to carry out the service provisioning process of the CSP, while maintaining the information assets required for the same. Thus, primary assets depend on supporting assets to fulfil their objectives. Important supporting assets are hardware, software, network and personnel (ISO/lEC 27005 2011).

Table 1: CSP Asset list.

Asset Name	P / S	Asset Type
Datacenter	S	Hardware Asset
Host/Server	S	Hardware Asset
Resources	S	Hardware/Software Asset
Virtual Machine (VM)	S	Software Asset
Virtual Machine Image (VMI)	P	Information Asset
Virtual Network	S	Network Asset
Personal Data of CSC	P	Information Asset
User Credentials	P	Information Asset
Data Storage (Files/disk blocks) in the form of SAN/NAS	P	Information Asset
Services	P	Cloud processes and activities
Security Logs	P	Information Asset
Functional Components (Required for Support, Patch and change management, Maintenance, monitoring, security of the deployed/offered cloud services (ISO/ lEC 17789:2014(E)))	P	Cloud processes and activities
SLA (Software Level Agreement) (with CSC as well as CTS)	P	Information Asset
Cloud Service Management Interface	S	Software Asset

Some of the important assets that are used by CSP are shown in Table 1. The categories and types of those assets have also been mentioned. In addition to these, a CSP usually consists of the following types of personnel (ISO/ lEC 17789 2014): i) Cloud Service Operations Manager, ii) Cloud Service Deployment Manager, iii) Cloud Service Manager, iv) Cloud Service Business Manager, v) Customer support and Care representative, vi) Inter-Cloud Provider, vii) Cloud Service Security and Risk Manager, and viii) Network Provider. Responsibilities and functions of each of these personnel have been detailed in (ISO/lEC 17789 2014).

Relationships between assets of the CSP are defined in terms of the interactions they have with each other. The following example illustrates such an interaction.

Example: The security and risk manager is responsible for ensuring that the CSP appropriately manages the risks associated with the development, delivery, use and support of cloud services. The manager also ensures that all relevant security policies and controls, mentioned in the SLA, are maintained. For carrying out this particular task, the manager is required to access the following processes and activities: i) Manage security and risk, ii) Design and implement service continuity, and iii) Ensure compliance. These activities in turn access several information assets like SLA, security logs, etc. to carry out the necessary functions. Finally, relevant hardware and software assets like VM, physical hosts, IDS/IPS, firewall, etc. need to be configured correctly to ensure protection of the cloud management network and maintain privacy and security of customer data and applications. Thus, there exist inherent dependencies between various assets of a CSP. Similar types of dependencies exist between assets of CSC and CTS as well.

Table 2: CSC Asset list.

Asset Name	P / S	Asset Type
User/Organization Data (Includes PII i.e. Personally identifiable information, Other application data, data in form of pictures, videos, etc.)	P	Information Asset
Encryption Keys	S	Software Asset
Functional Components (Required for Service Trial, Monitoring, administering security services, etc(ISO/ lEC 17789:2014(E)))	P	Cloud processes and activities
SLA (Software Level Agreement) (with CSP as well as CTS)	P	Information Asset
Cloud Service Management Interface	S	Software Asset
Audit Report	P	Information Asset

Table 2 lists the important assets of CSC. It should be noted that a CSC may act as a CSP in some cases. E.g. Suppose Organization A provides IAAS (Mell and Grance 2011) (Infrastructure as a Service) to Organization B. Organization B, in turn, provides SaaS (Mell and Grance 2011) (Software as a Service) to Organization C. Therefore Organization B is the CSC with respect to Organization A while it acts as a CSP with respect to Organization C. Such cases should be considered while identifying and establishing dependencies between assets.

A Cloud Third-Party Service Provider (CTS) is engaged in support of, or auxiliary to, the activities of either the CSP or CSC, or both (ISO/lEC 17789 2014). The important assets of CTS are depicted in Table 3.

Table 3: CTS Asset list.

Asset Name	P / S	Asset Type
Market Information (Includes present market status/services offered of/by various CSP and CSC (ISO/ lEC 17789:2014(E)))	P	Information Asset
Functional Components (Design Compose, Test services, etc (ISO/ lEC 17789:2014(E))])	P	Cloud processes and activities
SLA (Software Level Agreement) (with CSP as well as CSC)	P	Information Asset
Cloud Service Management Interface	S	Software Asset
Audit Report	P	Information Asset

4 ASSET VALUATION

After identifying all assets within the scope of risk assessment, their values need to be assigned, or computed. In a Cloud environment, Asset Value (AV) can be computed based on the following parameters:

- Security **(SR)**: This comprises of confidentiality (C), integrity (I) and availability (A) needs of an asset. SR may be computed as follows:
  $SR = x*C + y*I + z*A$, such that $(x + y + z = 1)$.

x, y and z are the relative weights associated with each security requirement and may be configured by the Cloud stakeholders based on their requirements and kind of asset considered.

- Auditability **(AR)**: Auditability may be defined as the need for collecting, and making available, necessary evidential information related to the operation and use of a cloud service, for the purpose of conducting an audit (ISO/lEC 17789 2014). Thus, AR denotes the significance of an asset in the context of an overall audit.
- Governance **(GR)**: This consists of External Governance (EG) and Internal Governance (IG). EG defines some sort of agreement between the CSP, CSC and CTS, or relevant regulations, for the use of Cloud services. IG refers to the set of internal policies followed by each of the stakeholders for assuring the expected delivery of services (ISO/lEC 17789 2014).

Asset Value may be calculated as follows:

$$AV= \mathit{ceil}(a*SR + b*AR + c*GR) \quad \text{such that } (a + b + c = 1). \tag{1}$$

Each of the above asset requirements may assume an integer value within the range 1-5. a, b, c are the relative weights associated with each asset requirement and may be configured by the Cloud stakeholders based on their requirements. Table 4 presents a set of guidelines that may be used by different categories of organizations for assigning values to asset requirements. It should be noted that asset valuation is usually organization and sector specific. The guidelines given in Table 4 are generic in nature and may be tailored to suit the needs of a particular organization.

The following section describes the dependencies between different assets and shows how the values of assets may be adjusted accordingly.

4.1 Asset Dependency

Identifying and analyzing the existing asset dependencies is essentially required for realizing the varied relationships that exist between the assets of an organization/stakeholder (CSP/CSC/CTS).

Based on the organizational framework of a Cloud system, two types of dependencies may be considered: Physical dependency and Logical dependency. An asset is physically dependent on another asset if it is connected to it, or included within it (Sengupta, Mazumdar and Bagchi 2009). In a Cloud environment, physical dependency may be manifested as *connections* between host machines, host and client machines, and host machines and storage devices. Such connectivity is implemented with the help of a physical network structure. Another type of physical dependency occurs owing to *inclusion* of documents/files within a VM or physical hosts of a data center.

On the other hand, logical dependency exists due to the need to know (*read* access) or need to use of a particular asset (*write*, *execute* or *modify* accesses). E.g. Processes pertaining to the management of

Table 4: Guidelines for assigning values to asset requirements.

Asset Values		5	4	3	2	1
Security (SR)	C	Govt. Organization/ Defense Data, Encryption Keys	Hospital Patient Records	Public Sector Data	Business Enterprise Data (Medium Sized)	Business Enterprise Data or Service (Small Sized)/ Customer Id, Product details
	I	Govt. Organization/ Defense Data, SLA	Hospital Patient Records	Public Sector Data	Business Enterprise Data (Medium Sized)	Business Enterprise Data (Small Sized)/ Customer Id, Product details
	A	Data Centre	Physical Hosts	VM (Containing Enterprise Applications)	Service/Application/Data (Mail Service/ Bank Applications), Network, SLA	Audit Report
Auditability (AR)		Cloud Data/ Services (Govt. Organization/ Defense)	Hospital Patient Records, VM, VMI	Public Sector Data	Business Enterprise Data (Medium Sized)	Business Enterprise Data (Small Sized)/ Customer Id, Product details
Governance (GR)		Data/ Applications with certain compliance requirement	Functional Components requiring Internal Policy Compliance	VM,VMI that should follow certain constraints in order to ensure expected delivery of deployed services	Physical Hosts that should follow certain constraints in order to ensure expected delivery of deployed services	Data centre, Virtual Network etc.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

security risks access the SLA (*read*) to ensure that proper security controls are being implemented. Similarly, audit processes prepare audit reports (*read*, *write*, *modify*), thus having logical dependency with them.

It is important to note that, the values of asset requirements (discussed in the previous section) need to be adjusted based on identified dependencies. Lack of such adjustments may lead to undervaluation of an asset which, in turn, may give rise to various risks. This is discussed in the following section.

4.1.1 Physical Asset Dependency

In case of physical dependencies the asset values may be adjusted as follows:

1. Assets a_{i1}, a_{i2},… a_{in} are included in another asset a_j

In case of cloud, a common inclusion relation is: Documents/Software<VM<Hosts<Datacenter

Where A<B signifies that asset A is contained in or part of asset B

We now look at ways by which values of security (SR), auditability (AR) and governance (GR) requirements of asset a_j can be adjusted in the presence of included assets.

The adjusted SR value of asset a_j can be computed as

$$SR({}^{inc}a_j)_{ai1,\ ai2,\ldots\ ain} = Max(SR(a_j), SR(a_{i1}), SR(a_{i2}), \ldots SR(a_{in}))$$

$SR({}^{inc}a_j)_{ai1,\ ai2,\ldots\ ain}$ can be interpreted as the adjusted SR requirement value of asset a_j owing to existence of *inclusion* relations with assets a_{i1}, a_{i2},… a_{in}. From this point onwards, we will use a more compact notation as follows:

$$SR({}^{inc}a_j) = Max(SR(a_j), SR(a_{i1}), SR(a_{i2}), \ldots SR(a_{in})) \tag{2a}$$

Values of AR and GR can be computed similarly. Thus,

$$AR({}^{inc}a_j) = Max(AR(a_j), AR(a_{i1}), AR(a_{i2}), \ldots AR(a_{in})) \tag{2b}$$

$$GR({}^{inc}a_j) = Max(GR(a_j), GR(a_{i1}), GR(a_{i2}), \ldots GR(a_{in})) \tag{2c}$$

2. An asset a_i is connected to another asset a_j

In case of connection relations, only SR requirements of assets need to be adjusted. This is owing to the fact that breach of security of an asset may result in the propagation of the same to other connected assets. However, the same does not hold for other kinds of requirements.

Connection may result in two types of situations:
i) the value of SR of a_j is greater than or equal to that of a_i
The value adjustment can be carried out as follows:
Let $SR(a_j) \geq SR(a_i)$. Then

$$SR({}^{con}a_j)_{ai} = SR(a_j) \tag{3a}$$

Since, the SR value of a_j is greater than that of a_i, no adjustment is needed.

ii) the value of SR of a_j is less than that of a_i.
In this case, the proposed value adjustment may be carried out as follows:
$SR(a_j) < SR(a_i)$. Then

$$SR({}^{con}a_j)_{ai} = ceil(SR(a_j) + ½\ (SR(a_i) - SR(a_j))) \tag{3b}$$

Thus, the SR value of a_j is increased by 50% of the difference in values between a_i and a_j. This is done to consider the security requirements of connected assets, without being too conservative.

4.1.2 Logical Asset Dependency

As already mentioned, logical asset dependency implies the access dependency between assets. This may be illustrated with the help of the following example.

Example: Processes pertaining to maintenance of service levels need to have *read* access on the SLA document in order to execute relevant actions.

Similarly, an asset may need *write*, *modify*, *delete* or *execute* access on another asset in order to carry out specific tasks. Each of these accesses may either cause information flow or modification of assets, or both. Hence, it is obvious that the security requirements (SR) need to be adjusted accordingly. We have adopted aspects of BellLaPadula rules (Bell and LaPadula 1976) to propose the following scheme for adjusting asset values considering logical dependency:

If asset a_i is allowed to have *read* or *execute* access on asset a_j, then

$$C(a_i) = Max(C(a_i), C(\{a_j\}) \tag{4a}$$

If asset a_i is allowed to have *write*, *modify* or *delete* access on asset a_j, then

$$I(a_j) = Max(I(a_i), I\{a_j\}) \tag{4b}$$

$$A(a_j) = Max(A(a_i), A\{a_j\}) \tag{4c}$$

This implies that security requirements of assets need to be adjusted considering logical dependencies.

5 VULNERABILITIES AND THREATS

After the computation of asset values has been completed, the vulnerabilities within assets, and their corresponding threats, need to be identified. These are discussed in the following sub-sections.

5.1 Vulnerabilities

Vulnerability is defined as an inherent weakness in an asset that can be exploited by threat(s) to breach security of assets (ISO/lEC 27005 2005). This breach may be realized in one of the following ways:

1) Unauthorized subjects at CSP end may have logical access to the CSC assets

2) Unauthorized subjects at CTS end may have logical access to the CSC assets

3) Unauthorized customers (other CSCs) may have logical access to the CSC assets

4) Unauthorized subjects at CSC/CTS end may have physical/logical access to the CSP assets

5) Unauthorized subjects at CSP/CSC end may have physical/logical access to the CTS assets

Vulnerabilities can be formally modelled with the help of two properties - severity and exploitability (Bhattacharjee, Sengupta and Mazumdar 2013).

5.1.1 Severity

Severity (Sev) of vulnerability indicates how critical the vulnerability is. In some cases, exploiting vulnerability within an asset might result in other (related or connected) assets to be impacted as well. We have modelled severity of vulnerability on a 5-point scale, as shown in Table 5.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 5: Severity of Vulnerability.

Severity	Interpretation
Very High (5)	Unauthorized subjects (CSP, CTS and other CSCs) can obtain logical access to multiple CSC assets Or Unauthorized subjects (CSC and CTS) can obtain both physical and logical access to multiple CSP assets Or Unauthorized subjects (CSP and CSC) can obtain both physical and logical access to multiple CTS assets
High (4)	Unauthorized subjects (CSP and CTS) can obtain logical access to multiple CSC assets Or Unauthorized subjects (CSC or CTS) can obtain both physical and logical access to multiple CSP assets Or Unauthorized subjects (CSP or CSC) can obtain both physical and logical access to multiple CTS assets
Medium (3)	Unauthorized subjects (other CSCs) can obtain logical access to multiple CSC assets Or Unauthorized subjects (CSC or CTS) can obtain either physical or logical access to multiple CSP assets Or Unauthorized subjects (CSP or CSC) can obtain either physical or logical access to multiple CTS assets
Low (2)	Unauthorized subjects (other CSCs) can obtain logical access to a single CSC assets Or Unauthorized subjects (CSC or CTS) can obtain either physical or logical access to a single CSP assets Or Unauthorized subjects (CSP or CSC) can obtain either physical or logical access to a single CTS assets
Very Low (1)	Vulnerability allows neither physical nor logical access to unauthorized subjects

5.1.2 Exploitability

Exploitability (Exp) of vulnerability denotes the ease with which the vulnerability can be exploited by a threat. It can be determined with the help of the following factors (Mell et. al. 2007):

Physical Access Vector (PAV) - This indicates the physical proximity requirement of the agent (attacker) that may exploit the vulnerability. It can assume values on a 3-point scale: (i) if local access (access from the same VM where the asset with the concerned vulnerability resides) is required, then PAV = 1; (ii) if the attack can be launched from any adjacent VM (i.e. within the same Physical Host) to the one where the target asset (containing the vulnerability) resides, then PAV = 2; (iii) if the attack can be launched from any physical host, then PAV = 3.

Logical Access Vector (***LAV***) - This denotes the access requirement of the agent (attacker) that may exploit the vulnerability. It can assume values on a 3-point scale: (i) if *write*, *modify* or *delete* access is required for the attacker, then LAV = 1; (ii) if *execute* access is required for the attacker, then LAV = 2; (iii) if *read* access is required for the attacker, then LAV = 3.

Attack Complexity (AC) - This factor signifies the amount of difficulty that needs to be encountered for launching a successful attack. Higher is the complexity, lower is the corresponding exploitability of vulnerability. This may include the cost (financial/time/bandwidth etc.) that is associated with launching an effective attack. AC assumes subjective values as High (3), Medium (2), and Low (1).

Authentication Level (AL) - This denotes the number of authentication stages that are needed for gaining access to the target asset. It can assume values on a 3-point scale: (i) if multiple instances of authentication are required before being granted access to the target asset, then AL = 1; (ii) if a single instance of authentication is needed, then AL = 2; (iii) if no authentication needed, then AL = 3.

Based on the values of the factors stated above, exploitability of vulnerability v is computed as:

$$\text{Exp}(v) = \textit{ceil}((\text{PAV} * \text{LAV} * \text{AL}) / (6 * \text{AC})) \qquad (5a)$$

Integer 6 is used in the denominator to scale down the value. Thus, $\text{Exp}(v)_{(max)} = \textit{ceil}((3 * 3 * 3) / (6 * 1)) = 5$ and $\text{Exp}(v)_{(min)} = \textit{ceil}((1 * 1 * 1) / (6 * 3)) = 1$

$$\text{Hence, Exp}(v) \in \{1, 2, 3, 4, 5\} \qquad (5b)$$

5.2 Threats

Threat is defined as an active agent that can exploit vulnerabilities to cause harm to an asset (ISO/lEC 27005 2005). It comprises of: agent (primary and secondary), motive, resource, and result. Primary agents are the sources which initiate the exploitation of vulnerability. These can be of the following types (Bhattacharjee, Sengupta and Mazumdar 2013):

1) Nature (E.g. Earthquake, Flood, etc)
2) Environment (Power Fluctuation, Chemical Contamination, Fire, etc)
3) Human Beings (Internal Stakeholders, External Stakeholders)

The above mentioned agents may directly exploit vulnerabilities or may use secondary agents for the same. Secondary agents in a Cloud environment include accounts, services, data, interface, VM, VMI, hypervisor, virtual as well as physical networks, and physical hosts.

Motive is related to primary agent; it indicates the purpose or intent of the agent. Types of motives are Deliberate (Malicious) intent and Accident. Malicious intent is associated with human beings; accidents can be caused by human beings as well as the environment (e.g. fire); while, Nature has no specific motive or agenda.

Different resources may be required for the realization of a threat. Types of resources are: (i) financial resource; (ii) manpower; (iii) knowledge or expertise; (iv) tools, techniques, and infrastructure; (v) time; and vi) administrative rights

The result (impact) caused by the exploitation of vulnerabilities by threats in a Cloud environment can be one or more of the following (Hashizume et. al. 2013):

1) Account or service hijacking: Account theft may affect the confidentiality, integrity as well as the availability of the associated service
2) Data scavenging: In certain cases, data may not be permanently deleted and may be recovered by some malicious user. This mainly affects the confidentiality of service data.
3) Data Leakage: Data leakage happens when it is accessed by an unauthorized user while it is being transferred, stored, audited or processed. This may again affect C, I, A requirements of the data.
4) Denial of Service: This mainly affects the availability of the services as well as data. EDoS (Economic Denial of Sustainability) is specific to Cloud environment which results in exploitation of financial resources of the concerned stakeholder.
5) VM escape: This is caused by exploitation of the hypervisor (code) resulting in the transfer of control of the underlying hypervisor to the attacker. This mainly causes loss of integrity of the infrastructure (as a whole).
6) VM hopping: A VM may illegally gain access to the resources as well as data of another VM by manipulating hypervisor code or by covert channel. It may be the case that an illegal Virtual Network has been set up between the two VMs for this purpose.
7) Malicious VM creation: An attacker who manages to create a valid user account in the CSP end may upload malicious VMIs (containing malware) into the Cloud VM repository. A normal user who accesses this VMI gets affected. The user’s data as well as the CSPs infrastructure is compromised as an effect of this action.
8) Insecure VM migration: Exposure of VM metadata and sensitive data within the VM remain vital issues in the context of VM migration. Both, during the migration of VM through the network, and after the migration is completed to some other physical host, the VM data/metadata may be compromised.
9) Sniffing/Spoofing virtual networks: This is similar to (6) where virtual networks may be utilized for establishing unauthorized communications between two VMs (Address Resolution Protocol spoofing may be used to redirect packets illegally).

Threat can be formally modelled with the help of its likelihood of occurrence.

Likelihood of Occurrence: Likelihood of occurrence (LoC) defines the probability of occurrence of a threat. This can be determined by the following factors:

Past occurrences: This represents previous incidents that have occurred due to the threat (being considered). This includes incidents both in the recent past as well as distant past (with appropriate weights). This is denoted by t_p (Bhattacharjee, Sengupta and Mazumdar 2013). t_p can be calculated depending on the i) no. of occurrences of threat t; and ii) time (year) when threat occurred.

For example, if a 5-year period is considered, and if "t" has occurred twice during the previous year, 3 times during the year before, and so on, then $t_p = 2 * 5 + 3 * 4 + ...$, with greater weight having been assigned to incidents that have occurred more recently. Moreover, a threshold value is chosen for no. of occurrences i.e. for 5 or more than 5 incidents the value taken for calculation is 5 and for lower occurrences that particular occurrence value is taken for the calculation. Again, certain weights are assigned depending on which year the incident had occurred. A recent incident is assigned a higher weight i.e. if an incident has occurred in the previous year then the weight assigned is 5, if it has occurred during the year before then the weight assigned is 4 and so on. This period may even be taken as a "month"/ "week"/ "day" / "hour" depending on the particular threat. Thus,

$$t_p = \mathit{ceil}(\Sigma(\text{count}(t) * \text{weight}(\text{period})) / \Sigma \text{weight}(\text{period})), \text{ when count}(t) > 0 \quad (6a)$$
$$= 1, \text{ when count}(t) = 0$$

It can be seen that

$$\max(t_p) = \mathit{ceil}((5 * 5 + 5 * 4 + 5 * 3 + 5 * 2 + 5 * 1) / (5 + 4 + 3 + 2 + 1)) = \text{ceil}(75/15) = 5. \quad (6b)$$
$$\text{Hence, } t_p \in \{1, 2, 3, 4, 5\}$$

Proximity of assets to threat-prone areas: This is mostly applicable to natural and environmental threats. It represents the physical proximity of assets to areas that are prone to threats. It is denoted by a_t (Bhattacharjee, Sengupta and Mazumdar 2013). It is determined on a 3-point scale. The areas where natural threats (Earthquake prone regions, Volcanic regions, High altitude areas etc.) exist can be categorized into "danger zone" (most threat-prone), "striking zone" (less prone to threats i.e. some environmental threat like power fluctuations might occur), and "safe zone". If asset "a" is within the "danger" zone, then a value of 3 may be assigned to a_t; if it is within "striking" zone, a value of 2 may be assigned; anything beyond has value 1. If this is not applicable for a threat, then a value of 1 is assigned to a_t (for ease of computation of LoC). Hence,

$$a_t \in \{1, 2, 3\} \quad (6c)$$

Combining the above factors the likelihood of occurrence of threat may be given by:

$$\text{LoC}(t) = \mathit{ceil}((t_p * a_t) / 3) \quad (6d)$$

Integer 3 is used in the denominator to scale down the value.

Thus, $\text{LoC}(t)_{(\max)=}$ $\mathit{ceil}((5 * 3) / 3) = 5$ and $\text{LoC}(t)_{(\min)} = \mathit{ceil}((1 * 1) / 3) = 1$

$$\text{Hence, LoC}(t) \in \{1, 2, 3, 4, 5\} \quad (6e)$$

6 SECURITY CONCERN AND RISK

After computing asset, vulnerability and threat values, the security concern and risk factors need to be determined. Security concern (SC) may be defined as the apprehension of the exploitation of a particular vulnerability in an asset by some threat. It can be mathematically expressed in terms of severity of vulnerability (Sev) and Breachability. Breachability defines the potential of a threat being able to exploit a given vulnerability (Bhattacharjee, Sengupta and Mazumdar 2013). Intuitively, this is possible when vulnerability is exploitable and both motive, as well as resources, for realization of a threat, is present. Therefore, Breachability can be computed as:

$$\text{BT}(t,v) = \mathit{ceil}((\text{LoC}(t) * \text{Mvn}(t) * \text{Res}(t) * \text{Exp}(v)) / 5), \text{ when Mvn}(t)=\text{Res}(t) = 1 \quad (7a)$$
$$= 1, \text{ otherwise}$$

Here, LoC(t) is the likelihood of occurrence of threat t, Mvn(t) denotes the existence of motive of threat t, Res(t) denotes resource availability for t, and Exp(v) is the exploitability of vulnerability v. Both Mvn(t) and Res(t) can be modelled on a binary scale, with 0 representing absence of motive, or resource, and 1 denoting presence of the same. It may be noted that the formula for Breachability has been devised in a way such that its minimum value is 1. This has been done to reflect the fact that any vulnerability is breachable, sooner or later. It depends on the availability of resources, motive, etc. Absence of sufficient threat factors at a particular moment does not imply that the vulnerability will never be breached.

It is obvious from (5b) and (6e) that

$$\text{BT}(t,v) \in \{1, 2, 3, 4, 5\} \quad (7b)$$

Security concern is computed as:

$$\text{SC}(t, v) = \mathit{ceil}((\text{BT}(t, v) * \text{Sev}(v)) / 5) \quad (8a)$$

Here, SC(t, v) is the concern that threat "t" will exploit vulnerability "v", BT(t, v) is the breachability of vulnerability v against threat “t”, and Sev(v) is the severity of vulnerability “v”. The denominator helps to scale down the value of SC.

Now the Max and Min values for SC(t, v) are as follows:

$SC(t, v)_{max} = \mathit{ceil}(5 * 5 / 5) = 5$

$SC(t, v)_{min} = \mathit{ceil}(1 * 1 / 5) = 1$

$$\text{Thus, } SC(t, v) \in \{1, 2, 3, 4, 5\} \quad (8b)$$

Finally, asset value and security concern are combined to obtain the value of risk. As stated in Section 1, the proposed methodology computes and presents risk values in two forms – Asset-specific risk and Stakeholder (CSP, CSC and CTS) specific risk.

Assets of a stakeholder can be evaluated as shown in Section 4. Moreover, the security concern values for a stakeholder can be computed by considering severity and breachability values for only that particular stakeholder. These can be combined to obtain stakeholder-specific risk values.

Let a_i be an asset of CSP. Since, an asset may contain multiple vulnerabilities, there will be multiple security concern values corresponding to each threat-vulnerability pair. Let SC_{imax} denote the maximum security concern value for asset a_i. Then the risk factor corresponding to asset a_i is given by

$$RF(a_i) = \mathit{ceil}((AV_i * SC_{imax}) / 5) \quad (9a)$$

where, AV_i denotes the asset value of asset a_i. It can be seen from (1) and (8b) that

$$RF(a_i) \in \{1, 2, 3, 4, 5\} \quad (9b)$$

The combined risk value for all assets of CSP can be computed as:

$$RF_{CSP} = \mathit{RoundOff}(\sum(RF(a_i) / n) \quad (9c)$$

where, i = 1,…,n, and “n” denotes the no. of assets of the CSP.

It is obvious from (8b) that

$$RF_{CSP} \in \{1, 2, 3, 4, 5\} \quad (9d)$$

The risk values for CSC and CTS can be computed following a similar approach. The values of RF may be interpreted as follows:

$RF_{CSP} = 5 \Rightarrow$ “Very High Risk”

$RF_{CSP} = 4 \Rightarrow$ “High Risk”

$RF_{CSP} = 3 \Rightarrow$ “Medium Risk”

$RF_{CSP} = 2 \Rightarrow$ “Low Risk”

$RF_{CSP} = 1 \Rightarrow$ “Very Low Risk”

Analyses of the value of risk factor (RF) show that it is directly proportional to the values of (i) security requirement (SR); (ii) auditability requirement (AR); (iii) governance requirement (GR); (iv) severity of vulnerability (Sev); (v) likelihood of occurrence of threat (LoC); and (vi) exploitability of vulnerability (Exp). This follows from equations (1), (7a), (8a) and (9a). Hence, any increase / decrease in values of those parameters cause the risk factor to proportionately increase / decrease. The percentage of change in the value of RF is exactly same as that of the percentage of change in the values of Sev, LoC and Exp. However, the amount of change in RF vis-à-vis SR, AR and GR would depend on the values of relative weights of those parameters (a, b, c in Eq. 1).

It is important to identify stakeholder-specific risk when a CSC selects a particular CSP for availing its services. This is also required during the selection of CTS by a CSP. The current risk value helps a stakeholder evaluate the security posture of a probable provider / partner, before availing of its services. The calculation of stakeholder-specific risk may be done by a third-party (e.g. Cloud Broker) or the stakeholder itself. When a particular organization opts for a Cloud-based service, the Cloud Broker or the stakeholder can provide the values of RF to the organization. This would help the organization to make an informed decision regarding stakeholder selection.

7 CASE STUDY

A case study is described here which applies the proposed methodology to compute risks to assets of a Cloud enterprise (CSP1). The enterprise has assets as shown in Figure 1.

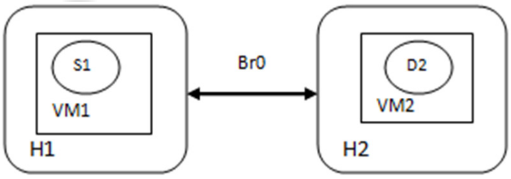

Figure 1: CSP1 Infrastructure.

H1& H2 are Physical Hosts residing in the CSP premises. VM1 is the Virtual Machine in H1 and VM2 is the Virtual Machine in H2. Service S1 is deployed in VM1 and Data file D2 is stored in VM2. Hosts H1 and H2 share the Bridge Network Br0 (assets may be referred from Table 1). The asset values (with dependencies) for the above mentioned assets have been listed in Table 6; these are based on the guidelines depicted in Table 4.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 6: Asset Values of CSP1.

Asset ID	SR			AR	GR
	C	I	A		
H1	5	4	5	4	3
H2	4	3	4	4	3
VM1	5	4	5	4	3
VM2	4	3	4	4	3
S1	1	4	5	4	3
D2	4	3	2	4	3
Br0	1	1	5	2	2

Here RF(a_i) is calculated for each asset depending up on the AV and SC values for each. The Final value AV (Asset Value) for each asset is calculated as follows:

SR_{HI} = 5*.3 + 5*.3 + 4*.4 = 4.6 and AV_{HI} = *ceil*(4.6*.3 + 4*.3 +3*.4) = 4

SR_{H2} = 4*.3 + 3*.4 + 4*.3 = 3.6 and AV_{H2} = *ceil*(3.6*.3 + 4*.3 +3*.4) = 4

SR_{VM1} = 5*.3 + 4*.4 + 5*.3 = 4.6 and AV_{VM1} = 4.6*.3 + 4*.3 + 3*.4 = 4

SR_{VM2} = 4*.3 + 3*.4 + 4*.3 = 3.6 and AV_{VM2} = *ceil*(3.6*.3 + 4*.3 +3*.4) = 4

SR_{S1} = 1*.5 + 4*.3 + 5*.2 = 2.7 and AV_{S1} = *ceil*(2.7*.5 + 4*.1 +3*.4) = 3

SR_{D2} = 4*.3 + 3*.4 + 2*.3 = 3 and AV_{D2} = *ceil*(3*.4 + 4*.2 +3*.4) = 4

SR_{Br0} = 1*.3 + 1*.4 + 5*.3 = 2.2 and AV_{D2} = *ceil*(2.2*.4 + 2*.3 +2*.3) = 3

The list of vulnerabilities and threats considered, along with their corresponding values, has been shown in Table 7.

Table 7: Vulnerability & Threat list.

Vulnerability	Sev (Severity)	Threat	LoC
Information about the location of the data usually is unavailable or not disclosed to users(V1)	3	Data Scavenging + Data Leakage (T1)	3
Uncontrolled placement of VM images in public repositories, (V2)	4	Malicious VM Creation (T2)	3
Insufficient input-data validation (V3)	5	Account/ Service Hijacking (T3)	4

Next the Exp values for V1, V2, and V3 are calculated using Equation (5a).

Exp(V1) = 4, Exp(V2) = 4, Exp(V3)= 5

Considering α=0.5, β= 0, γ=0 and δ=0.5 (In Eqn. 7a),

BT(T1,V1)= *ceil*(3 * 4 / 5)= 3

BT(T2,V2)= Roundoff (3 * 4 / 5)= 3

BT(T3,V3)= Roundoff (4 * 5 / 5)= 4

Next the Security Concern, SC is computed as Eq. 8a

SC(T1,V1) = *ceil*((BT(T1, V1) * Sev(V1))/5)
= *ceil* (3*3/5) = 2

SC(T2,V2)= *ceil* (3*4/5) = 3

SC(T3,V3)= *ceil* (4*5/5) = 4

Finally,

RF(H1) = *ceil*((AV_{H1} * SC_{H1max}) / 5)
= *ceil*((4 * 2) / 5) = 2

Similarly, RF(H2) = 2, RF(VM1) = 2, RF(VM2) = 2, RF(S1) = 3, RF(D2) = 4, & RF(Br0) = 2.

Therefore the value of RF_{CSP1}=
RoundOff ((2+2+2+2+3+4+2)/6) = 3

Thus, assets of CSP1 exhibit "Medium Risk" overall.

8 CONCLUSIONS

The quantitative Cloud risk assessment methodology, proposed in this paper, models assets, vulnerabilities, threats and computes the individual risks associated with an asset. The methodology also computes combined risk values from the perspective of CSP, CSC and CTS. The proposed scheme first lists the various assets of a Cloud organization. Values are assigned to these assets after considering the possible physical and logical dependencies between them. The vulnerabilities associated with these assets are modelled using their Severity and Exploitability values. Similarly, modelling of threats is performed using LoC (Likelihood of Occurrence) values. Then, Breachability value is calculated for threat-vulnerability pairs and Security Concern is derived from Breachability and Severity values. Finally, risk factors are computed for assets and stakeholders.

It should be noted that the Asset-specific risk factor is essential for a particular Cloud organization for deciding the specific measures (mitigation/ prevention/ transfer/ acceptance) that should be implemented to protect its assets. On the other hand, when a Cloud organization needs to utilize the services of another organization, the Stakeholder-specific risk should be considered for choosing a suitable service provider.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Future work is geared towards the validation of the proposed methodology in actual organizations and subsequent development of a tool based on this. Moreover, we intend to include information regarding cloud security capabilities (e.g. Data at rest encryption, multi-factor authentication, Trusted Cloud Computing Platform) of the provider during computation of risk factors. This would help provide assurance about the security measures that are deployed by the cloud service provider.

REFERENCES

Bell, D.E., and LaPadula, L.J., 1976 "Secure Computer Systems: Unified Exposition and Multics Interpretation", ESD-TR-75-306, MTR 2997 Rev. I, Mitre Corporation, Bedford, Massachusetts, USA, 1976.

Bhattacharjee, J., Sengupta, A., and Mazumdar, M., 2013. “A Formal Methodology for Enterprise Information Security Risk Assessment”. In International Conference on Risks and Security of Internet and Systems (CRiSIS). France: IEEE, pp. 1-9.

Casola V., et.al. 2005. “A Reference Model for Security Level Evaluation: Policy and Fuzzy Techniques.” In Journal of Universal Computer Science. 11(1), pp. 150–174.

Cayirci, E., Garaga, A., Santana, A., and Roudier, Y., 2014. “A Coud Adoption Risk Assessment Model”. In 7th International Conference on Utility and Cloud Computing. London: IEEE, pp. 908-913.

CSA. (2014), The Notorious Nine Cloud Computing Top Threats in 2013, [online] Available at https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. [Accessed 16 November 2016]

Djemame, K., Armstrong D., Guitart J., and Macias M., 2016. “A Risk Assessment Framework for Cloud Computing”. In IEEE Transactions on Cloud Computing. 4(3), pp. 265-278.

ENISA, “Cloud Computing; Benefits, Risks and Recommendations for Information Security,” 2009 Edition, Place: Available at http://www.enisa.europe.eu, [Accessed 16 November 2016]

Hashizume, K. Rosado, D.G., Fernández-Medina, E., and Fernandez, E.B., 2013 “An analysis of security issues for cloud computing”, In J. Int. Serv. App. vol. 4(5), . pp. 1-13.

“ISO/lEC 27005:2005,” Information technology - Security techniques - Code of practice for information security management”, Switzerland, 1st Edition.

“ISO/lEC 27005:2011, “Information technology - Security techniques Information security risk management”, Switzerland, 1st Edition.

“ISO/ lEC 17789:2014(E), Information technology – Cloud Computing – Reference Architecture”, Switzerland, 1st Edition.

Jansen, W. and Grance, T., 2011. “Guidelines on Security & Privacy in Public Cloud Computing”. In Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800-144. Gaithersburg: National Institute of Standards & Technology.

Kaplan, S., and Garrick B.J., 1981. “On The Quantitative Definition of Risk,” In the Journal of Risk Analysis 1(1), pp. 11-27.

Luna, J. L., Langenberg, R., and Suri, N. 2012. “Benchmarking cloud security level agreements using quantitative policy trees”. Cloud Computing Security Workshop, 103. doi:10.1145/2381913.2381932.

Mell, P. M., and T. Grance., 2011. “The NIST Definition of Cloud Computing.” In Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800-145. Gaithersburg: National Institute of Standards & Technology.

Mell, P., Scarfone, K., and Romanosky, S., 2007 “CVSS – A Complete Guide to the Common Vulnerability Scoring System Version 2.0”.

Sengupta, A., Mazumdar, C., and Bagchi, A., 2009. “A Formal Methodology for Detection of Vulnerabilities in an Enterprise Information System”, In Proceedings of the Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS), 2009, France:IEEE, 74-81.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS