DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4813

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

THE ASSESSMENT OF RISKS IN PUBLIC CLOUD ENVIRONMENT BY DEVELOPING MULTINOMINAL LOGISTIC REGRESSION MODEL

M.Sri Bindu
Student, Department of Computer Science,
K.L.University, Guntur, Andhra Pradesh
India

G.Sravani
Student, Department of Computer Science,
K.L.University,Guntur,Andhra Pradesh
India

M.S.R Prasad
Professor, Department of Computer Science,
K.L.University,Guntur, Andhra Pradesh
India

Abstract: The public cloud information infrastructure is getting increasing complex and well-connected which, in parallel, increases the risks to the cloud assets. Hence it becomes the need of the hour to identify, analyze and mitigate the risks towards the information security systems and the data associated with it. In the current research work, a quantitative information security risk analysis methodology is proposed for public clouds. In the existing methodology, enterprises follow two approaches such as consolidated and detailed approach towards information security in which the former computes risk as single value for every asset, whereas, the threat-vulnerability pair responsible for a risk is identified and a risk factor corresponding to each security property for every asset is computed in latter approach. In the proposed methodology, the assets in the public cloud are studied in which the consolidated approach is used to find the risk factor of each of these assets. The assets are classified into three different risk zones namely high, medium and low risk zone. In case of high-risk assets, it becomes mandatory for the management to install high cost infrastructure to overcome the risk. For medium-risk assets, proper auditing and ensuring all policies, guidelines and procedures in place may reduce risks. For low-risk assets, there is no such need to invest much from the management.

Keywords: Public Clouds, Risk analysis, Risk Factor

1. INTRODUCTION

There is a tremendous growth experienced in the speed and scale of Information Systems. In spite of the fact that computer networks entered our life like never before and made activities simpler and faster, the threats coupled with information system is annoying. During the instance, when a system is loaded with huge assets of information, but exposed to outside world, the possibility of losing important information and resources is high. Threats attack the assets and exploit the vulnerabilities associated with it. Generally, in any business, assets are the backbone and any damage occur to these assets bring chaos in the enterprise which is of great concern for its shareholders. So, it is a need to develop a systematic approach to mitigate such risks by evaluating the available information on security risks and framing protection strategies accordingly [1].

The present risk assessments for system security are mostly qualitative-based which are designed on the grounds of different security assessment standards that predominantly reflect few properties during the statistic design and the system development. In parallel, another kind of system security assessment deploys attack-simulation during security test. Still, this kind of attack test can only show the system insecurity and cannot prove the system security. In both the methods discussed above, uncertainty and dynamic property that arise from the mutual influence between the operation circumstance and information system, left unnoticed [2].

The importance behind risk assessment is to derive a systematic and comprehensive evaluation of the risks associated with the information systems. Human or natural threats may introduce a security event or otherwise a security risk in information systems because of the survivability of information system. Otherwise, the security events' probability and how severe those events are will decide the security risk [3]. The main objective of risk analysis is to estimate the risk factor of the assets present in the cloud. Each asset may have different risk factor values depending upon its threats and vulnerabilities. In threat action, one asset may have one or more than one vulnerabilities which might be exploited by the threat agents. The result of this action may potentially cause harm in terms of data security breach, confidentiality, integrity and/or resource availability that belongs to the cloud organization or third parties whomever involved with it.

A cloud asset is any information, system or hardware that is used in the course of business activities in the cloud. The assets which are thoroughly studied and considered in the project are physical and logical assets. Physical assets include software and hardware components whereas Logical assets include cloud management and asset monitoring. Vulnerability is nothing but a weakness using which an attacker may possibly create a mishap in the system's information and the assurance provided on it. Threat, a possible danger may exploit such a vulnerability discussed above to break the security and may harm the system. The threats for these assets include Power faults, Equipment incompatibilities, Corruption of data, Theft of media & documents, Link breaks and Coding errors. Generally, assets are the primary business needs in an organization, which when damaged or when attempted to damage, cause risk which is of greater concern to the enterprise and to its shareholders.

2. RISK ANALYSIS PROCESS

To carry out the process of risk analysis process, three main requirements are included, which are security requirement, business requirement and legal requirement [4].

2.1. Security Requirement

- Access-In private organizations, only authorized users can have data access. Such access need to be provided only to limited people such as specific customers and auditors to mitigate such risks. The values ranging from 1 to 5 are taken.
- Availability-As customers have to be addressed without any time delays, availability plays a major role in cloud computing. The values do range from 1-5 are considered.
- Network Load-Cloud network load is also proved to reduce the performance of the cloud computing system. The values ranging from 1 to 5 are taken.
- Reliability- Reliability determines the recovery of a system when any faults occur. Values ranging from 1 to 5 are taken.
- Data Security– Data security is one another key criterion in cloud since the data needs to be secured in an appropriate manner from outsiders. Data protection is mandatory and there is a need to ensure that that data security is less prone to corruption. The values ranging from 1 to 5 are taken.
- Data Location– In cloud computing, data location is one more aspect since the service providers are spread across the globe and not from a single location. The values, ranging from 1 to 5 are taken.

2.2. Business Requirement

An asset within a CLOUD is primarily used to run the entire processes in a proper manner. Since it is a graded parameter, it is scaled from 1 to 5 on the basis of magnitude of the loss incurred.

2.3. Legal Requirement

Legal requirement is a bundle of statutory and contractual requirements which have to be satisfied among the organization, its service providers, trading partners and contractors. Legal requirement parameter has only two values such as 0 and 5 in which the former denotes if there is no such requirement and latter, the vice versa.

3. RISK ANALYSIS METHODOLOGY

Risk analysis is conducted only for two main aims. The first aim is, risk analysis helps in identifying the actual risks to organizational assets. The second aim is, it supports to select security controls for protecting the organizational assets. On the basis of these two aims, two different approaches have been proposed in the current research work to identify the risks which are associated with an asset. The first approach is consolidated approach which computes a risk factor value for every asset. This specific value defines an asset as whether it is at high or medium or low risk. The second approach seems to be a broad approach which not only computes a risk factor value, but in addition, it also identifies the threat-vulnerability pair, the reason behind the risk. Risk management standards also suggest a two-pronged approach in which the first one is ‘high-level risk assessment’ which usually takes business values of information assets, and the risks from the organization’s business point of view into account whereas a detailed risk assessment encompasses the in-depth identification and valuation of assets, assessment of threats to those assets, and assessment of vulnerabilities [6]. In the proposed methodology of current research work, the consolidated approach corresponds to high-level risk assessment, while a detailed approach helps to perform a detailed risk assessment

Consolidated Approach

As discussed earlier, a risk factor value is computed in consolidated approach for every asset.

Risk Factor: Risk Factor [*RF*], is defined as a function of the asset value and its security concern and since it is usually associated with an asset, one can identify the risks involved with an asset based on this value such as high, medium or low risk.

Risk Factor (*RF*) = *Function* (*AV, SC*)

where, AV is asset value and SC is Security Concern (defined later) of an asset

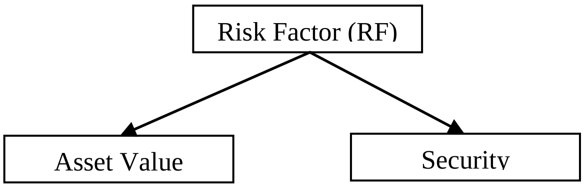


Fig. 1. Risk Factor Calculation

Asset Value: Asset Value [*AV*] of an asset can be defined as a function of security, business and legal and contractual requirements which are associated with an asset. AV is a graded parameter and its value is obtained on a scale of 1 to 5.

AssetValue (AV) = Function (SR, BR, LR)

where, SR is Security Requirement, BR is Business Requirement and LR is Legal Requirement [8]. The above said parameters are calculated as below.

SR = Avg of all SR’s

BR = Li

LR = Lr

Asset Value [*AV*] is calculated as

AV = a*SR+ b*LR+ c*BR, a +b+c=1, *if LR not equals* 0;

a*SR + b*BR, a +b =1, *if LR* = 0. where a= alpha, b= beta and c= gamma

In the above formula, the relative weights are denoted as alpha, beta and gamma assigned towards security, business and legal requirements respectively. One must observe that the individual components of the SR were assigned equal weights. However, on the basis of requirement and priorities in an institution, it is fine to apply the relative weights. For instance, in military organizations, confidentiality requirements may be given higher priority than other security parameters due to which the weights may be altered according to custom needs. Since, in any organization, security requirement is the prime determinant for evaluating the security risk, it is obvious to assign increased weight to it. Based on the organizational type, assets owned by the organization, the way how these assets are utilized, the decision towards the business, legal and contractual requirements are made. Accordingly, the organizational type (otherwise, the type of business which an organization conducts) can be taken as a base to adjust the weights for calculating AV.

For instance, considering a= 0.5, b = 0.25, and c = 0.25

AV = 0.5*SR + 0.25*LR + 0.25*BR

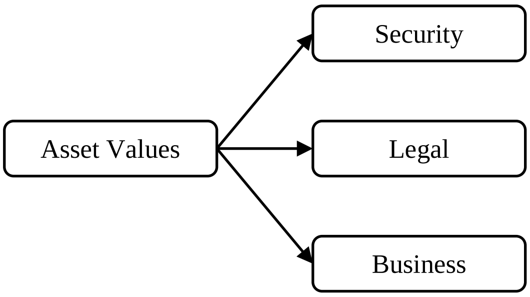


Fig. 2. Asset Value Calculation

Security Concern: It is defined as a function of threats and vulnerabilities which might be connected to an asset. Threats and vulnerabilities have many-to-many relations [8]. It is possible to obtain the SC value through the determination of vulnerabilities that can potentially be exploited by a threat. Security Concern is a graded parameter and have a scale of 1 to 5.

Security Concern (SC) = function (Tv, Vv) where Tv is Threat value and Vv is Vulnerability value [8].

For the purpose of computing asset A’s Security Concern [*SC*], one must obtain a list of threats such as [*T*1, *T*2, . . ., *Tm*] that can positively be in association with specific asset in addition to their Likelihood of Occurrence [*Loc*(*T*)] values. Loc value is defined as the probability of incidents of a threat that may be connected with an asset based on the earlier experience or availability statistics. Loc value is a three-scale value such as Low (1) / Medium (3) / High (5) specified with their numerical values in brackets. Then, for each threat *Ti*, a list of vulnerabilities [*Vi*1, *Vi*2 ..., *Vin*] that might be capable to be exploited by the threat are identified in addition to their Severity [*Sev*(*V*)] values [8]. Sev value is defined as the level upto which the vulnerability (associated with an asset) is or can be exploited by some threat. Sev too produces a three-scale value as in Loc.

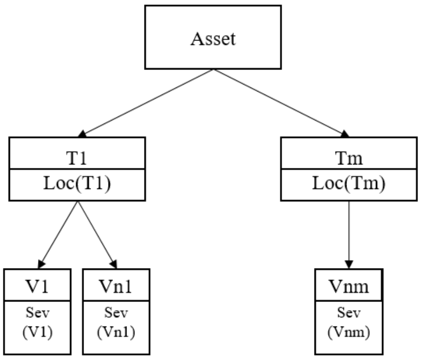


Fig. 3. Security Concern Calculation

The figure 3 shows how a threat-vulnerability tree is formed and how it helps to compute the Security Concern of an asset. When calculating from the bottom of the tree, the vulnerability value is calculated based on each threat to the asset. Imagine if there are ‘n’ number of vulnerability to an asset which can be exploited by a specific threat, say Ti low/medium/high converted to numerical values 1/3/5, depending on how easily it can be exploited. Vulnerability value *Vv* corresponding t0 threat Ti is determined as

Vvi = (sigma(Sev(Vj))/n,j=1...,n,if n>0;

1, if n=0

Threat value corresponding to threat Ti is determined as

Tvi = RoundOf [log2 (Vvi * Loc (Ti))]

The reason behind taking base 2 of the logarithm is to normalize the result within a scale of 0 to 5. Through the identification of the most critical threat, Security Concern value is obtained. So SC value for an asset remains the maximum of all the threat values for an asset as given below

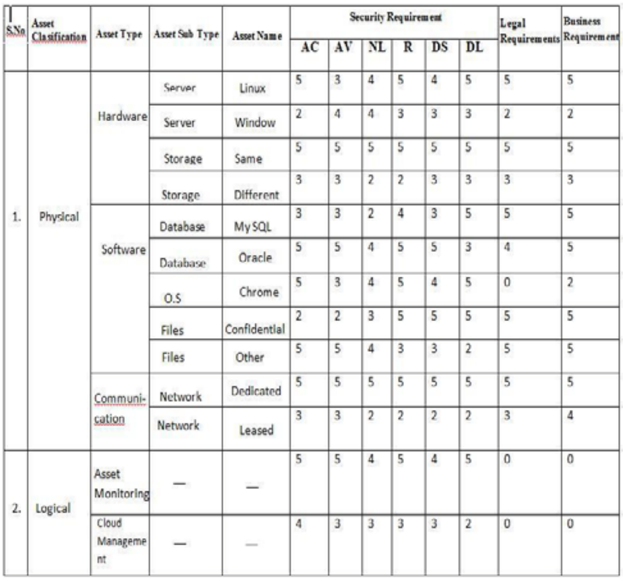
SC=max(Tv1,Tv2,.....,Tvm)

Provided there are no threats for an asset, then the SC value is assumed to be zero. (SC = 0), where SC is considered as the quantitative measure of the risk [5].

4. CASE STUDY

The current section presents a case study in which a sample implementation of the proposed methodology is shown. Consider a public cloud, say XYZ Ltd., has Physical and Logical assets as shown in the given table 1; their Security Requirements (SR), Business Requirements (BR) and Legal Requirements (LR) are also given. “Location” refers to the hardware in which the software and information assets are installed.

Table 1 Assets with their SR, LR, BR



S.No	Asset Clasification	Asset Type	Asset Sub Type	Asset Name	Security Requirement						Legal Requirements	Business Requirement
					AC	AV	NL	R	DS	DL		
1.	Physical	Hardware	Server	Linux	5	3	4	5	4	5	5	5
			Server	Window	2	4	4	3	3	3	2	2
			Storage	Same	5	5	5	5	5	5	5	5
			Storage	Different	3	3	2	2	3	3	3	3
		Software	Database	My SQL	3	3	2	4	3	5	5	5
			Database	Oracle	5	5	4	5	5	3	4	5
			O.S	Chrome	5	3	4	5	4	5	0	2
			Files	Confidential	2	2	3	5	5	5	5	5
			Files	Other	5	5	4	3	3	2	5	5
		Communi-cation	Network	Dedicated	5	5	5	5	5	5	5	5
			Network	Leased	3	3	2	2	2	2	3	4
2.	Logical	Asset Monitoring	—	—	5	5	4	5	4	5	0	0
		Cloud Manageme nt	—	—	4	3	3	3	3	2	0	0

To find out the Asset values of the assets we have to calculate it using the formula

AV=Function (SR,LR,BR),

where AV=a*SR+b*LR+c*BR

AV of Hw1 = 5

AV of Hw2 = 3

AV of Hw3 = 5

AV of Hw4 = 3

AV of Sw1 = 4

AV of Sw2 = 5

AV of Sw3 = 3

AV of Sw4 = 4

AV of Sw5 = 4

AV of Cm1 = 5

AV of Cm2 = 3

AV of Lg1 = 4

AV of Lg2 = 3

In this research work, the threats in addition to the likelihood of occurrences are found out for a group of assets which are listed in the table 2.

Table 2 Threats with their Likelihood of Occurrence

S.No	Asset Type	Threat	Loc (T)
1	Hardware	Power Faults	1
2	Hardware	Equipment Incompatibilities	2
3	Software	Corruption of Data	5
4	Software	Theft of media and documents	5
5	Communication	Link Breaks	3

In the current research work, a number of threat-vulnerability relations have been considered. The table 3 shows all the threats and vulnerabilities.

Table 3 Threats and Vulnerability Mapping

Threat Number	Threat	Vulnerability
T1	Poor Faults	Susceptibility to voltage vulnerabilities
T2	Equipment Incompatibilities	Lack of attention during installation
T3	Corruption of Data	Widely Distributed Software
T3	Corruption of Data	Applying Application program to wrong data in terms of time
T4	Theft of media or documents	Unprotected Storage
T4	Theft of media or documents	Unprotected Storage
T5	Line Breaks	Exploited Servers
T6	Coding Errors	Poor Programming

Vulnerability value Vi corresponding to threat Ti, is determined as

Vv1=sigma(sev(V1))/n=2/1=2

Vv2=sigma(sev(V2))/n=2/1=2

Vv3=sigma(sev(V3,V4))/n=4+3/2=4

Vv4=sigma(sev(V5,V6))/n=5+5/2=5

Vv5=sigma(sev(V5))/n=3/1=3

Vv6=sigma(sev(V6))/n=3/1=3

Table 4 Severity values

Vulnerability	Sev(V)
V1	2
V2	2
V3	4
V4	3
V5	5
V6	5
V7	3
V8	3

Tv2 = Roundof(log2(Vv2*Loc(T2)))
= Roundof(log2(2*2)) = 2
Tv3 = Roundof(log2(Vv3*Loc(T3)))
= Roundof(log2(4*5)) = 4
Tv4 = Roundof(log2(Vv4*Loc(T4)))
= Roundof(log2(5*5)) = 5
Tv5 = Roundof(log2(Vv5*Loc(T5)))
= Roundof(log2(3*3)) = 3
Tv6 = Roundof(log2(Vv6*Loc(T6)))
= Roundof(log2(3*3)) = 3

Threat value corresponding to threat Ti is obtained by applying Tvi = RoundOf [log2 (Vvi * Loc (Ti))] to the Loc values of threats shown in Table 2 and the vulnerability values computed in the previous section. Thus, Threat value for threat Ti is

Tv1 = Roundof(log2(Vv1*Loc(T1)))

= Roundof(log2(2*1)) = 1

Finally, the security concern values of assets are calculated using the formula SC=max(Tv1,Tv2,.....,Tvm) as follows:

Security Concern of Hardware = max(Tv1, Tv2)= max (1,2) =2

Security Concern of Software = max(Tv3, Tv4)= max (4,5) =5

Security Concern of Communication = max (Tv5)= 3

Security Concern of Logical = max (Tv6)= 3

After calculating Asset Value (AV) and Security Concern (SC), consolidated risk to the assets are obtained by the logarithm of the product of asset value AV and security concern SC. Hence, risk factor of Hw1 is

RF (Hw1) = RoundOf [log2(AV*SC)]

= Roundof[log2(5*2)]

= 3

Similarly, risk factor of Hw2 is

RF (Hw2) = RoundOf [log2(AV*SC)]

= Roundof[log2(3*2)]

= 3

Similarly, risk factor of Hw3 is

RF (Hw3) = RoundOf [log2(AV*SC)]

= Roundof[log2(5*2)]

= 3

The Risk Factor for all the assets are calculated likewise and the RF values for all the assets are shown in the table 5 along with weights for assets.

Table 5 Risk Factor

Asset	Risk Factor	Weight for each asset
HW1	3	0.8
HW2	3	0.4
HW3	3	0.5
HW4	3	0.5
SW1	4	0.5
SW2	5	0.5
SW3	4	0.8
SW4	4	0.9
SW5	4	0.6
CM1	4	0.8
CM2	3	0.5
LG1	4	0.7
LG2	3	0.7

In table 5, the weights for all the assets given by assigning a particular weight to each asset and the weight is calculated in the scale of range 0 to 1.

Weighted Average (WA) for the assets is,

WA = [(3*0.8) + (3*0.4) +(3*0.5) +(3*0.5) +(4*0.5) +(5*0.5) +(4*0.8) +(4*0.9) +(4*0.6) + (4*0.8) +(3*0.5) +(4*0.7) +(3*0.7)] / (sum of weights of all assets)

= 31.3/8.5

= 3.68

5. CONCLUSION

Risk assessment in cloud information security management remains is a crucial and challenging process. Public clouds need to adopt a systematic and well-structured process in order to assess the information security risks to its assets. Not only in computing the risk values, the risk assessment and management should also focus on identifying such contributors to this values. Through this way, the negative impacts of the contributors can be reduced leading to risk mitigation.

In the current proposed methodology, with the help of two-pronged approach, it is strived to achieve the above-said scenario. In the first phase i.e., consolidated approach, the risk values are computed and the assets are classified into specific risk zones. During the second phase, i.e., detailed approach, contributors to such risks are identified. The current research work however focused only on the consolidated approach for calculating the risk factor. An unsaid advantage is, in case, if a public cloud face any budgetary or other challenges, only a consolidated risk analysis can be performed at initial stages. When favorable conditions permit, it can go for a detailed risk analysis. There is no exact ‘value’ of risk since risk quantification in scalar values is always subjected to uncertainties due to various reasons that includes challenges in defining the likelihood and consequence severity and the mathematics to combine them.

6. FUTURE WORK

Risk assessment is long investigated and complex subject with full of uncertainties and vague in nature. So, in order to formulate new risk analysis methodologies, one can use fuzzy logic since it can also be applied to process the vaguely defined variables and those that is not possible through mathematical modelling [7]. Risks that can be segregated as ‘high’, ‘low, ‘tolerant’, either in terms of qualitative or quantitative, requires in-depth experience, expertise and excellence. Fuzzy logic can be the best in incorporating the human judgment for defining such variables and its relations. This will help define a model that closely resembles the real world. In the current research work, for the purpose of defining the risk zone, the final risk value is calculated by defining the weights to individual risks followed by the calculation of final risk value as the “weighted average” of these weighted individual risks. Further research can be carried on with a detailed approach in which an in depth analysis about the contributors of individual risks can be investigated.

7. REFERENCES

[1] Jaya Bhattacharjee , Anirban Sengupta , Chandan Mazumdar , Mridul Sankar Barik , “A Two-Phase Quantitative Methodology for Enterprise Information. Security Risk Analysis”, ACM New York, NY, USA ©2012

[2] Yu Fu ,Yanlin Qin ,Xiaoping Wu , “A Method of Information Security Risk Assessment Using Fuzzy Number Operations”,IEEE 2008

[3] Zuo Xiaodong and Liu Yi, “Some important cognitions on information security assessment”, Network & Computer Security, pp. 64-66, -XO\ 2004.

[4] Peltier, T.R. 2010.Information Security Risk Analysis.Third Edition, Auerbach Publications, USA.

[5] Mazumdar, C., et. al. 2007. Enterprise Information Security Risk Analysis: AQuantitative Methodology.In Proceedings of the National Workshop on Software Security (New Delhi, India, 2007), S.I.Ahsonand M.Mehrotra, Ed.NWSS2007. I. K. International Publishing House Pvt. Ltd., New Delhi, India, 1-12.

[6] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2011. ISO/IEC 27005:2011, Information technology –Security techniques - information security risk management. Edition 1. Switzerland.

[7] That JHM, Carr V.A proposal for construction project risk assessment using fuzzy logic[J].Construction Management and Econom ics.2000,18:491~500.

[8] KVD Kiran, LSS Reddy, M Seetharama Prasad A novel risk analysis and mitigation method in distributed banking system. International Journal of Advances in Engineering & Technology, Sept 2013