A NOVEL RISK ANALYSIS AND MITIGATION METHOD IN DISTRIBUTED BANKING SYSTEM

K. V. D. Kiran[1], L. S. S. Reddy[2], M. Seetharama Prasad[1]
[1]Department of C.S.E, K. L. University, Guntur, India
[2]Department of C.S.E, LBRCE, Vijayawada, India

ABSTRACT

The paper introduces a Fractional Reverse Banking like Distributed Banking System and the infrastructure is becoming more and more complex, and connected to large number of security issues and amount of risks to readiness assets are increasing. This is done to expand the economy by freeing up capital that can be loaned out to other parties. Most countries operate under this type of system. Hence, the process of identification, analysis, and mitigation of Information Security risks has assumed utmost importance. This quality paper grants combination of quantitative and qualitative information security risk analysis methodology for the system. The proposed methodology incorporates three approaches. Asset identifying approach identifies assets and their risk. Partitioned approach identifies risk factor for all the requirements in an asset depending on value. Exhaustive approach identifies the threat-vulnerability pair responsible for an asset associate with risk and computes a risk factor corresponding to each security property for every asset. The assets are classified into three different risk zones namely high, average and low risk zone. For utmost-risk assets, management may install high cost infrastructure to safeguard an asset; for average-risk assets, management may apply security policies, guidelines and procedures; for under risks management may invest very less for assets. In this paper a new method has been proposed to analyse and mitigate the potential problems in Distributed Banking System.

KEYWORDS: *Fractional Reverse Banking, Distributed system, Information security, Risk analysis, Risk management*

I. INTRODUCTION

The quickness and measure of facts is increasing time by time. Computer networks have become ever pervasive and have made life simple and fast, but along with that it gives rise to innumerable threats to information systems. A Fractional Reverse Banking like Distributed Banking system containing information assets, when associated to the outside world, is exposed and is vulnerable to attacks that could lead to loss of important information to assets. When you put your money into a savings account or a checking account at a bank, the bank doesn't just hit it away in a vault underground somewhere. Instead, it lends your money to other individuals and companies who need it. Thanks to the magic of fractional banking, when your bank lends your money to other people, it is actually creating money.

How Fractional Reserve Banking Works

When you put your money into a bank, the bank is required to keep a certain percentage, a fraction, of that money on reserve at the bank, but the bank can lend the rest out. For instance, if you deposit Rs.1,00,000 at the bank and the bank has a reserve requirement of 10 percent, the bank must keep Rs.10,000 of your money on reserve and can lend out the Rs.90,000.In essence, the bank has taken Rs.1,00,000 and has turned it into Rs.1,90,000 by giving you a Rs.1,00,000 credit on your deposits and then lending the additional Rs.90,000 out to someone else

Total Money Created = Initial Deposit x (1 / Reserve Requirement)

Assaults to assets are caused by threats that have the potential to exploit the vulnerabilities associated with an asset. In general, assets serve the business needs of an enterprise and any damage to these

assets in any form causes risk and is of great concern to that system. This requires an organized approach to assess and analyse information security risks and develop a right safeguard strategy. Formally, *risk* can be defined as the probable harm produced if a particular threat exploits a particular vulnerability to cause damage to an asset. Whereas specific definitions of risk might vary, a few characteristics are common to all definitions. *Risk analysis* is defined as the process of identifying security risks and determining their degree and effect on an organization. Risk analysis should be carried out prior to any application, system, project, or process going into production. For risk to exist in any circumstance, the following three conditions must be satisfied.

1. The potential for loss must exist.
2. Uncertainty with respect to the eventual outcome must be present.
3. Some choice or decision is required to deal with the uncertainty and potential for loss

A critical fact in information security is that a fact asset often ceases to be delicate after a certain period of time i.e. security requirements of an asset may change with period by period. Manual methods of assessing risks and correcting security vulnerabilities cannot keep up with the absolute number and increasing complexity of possible vulnerabilities and rising incidents of threats. These facts necessitate automation of the risk analysis process; this will allow management to quickly identify risks to their critical assets [1].

Figure 1 illustrates the three components of risk:

Potential event – an act, occurrence, or happening that alters current conditions and leads to a loss

Condition – the current set of circumstances that leads to risk

Consequence – the loss that results when a potential event occurs; the loss is measured in relation to the status quo (i.e., current state)

From the risk perspective, a condition is a passive element. It exposes an entity3 (e.g., project, system) to the loss triggered by the occurrence of an event. However, by itself, a risk condition will *not* cause an entity to suffer a loss or experience an adverse consequence; it makes the entity *vulnerable* to the effects of an event

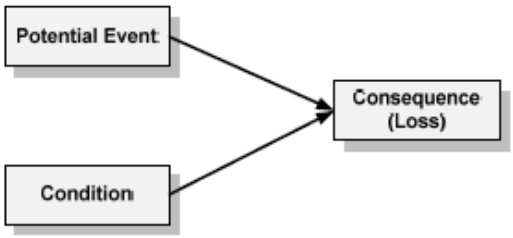

Figure1 Components of Risks

In this paper, a combined risk analysis methodology, that identifies risks associated with an asset, has been proposed. It has been enhanced based on the requirements of security principles, and validated with engineering case studies.

A brief introduction is given in section I, rest of this paper is organized as follows: Section II discusses related work. Section III describes the risk analysis process in general, and how it must be performed. Section IV details the proposed risk analysis methodology. It first describes the Asset identifying followed by consolidated approach and then the exhaustive approaches. A brief discussion follows about how both these approaches can be implemented. Finally, a case study with our conclusions is in Section V.

II. RELATED WORK

Some significant information security risk analysis methodologies are as follows:

(a) OCTAVE method the next generation of the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, which defines the essential components of a context-driven information security risk evaluation. This method allows an organization to make information-protection decisions based on risks to confidentiality, integrity, and availability of critical information technology assets. Using a three-phase approach, *OCTAVE-L* is led by a Large, interdisciplinary team of an organization's personnel who gather and analyse information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks.

To conduct *OCTAVE-L* effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself. It examines organizational and technology issues to assemble a comprehensive picture of the information security needs of a system. A team is established within an organization to perform risk analysis. The team identifies the assets that are important for the organization. Inter asset dependencies are also considered. The method is nonlinear and also iterative in nature.

(b) MEHARI

MEHARI (Method harmonized analysis risk information) methodology is a risk analysis method, designed for security. It proposes an approach for defining risk reduction measures suited to the organization objectives. *MEHARI* provides a Risk Assessment and modular components and processes them. It enhances the ability to discover vulnerabilities through audit, analyse risk situations.

MEHARI includes formulas facilitating:

• Threat identification and characterization,

• Optimal selection of corrective actions.

(c) Facilitated Risk Analysis and Assessment Process (FRAAP) is a qualitative risk assessment methodology that tries to identify risks in terms of their effects on business. It does not attempt to obtain specific numbers for threat likelihood or loss estimates. It focuses on identifying risk-prone areas and appropriate controls to mitigate them. An expert acts as the facilitator during the entire process. Since, FRAAP relies heavily on inputs from an expert; it suffers the disadvantages that most qualitative methodologies have lack of consistency in risk values.

*(d)RA2(Risk analysis):*It is a methodology for Risk analysis based on the ISO standards. For each of the steps in this process the method contains a dedicated step with report generation and printing out of the results. RA2 Information Collection Device, a component that is distributed along with the tool, can be installed anywhere in the organization as needed to collect and feedback information into the Risk Assessment process. *RA2* art of risk addresses the different steps in the process of establishing and implementing security systems, in accordance with the requirements lined out in the international standard for each of the steps in this process the tool contains a dedicated step with a report generation and printing out of the results.

Some of the automated tools for information security risk analysis are:

(a) COBRA consists of a range of risk analysis, review and security assessment tools. It includes both qualitative and quantitative approaches to risk analysis and essentially uses skilled system principles and an extensive knowledge base. Risk is computed by multiplying asset value, likelihood of occurrence of threat and severity of vulnerability [8].

(b) CORAS provides a framework for risk analysis of safety critical systems. Here, risk analysis decisions are made by UML class diagrams of each asset. It does not use any mathematical calculation and loss is estimated by multiplying Impact and Probability of occurrence of threats. Due to its simplicity, it can be easily implemented by organizations. However, it cannot provide precise risk analysis results [9].

(c) CRAMM is a comprehensive collection of tools for risk assessment. It includes tools for asset dependency modelling, business impact assessment, identification and assessment of threats and vulnerabilities, assessment of levels of risk, and identification of security controls based on results of risk assessment. CRAMM is best suited for large organizations, like government departments [10].

Table 1 presents a relative report of the risk assessment methodologies

Risk Analysis and Assessment Methods	**Elements considered**	**Follows Quantitative approach (Yes/No)**
OCTAVE	Security Parameters, Threats, Vulnerabilities	Partial
OCTAVE-L		Partial
MEHARI		Yes
FRAAP		No
COBRA		Yes
CORAS		Partial
RA2		Yes
CRAMM		Yes

III. RISK ANALYSIS PROCESS

Risk Analysis process begins with the identification of assets. Once an asset is identified, its security and business requirements such as confidentiality, integrity and availability are determined. Some assets also have legal and contractual requirements and violation of these may cause risk to an organization [1]. Threats, that can attack an asset, are also identified along with the corresponding vulnerabilities exploited by those threats. The requirements that are taken care of in the proposed methodology are as follows:

Confidentiality Requirement [*C*] refers to the protection of information from unauthorized access or accidental disclosure. It is a graded parameter and is scaled from a value of 1 to 5. Value of 1 is assigned to publicly available assets and for highly confidential asset a value of 5 is assigned.

Integrity Requirement [*I*] refers to the completeness and accuracy of information i.e. protection of information, data, or transmissions from unauthorized, uncontrolled, or accidental alterations. It is a graded parameter and is scaled from a value of 1 to 5.

Availability Requirement [*A*] ensures that information systems, and the necessary data and services, are available to authorized users for use when they are needed. It is a graded parameter and a value of 1 to 5 is assigned to an asset depending on the level of availability requirement for that asset.

Authenticity Requirement [*Au*] refers to the verification of the authenticity of either a person or of data. Data authentication is a combination of authentication and data integrity. It serves as a proof that "you are who you say you are or what you claim to be". This parameter has only two values- 0 if there is no authenticity requirement or 5 if authenticity requirement exists for an asset.

Non-Repudiation Requirement [*Nr*] demands the ability to prevent individuals or entities from denying that information, data or files were sent or received or that information or files were accessed or altered, when in fact they were. This parameter also has two values, 0 if there is no non-repudiation requirement for an asset or 5 otherwise.

Loss Impact [*Li*] defines the business requirement of an asset. An asset within an enterprise is mainly used for the proper running of its business. It is necessary to find out how business processes may be affected if there is any security breach to that asset and the estimate of loss in terms of revenues, the depreciated price of the asset, loss of customer confidence, competitive advantage or the Organization's reputation. It is a graded parameter and is scaled from a value of 1 to 5 depending on the magnitude of loss incurred to an organization.

Legal and Contractual Requirement [Lcr] is a set of statutory and contractual requirements that an organization, its trading partners, contractors and services providers have to satisfy. It is important, for example, for the control of proprietary software copying, safeguarding of organizational records and data protection. It is vital that the implementation, or absence, of security controls do not breach any statutory, criminal or civil obligations, or commercial contracts. This parameter has only two values, 0 if there is no such requirement or 5 otherwise.

Maintenance requirement [Mr] is a set of maintenance requirements and it provides services for conserving the above requirements and keeping the organization needs. . It serves as a proof that "you are who you say you are or what you claim to be for maintenance". This parameter has only two values- 0 if there is no maintenance requirement or 5 if maintenance requirement exists for an asset.

Other Institutional Risks [Or] is a set of locational requirements of an organization and it demands the ability to prevent individuals or entities from changing of location of information, data or files were sent or received which were accessed or altered, when in fact they were. This parameter also has two values, 0 if there is no location requirement for an asset or 5 otherwise.

IV. PROPOSED RISK ANALYSIS METHODOLOGY

There are two key types of risk analysis. Two distinct risk analysis approaches can be used when evaluating systems

1. Tactical risk analysis
2. Mission risk analysis

The basic goal of tactical and Mission risk analysis is to assess a system's mechanism for potential failures. Tactical risk analysis is based on the principle of system disintegration and component analysis. The first step of this approach is to decompose a system into its components. This approach

is to manage project risk and Analysts need to understand the limitations of using tactical risk analysis to evaluate interactively complex systems, which include the following: Only significant components are analyzed. Non-significant components are not examined, and interdependencies among components are not addressed [1] .Primarily, it helps in recognizing the actual risks to organizational assets. Next keeping with these goals, three different approaches have been proposed in this paper to identify risks associated with an asset.

4.1 Asset identifying approach

Finding and making value to the assets according to cause a loss of confidentiality and availability with violation of integrity. During this approach, employees must be aware of the resources which are owned by the organization, and that they need special protection. Safety requirements for this type of resource must be specified First of all, hardware and software assets are identified, because they are the most tangible assets, so they can easily be determined without much effort [6]. After these assets are identified, the information assets and firm ware assets that are processed by and are identified.
Are system assets well understood to the Customer, user, and stakeholder requirements and needs, Functional and nonfunctional requirements, Operational requirements, System growth and expansion needs, Technology maturity and how the architecture and design of assets are sufficient to meet system requirements and provide the desired operational capability and have barriers to customer/user adoption of the system asset been managed. Decides on the number of data asset levels to establish for identifying assets and prioritize the level of critical asset it contains.

4.2 Partitioned Approach

This approach computes a risk factor value for each asset. **Risk Factor**: Risk Factor [*RF*] associated with an asset is defined as a function of asset value and its security concern. This parameter identifies the risk involved with an asset and, depending on this value; an asset is determined to be at high, medium or low risk.

$$RiskFactor\ (RF) = (AV, SC)$$

where, AV is asset value and SC is security concern (defined later) of an asset.
Asset Value: Asset Value [*AV*] of an asset is defined as a function of security, business and legal and contractual requirements associated with an asset. It is a graded parameter and its value is obtained on a scale of 1 to 5.

$$AssetValue\ (AV) = (SR, BR, LR)$$

where, SR is security requirement, BR is business requirement and LR is legal requirement. These three parameters are calculated as follows

$SR = (C + I + A + Au + Nr + Mr + Or)/7,$ if $Au <> 0, Mr <> 0;$ (1)

$BR = Li$ (2)

$LR = Lcr + Or$ (3)

Asset Value [*AV*] is calculated as

$AV = \alpha*SR + \beta*LR + €*BR,\ \alpha+\beta+€ = 1$ (4)

Here, α,β,€ are relative weights that are assigned to security, business, and legal requirements, respectively. It may be noted that individual components of SR have been assigned equal weights. However, if needed, these components may be assigned relative weights based on priorities of an enterprise [5]. For example, a military organization may choose to attach greater importance to confidentiality requirements as compared to the other security parameters; hence, weights may be customized accordingly. Since security requirement is the major determinant for computing security risk, higher weight should be assigned to it. Business requirement and legal and contractual requirement for an asset depend on the type of organization, its assets and how they are used. Thus, the weights for calculating asset value *AV* can be adjusted depending on the specific requirements of an organization (or on the business that an organization conducts).
For instance, considering $\alpha = 0.5$, $\beta = 0.25$, and $€ = 0.25$

$AV = 0.5*SR + 0.25*LR + 0.25*BR$ (5)

SR=max(all the requirements)

Security Concern: Security Concern [*SC*] for an asset is defined as a function of threats and vulnerabilities associated with an asset. Threats have many-to-many relation with vulnerabilities.

Security concern value is obtained by identifying the vulnerabilities that can be exploited by a threat. It is a graded parameter and its value is obtained on a scale of 1 to 5.
SecurityConcern (*SC*) = π(*Tv, Vv)* where *T* is threat value and *V is the vulnerability value* To compute security concern [*SC*] of an asset *A*, a list of threats associated with that asset are obtained along with their Likelihood of Occurrence [*Loc*(*T*)] values. [Loc defines the likelihood of occurrence of a threat associated with an asset according to available statistics or past experience and produces a three-scale value i.e. low/medium/high, converted to numerical value as 1/3/5, respectively] Then, for each threat *Ti* a list of vulnerabilities [*Vi*1, *Vi*2 , . . . , *Vin*] which can be exploited by that threat are identified along with their Severity

$$Vvi \equiv \left(\sum Sev(Vj)\right)/n,\ j = 1,2...n \quad \text{if } n>0 \qquad (6)$$

= 1 if n=0

$$T_{vi}=\text{RoundOf}[\log_2(V_{vi}*\text{Loc}(T_i))] \qquad (7)$$

4.3 Exhaustive approach

This enables management to take specific actions depending on the threat- vulnerability pair causing risk. The process starts by first identifying those security parameters having a value greater than 2. Then, it identifies threats that can breach a particular security requirement, and the vulnerabilities exploited by those threats. Say for an asset *A*, the confidentiality requirement is high, i.e. confidentiality value is 4. The next step is to identify the threats that can breach confidentiality of the asset. Let the threats identified be T_1, T_2,,T_m. For each threat *Ti*, the corresponding vulnerabilities exploited are obtained. For threat *Ti*, let the vulnerabilities exploited be V_{i1} , V_{i2} ,..., V_{in}. For each vulnerability V_{ij} A risk value is computed [14].

$$RV(V_{ij})=\text{RoundOf}(\log_2(\text{ValueOf}(\text{SecurityRequirement})*\log_2(\text{Loc}(T_j)*\text{Sev}(V_{ij}))) \qquad (8)$$

In this approach, risks to an asset are identified as a 4-tuple as shown below
Risk = <SecurityRequirement, Threat(*Ti*), *Vulnerability*(*Vij),Risk Value)* *(9)*

High Risk Assets: An asset is at high risk if there is at least one risk (identified as a 4-tuple) having risk value>= 4.) that cause each of these risks, are identified. Depending on risk value, assets are classified as follows:

Medium Risk Assets: An asset is at medium risk if there is at least one risk having risk value of 3 and no risks with risk value >=4.

Low Risk Assets: An asset is at low risk if all of its risks have risk value <=2. Application of this methodology classifies a set of assets into three risk zones. The high-risk zone is *danger zone*. Management should take immediate steps to mitigate such risks by applying appropriate security infrastructure to reduce threats and/or strict procedures to plug the vulnerabilities exploited. The medium risk zone is a *warning zone* and management should control it by using some security tools, and applying some policies and guidelines, wherever required. Management may not invest anything for assets at low risk (indicating a *safe zone*).

V. CASE STUDY

This section presents a case study showing a sample implementation of the proposed methodology. A Fractional Reverse Banking and Distributed systems has Hardware and software assets and their Security, Business, and Legal requirements are shown in the following table

Table 2 presents with their assets and requirements

Asset	Asset Type	SR							LR	BR
		C	I	A	Au	Nr	Mr	O r		
Hw1	Server unit	5	5	5	5	5	5	5	5	5

Hw2	Data base Unit	4	4	0	5	5	0	0	0	3
Hw3	Printer	2	2	4	0	0	5	5	0	3
Hw4	MotherBoard	2	4	4	0	5	5	5	0	0
Hw5	RAM	4	4	4	0	0	0	0	0	0
Hw6	Hard Disk	2	4	4	0	5	5	5	0	3
Sw1	Funding Processing	5	4	2	0	0	0	0	5	5
Sw2	Funds accounting	5	5	5	0	5	5	5	5	5
Sw3	Funds reporting	2	2	0	5	5	0	0	5	5
Sw4	Operating Systems-win7	5	5	5	0	0	5	5	5	5
Sw5	Enterprise software	5	5	5	0	5	5	5	5	5
Sw6	Write and read File	5	5	5	5	5	5	0	5	5
Sw7	Data File	5	5	5	5	5	5	5	5	5

AV of hw1=0.5*5+0.25*5+0.25*5=5
AV of hw2=0.5*5+0.25*0+0.25*3=3.25
AV of hw3=0.5*5+0.25*0+0.25*3=3.25
AV of hw4=0.5*5+0.25*0+0.25*0=2.5
AV of hw5=0.5*4+0.25*0+0.25*0=2
AV of hw6=0.5*5+0.25*5+0.25*5=5
AV of sw1=0.5*5+0.25*5+0.25*5=5
AV of sw2=0.5*5+0.25*5+0.25*5=5
AV of sw3=0.5*5+0.25*5+0.25*5=5
AV of sw4=0.5*5+0.25*5+0.25*5=5
AV of sw5=0.5*5+0.25*5+0.25*5=5
AV of sw6=0.5*5+0.25*5+0.25*5=5
AV of sw7=0.5*5+0.25*5+0.25*5=5

Here threats with their occurrence value for the group of assets

Table 3 presents value of occurrence are recognized for a group of assets out of 5

S.No	Asset type	Threat(T)	Loc(T)
1	Hardware	Loss of power supply	3
2	Software	Corruption of data	4
3	Software	Malfunctioning of online accounts	4
4	Hardware	Debit/Credit Card Usage	4

Table 4 presents mapping between the threat and vulnerability values out of 5

TID	Threat(T)	Vulnerability(V)	Sev
T_1	Loss of power supply	Susceptibility of voltage variations-V_1	2
T_2	Corruption of data	Widely distributed data-V_2	3
T_3	Malfunctioning of online accounts	Unprotected storage and wrongly used ways ,Lack of care-V_3	4
T_4	Debit/Credit Card Mis Usage	Lack of care at the person-V_4	4

$$Vvi \equiv \left(\sum Sev(Vj)\right)/\, n,\ j = 1,2...n \quad \text{if } n>0$$

Now

$n=1, V_{v1}=2/1=2$
$n=2, V_{v2}=2+3/2=2.5$
$n=3, V_{v3}=2+3+4/3=3$
$n=4, V_{v4}=2+3+4+4/4=3.5$

Thus threat value for T_1 is

$T_{v1}=\text{RoundOf}(\log_2 (V_{v1}*\text{Loc}(T_1))$
$=\text{RoundOf}(\log_2 (2*3)=2.07=2$

$T_{v2}=\text{RoundOf}(\log_2 (V_{v2}*\text{Loc}(T_2))$
$=\text{RoundOf}(\log_2 (3*4)=4.39=4$

$T_{v3}=\text{RoundOf}(\log_2 (V_{v3}*\text{Loc}(T_3))$
$=\text{RoundOf}(\log_2 (3*3)=3.29=3$

$T_{v1}=\text{RoundOf}(\log_2 (V_{v1}*\text{Loc}(T_1))$
$=\text{RoundOf}(\log_2 (4*3)=4.14=4$

Security concern value of assets are

$SC(Hw1)=A=\max(T_{v1},T_{v2})=2$
$SC(Hw2)=B=\max(T_{v1},T_{v4})=3$
$SC(Sw1)=C=\max(T_{v2},T_{v3})=3$
$SC(Sw2)=D=\max(T_{v2},T_{v3})=3$

Some of the Risk Values are calculated as follows as required

$RV(V_1)$ of Hw1
$=\text{RoundOf}(\log_2 (\text{Value of (A)} * (\log_2 (\text{Loc}(T_1)*\text{Sev}(v_1))))$
$=\text{RoundOf}(2*(\log_2 (3*2)))=(2*2)=4$

$RV(V_2)$ of Hw2
$=\text{RoundOf}(\log_2 (\text{Value of (B)} * (\log_2 (\text{Loc}(T_2)*\text{Sev}(v_2))))$
$=\text{RoundOf}(3*(\log_2 (3*3)))=(3*2)=6$

$RV(V_3)$ of Sw1
$=\text{RoundOf}(\log_2 (\text{Value of (C)} * (\log_2 (\text{Loc}(T_3)*\text{Sev}(v_3))))$
$=\text{RoundOf}(3*(\log_2 (4*4)))=(3*3)=9$

$RV(V_4)$ of Sw2
$=\text{RoundOf}(\log_2 (\text{Value of (D)} * (\log_2 (\text{Loc}(T_4)*\text{Sev}(v_4))))$
$=\text{RoundOf}(3*(\log_2 (4*4)))=(3*3)=9$

Risk = <SecurityRequirement, Threat(Ti), Vulnerability(Vij),Risk Value)
Risk of Hw1(2,2,2,4)
Risk of Hw2(3,3,4,6)
Risk of Sw1(3,4,3,9)
Risk of Sw2(3,4,4,9)

These are all high risk assets

VI. CONCLUSIONS & FUTURE WORK

Risk assessment is a vital component in the wheel of Distributed Banking System in Information Security Management. It is important for banking to adopt a systematic and well-structured process

for assessing information security risks to its assets. In addition to computing risk values, risk assessment should also endeavor to identify the significant contributors to these values and reduces risk. The uniqueness of the proposed methodology is that it strives to achieve this by using these approaches. The first phase, namely Asset identifying approach, computes risk values, and classifies assets into specific risk zones. While, the second phase, namely Partitioned approach identifies risk factor for all the requirements in an asset depending on value. And the third approach Exhaustive approach identifies the threat-vulnerability pair responsible for an asset associate with risk and computes a risk factor corresponding to each security property for every asset. There is no such thing as an "exact" value of risk. Quantification of risk in scalar values is subject to uncertainties for several reasons including difficulties in defining the likelihood and consequence severity, and the mathematics for combining them. As risk in scalar values and is subjected to uncertainties for several reasons including difficulties in defining the likelihood and consequence severity, and the mathematics for combining them. As has been stated above, assessment of risk is a complex subject shrouded in uncertainty and vagueness. The advantage of using fuzzy logic is that it enables processing of vaguely defined variables, and those that cannot be modeled by mathematical relations. Risk can be interpreted as "high", "low" or "tolerable"- such assessment, whether qualitative or quantitative, requires analyst's judgment, expert knowledge and experience. This will help define a model that closely resembles the real world.

REFERENCES

[1] Jaya Bhattacharjee ,Centre for Distributed Computing ,Jadavpur University 2012 ,A Two-Phase Quantitative
Methodology for Enterprise Information Security Risk Analysis,In ACM 978-1-4503-1185-4/12/09.

[2] A. Shameli-Sendi and M. Dagenais, "Real Time Intrusion Prediction based on improving the priority of alerts with Hidden Markov Model," Journal of Networks, 2012.

[3] G. N. Matni and M. Dagenais, "Operating system level trace analysis for automated problem identification," The
Open Cybernetics and Systemics Journal, vol. 5, 2011,pp. 45-52.

[4] Debar, "A service dependency model for cost sensitive intrusion response," Proceedings of the 15th European Conference on Research in Computer Security, pp. 626-642, 2010.

[5] A. Shameli-Sendi, M. Jabbarifar, M. Shajari and M. Dagenais, "FEMRA: Fuzzy expert model for risk assessment," Proceedings of the Fifth International Conference on Internet Monitoring and Protection, pp.48-53, Barcelona, Spain, 2010.

[6] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2009. ISO/IEC 31010:2009, Risk management — Risk assessment techniques. Edition 1. Switzerland

[7] Alberts, C. and Dorofee, A. 2009. An Introduction to the OCTAVE Method. Software Engineering Institute, Carnegie Mellon University, USA- http://www.cert.org/octave/methodintro.html

[8] COBRA: Introduction to Security Risk Analysis - http://www.security-risk-analysis.com/

[9] CORAS: A platform for risk analysis of security critical systems - http://www2.nr.no/coras/

[10] CRAMM: Information Security Risk Assessment Toolkit http://www.cramm.com

[11] enisa: European Network and Information Security Agency - http://rm-inv.enisa.europa.eu/rm_ra_methods.html

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

[13] Sengupta, A., et. al. 2005. A Web-Enabled Enterprise Security Management Framework Based on a Unified Model of Enterprise Information System Security: (An Ongoing Project Report). In Proceedings of First International Conference on Information Systems Security (Kolkata, India, 2005). ICISS 2005. LNCS 3803, Heidelberg, Germany, 328– 331.

[14] The International Organization for Standardization, The International Electrotechnical Commission (ISO/IEC). 2005. ISO/IEC 27002:2005, Information technology – Security techniques - Code of practice for information security management. Edition 1. Switzerland.

[15] Zadeh, L.A. 1996. Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by L. A. Zadeh. In Advances in Fuzzy Systems: Applications and Theory Vol. 6, G. J. Klirand B. Yuan, Ed. World Scientific, Singapore.

AUTHORS

Venkata Durga Kiran.Kasula did M.Tech(CSE) from Archarya Nagarjuna University and pursuing Ph.D in risk assessment and security in Distributed systems from the same university. He has published thirteen international journal papers and four international conferences. He is presently working as an assistant Professor at KL University, Vijayawada.

L.S.S. Reddy did his Ph.D in Computer Science Engineering from **BITS, Pilani**, an efficient and eminent academician. He is an outstanding administrator, a prolific researcher and a forward looking educationist. He had 50 publications in reputed international journals and several paper presentations in international conferences. 9 of his Research Scholars were awarded Ph.D under his Guidance from various Universities. His Research interest areas are Parallel Processing, Software Engineering and Computer Architecture

M. Seetharama Prasad, did his B.E(cse) from University of Mysore , M.E(cse) from Vinayaka Missions University and obtained his Ph.D in Digital Image Processing in 2012 from Chandra Mohan Jha University. He has published fourteen research papers in various international journals, presently working as Professor in KLU, Vijayawada. He has got 13 years of academic and 7 years of industrial experience. His research interests includes DIP, Information systems security.

.