ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

A Decision Support System for Assessing risk using Halstead approach and Principal Component Analysis

B. Chaitanya Krishna*, Kodukula Subrahmanyam
Department of Computer Science and Engineering, KL University, Andhra Pradesh, India.
***Corresponding author: E-Mail: chaitu2502@kluniversity.in, Mob: 9390059251.**

ABSTRACT

Software Risk management is a process that helps to analyze a risk that have a concern about the proper functioning of the project, and find out all the possible ways that can reduce the probability of occurrence of the risk in an information systems. Identification of a risk can be done by using a Survey instrument method and source code analysis. Risk management in general prepares a procedure which can be implemented only in case of threat occurrence. Basically risks are categorized as Project risks, Technical risks, Business risks, Known risks, Predictable risks, and Unpredictable risks. Few principles like global perspective, forward looking view, integrated management are followed for risk assessment. Risk is not some flaw in the project but it is an occurrence of unforeseen event that impact the quality. Risk can never be eliminated but can be reduced to maximum extent. In this paper we proposed a model to identify the risk in effectively by using Halstead method to postmortem the product development and PCA method to extract risks from huge data sets.

KEY WORKDS: Risk, Source code, Technical risks, business risk, known risk, Predictable risks.

1. INTRODUCTION

Risk is defined as a virtual and event that limits the ability of an organization to achieve its mission or Occurrence of the event is unpredictable. Example Loss of data in a system due to system sudden demands to close the organization or Risk is a potential event that may negatively impact on the ability on the project undertaken or in other terms Risk is defined as the international interaction with uncertainty.

When a risk is identified necessary steps are to be taken so that the impact of the risk may not cause any further remark on the project or task. But, Risk cannot be eliminated completely rather its effect can be reduced to some extent. Primarily Risk must be calculated, an equation helps to know to what extent the risk have occurred. Risk is identified by using probability of hazard and degree of vulnerability. Probability of Hazard is any type of source that causes potential damage and probability of hazard defines the extent up to which a source that is present may cause damage to the software project being developed. Degree of Vulnerability is a degree to which a system or an environment may be susceptible to be in position of harm.

A project is always targeted with many risks. One of the main tasks of the project manager is to manage these risks and prevent them so that these risks do not ruin the development or changes that are going to be made. Risks in a project are broadly classified into the following types: Scope Risk, Scheduling Risk, and Resource Risk. Scope Risk is When a project is be initialized the scope should also be defined i.e what may be the requirements, the end result of the project, Objectives. All these cannot be done perfectly in the primary step. Changes may occur in the process of progress in the project this changes are remarked as Scope risk i.e the inability to define a perfect scope for the project. Schedule Risk is when a project is started timelines are to be declared and they must exhibit the progress of the project to the customer, this is a critical task for the project managers. Making delay in the submission of report about the progress is termed as schedule Risk like relying on external party for some part of project may be delayed as they don't consider the scope of schedule, Hardware delay, delay in taking decision, and delay in accepting an idea to proceed. Minimization of the schedule Risk can be done by cutting down the project into small components so that allocated time frame for each component becomes low and it becomes easy to finish a task at stipulated time period. Commonly suggested caution is that if any of the team members are unable to give the estimated time for a task or giving some unrealistic estimated time re-defines the work loops. Resource Risk is the base resources for any project are People and Funds. In case the people appointed for the project are unskilled to perform the task its risk is at very high level technically termed as ill-planned resource. Minimization of the Resource Risk can be done by estimating the project cost accurately, allocating a budget that meets the costs required, not expecting above the standards of the employed staff. Regular monitoring on the project development gives a large impact on minimizing the Resource Risk.

Risk Management is a process of thinking systematically about all the possible risk or disasters that may have a probability to occur and setting up written procedures that will try to reduce the impact or avoid the impact or cope with the impact of risk. It is a process to identify where the risk has occurred and setting up strategy's to deal with it by controlling and making evaluation to the true level of risk in a realistic manner. Apart from different kinds of risks that occur in any organization the process of management followed in many companies is the same. Risk management cycle followed in different companies is as follows this cycle defines four steps for risk management is Risk Assessment, Risk Evaluation, Risk Management, Risk Measure. Risk Assessment is the stage of the project is reviewed and the particular part of project where risks have occurred is assessed. Risk Evaluation helps to evaluate

the entire module where the risks have occurred. Risk Management supports to rectify the risk by managing the risk. Risk Measure evaluation & management how much a system functions accurately is measured.

2. METHOD AND METHODOLOGY

Purpose of Risk management:

Anticipate and identify risk: To perform any action on the risk occurred firstly the module where the risk has occurred must be identified.

Minimize the impact or damage or loss: After identifying the risk necessary steps are to be taken so that the damage that can be caused to the project can be minimized so that risk cannot abort the entire functionality.

Reduce the Probability: Risk cannot be completely reduced but by taking some necessary steps the risk can be reduced so that the risk occurred becomes negligible.

Monitor risk areas for early detection: After completion of every module it must be monitored so that risk can be identified at an early stage and by this process impact of risk can be reduced. If risk is monitored at the end it becomes very critical to rectify every risk.

Ensure management awareness of risk: All the project members must have awareness of the possible risk and how to manage them so that risk identification is an easy task to be done by all the project members.

There are several principles, guidelines and methods that are set for the process of risk management. Although many are proposed the standard format is mostly followed in many companies As per ISO 31000 (Risk Management-Principles and guidelines on implementation).

Risk management process consists of the following steps establishing the content, Identification, Assessment.

Establishing the context: Establishing the context signifies that all the possible risks are identified and possible ramifications are analyzed thoroughly.

Various strategies are considered and decisions are made to deal with break-up of various activities in this stage as follows:

- Identification of a risk in one particular domain
- Planning out the entire management process
- Mapping the manifestations of the risk, identification of objectives
- Outlining a framework
- Designing an analysis of risk involved at each stage
- Deciding upon the risk solutions

Identification: After the context being established successfully the next step is to identify the threats or potential risk. The identification may be at a) Level of risk or b) problem level.

Assessment: It means that the effect rather than the risk is analyzed. Eg: Problem risk examples are a) Drop in production b) Threat of losing money and life's the methods that are followed for risk identification varies from one organization to other.

Many organizations and company's follow different approaches to solve or handle risks that are occurred in a project mostly used methods are broadly two categories they are Qualitative analysis and Quantitative Analysis Qualitative is a descriptive way of approach while quantitative is a descriptive way of approach. Peculiarly they are a) Markov Analysis b) Fuzzy c) Event Tree analysis Logic. Where Markov Analysis is a Quantitative approach and Fuzzy logic is a Qualitative analysis.

Some common methods of risk identification are:

Taxonomy based Risk Identification: The possible risk sources are broke down, hence taxonomy. A questionnaire is made best on existent knowledge; the answers to the questions are the risk.

Objective based Risk Identification: An organization or any business activity has a certain objective/s. Any activity that is deemed an obstacle in the achievement of the same is perceived as risk.

Scenario based Risk Identification: Here various scenarios, which may be alternative ways to achieve an objective, are created. If an undesired scenario is created, a threat is perceived with the same

Common Risk Check: There are certain risks that are common to an industry. Each risk is listed and checked on time.

Markov Analysis: It is a sequence of possible events and each one depends on the previous state behavior.

Risk Assessment: Risk played key role in risk management methodology. They are used to discover the threats associated with the IT system through its software development life cycle. The output of this is useful to detect the threats in the project. The risk assessment methodology encompasses with nine primary steps they are:

a) Characterization of system, **b)** Identification of threat, c) Identification of Vulnerability, d) Control of analysis, e) Determination of Likelihood, f) Impact analysis, g) Determination of risk, h) Control Recommendations, i) Documenting the results.

Proposed Method: In evaluating risks for an Information Health System framework, the initial step is to characterize the extent of the exertion. In this step, the limits of the IT framework are distinguished, alongside with the assets and the data that constitute the framework. Portraying an Information System (Health System) framework sets up the extent of the risk appraisal exertion, outlines the operational approval (or accreditation) limits. The individual or persons who lead the risk evaluation should hence first gather related data about framework, usually classified as Hardware, Software, System interfaces, Data and information, System mission, System and data criticality, System and data sensitivity. In proposed model we use a systematic approach to evaluate large-scale risk through acquisition process, Halsted approach, and Principal of component analysis.

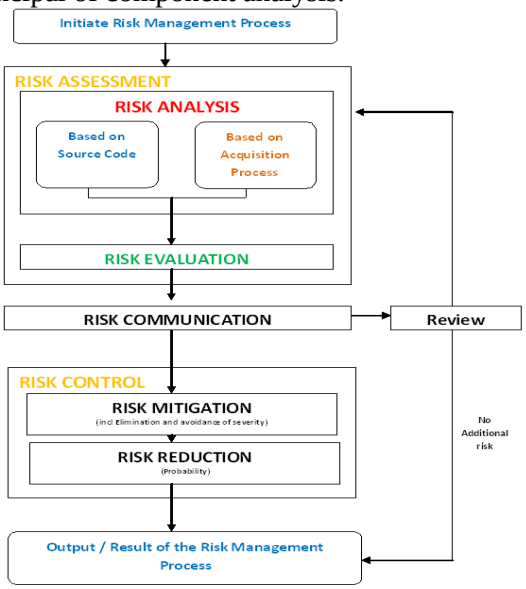

Fig.1. Architecture of Proposed System

The Halstead Approach: Halstead approach measures are software metrics introduced by Maurice Howard Halstead as part of his treatise on establishing an empirical science of software development. Halstead made the observation that metrics of the software should reflect the implementation or expression of algorithms in different languages, but be independent of their execution on a specific platform. These metrics are therefore computed statically from the source code. Halstead's goal was to identify measurable properties of software, and the relations between them. This is similar to the identification of measurable properties of matter (Program length, Volume, Difficulty, Effort, errors, delivered bugs) and the relationships between them (analogous to the source equation).

Principal Component Analysis: For a collection of returns series of the source code, the number of principal components (PCs) to be retained for further analysis is determined by the correlation structure of the data. If the data are all highly mutually correlated, one or two PCs will suffice to explain a large fraction of total data variation. On the other hand, if the data are either uncorrelated or only correlated across subgroups, more PCs need to be retained. By studying the fraction of the variance that is explained by successive PCs, one may obtain an estimate of the effective dimensionality of the data. Since PCA is sensitive to the units of measurement of the data, we report our results both for the "raw" and for "standardized" (zero mean and unit variance) series. Standardizations is found to have little qualitative effect except when groups of series with differing group variances, such as exchange rates and interest rates, are analyzed.

In Proposed model we gather information two ways, evaluated each one after combined the result and finalized the different types of Risks and their impacts.

Information gathering techniques are; a) Through acquisition process (Questioner), b) Based on source code analysis.

Questioner: For collecting the information relating to risk assessment a person can develop a questioner considering the management and operating controls used for the IT systems. The questions should belong to all aspects satisfying the technical and non-technical management person who are designing or support the IT system.

Through Source Code analysis process: In this process we are taking the skeleton of the source code using Halsted approach (i.e. entire code is divided into the tokens) based on the tokens we can identify dependability of the modules using Principle Component Analysis and identify the inheritance properties of the application and finalized the different types of risks and their impact.

Procedure of the proposed Model:

Step1: Entire application is divided into four modules (Technology, Organization, People, and Environment)
Step2: Each Module programs read as input individually and consider acquisition process
Step 3: Estimate the each Module defect.

Step 4: Estimate the induced risks and inherent risks.
Step 5: Based on the Step3 and Step4 find out the Risk factor
Step 6: Repeat the above step for all modules in the system
Step7: Estimate the individual program structure risk factor, calculate the average system risk factor.
Step 8: Based on PCA System 'safety' value and system risk factor estimated actual risk.
Step 9: Based on the risk value to display which module have the risk is display and give suggestions to develop healthy system
Step 10: For efficiency proposed model result Risk value compare with Markov analysis result for Electronic Health application.

3. RESULTS AND DISCUSSION

Based on the proposed model I consider basic Health automation system. Why I considered Health automation system is if health automation developed risk free product then only is use and considered their results otherwise the impact is one human life so I consider proposed model to health automation System. Here in this paper I compared proposed model with Markov analysis and Even tree analysis models.

In the following circumstances the proposed model is very efficient and it gives more accuracy results compare to the Markov analysis and Even tree analysis.

- The lack of dependence on functional mechanisms reduces their appeal to the functionally orientated ecologist.
- The disclosure is done entirely based on trust and an authentication mechanism is proposed in order to keep the info safe. Encryption is performed with in the circles in order to keep the VIP records safe.
- Due to the globalization of info government can easily track and conduct a research on the prevalent diseases and they can take measures accordingly
- Hierarchical diseases can be treated easily by getting access to their ancestor's info that is how they responded and what are symptoms they suffered with.
- Unique token numbers is assigned to the patients and they can use this number any where they would like to take treatment.

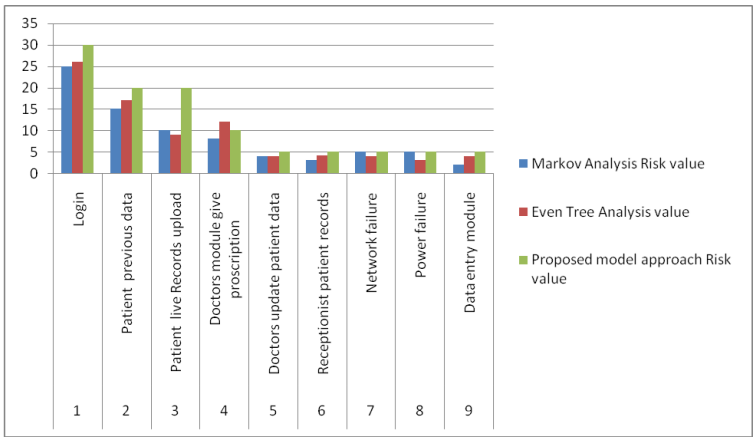

Fig.2.Comparisons of various other Risk Assessment models with the proposed system

4. CONCLUSION

The role of Information technology plays a crucial role in connecting and controlling disparate systems in a transparent fashion. Furthermore, IT analytics can handle the necessary risk analysis, mediation and compliance to meet the industry mandate. There are many lessons that can be learned from the health and pharmacy industries adoption of a risk methodology. The first is that risk analysis is going to play an ever greater role in meeting compliance standards of regulatory agencies. The logical outcome is that risk methodologies will assume a more active part in process modeling.

REFERENCES

Alavi M, and Leidner DE, Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, MIS Quarterly, 25 (1), 2001, 107-136.

Beynon-Davis TP, Information Systems `Failure' and Risk Assesment: The Case of London Ambulance Service Computer Aided Despatch Systemo Proc., Third European Conf. Information Systems, 1995, 153-170.

Boehm UBW, Software Risk Management, IEEE CS Press, 1989.

Davis GB, Strategies for Information Requirements Determination, IBM Systems J., 21 (1), 1982, 4-30.

Desmulliez M, and Topham D, 3D-Mintegration: the design and manufacture of 3D miniaturized integrated products, Proc. 2nd ESTC, London, 2008, 737-741.

Ding K, Zhou Z, and Liu C, Latin hypercube sampling used in the calculation of fracture probability, Reliability Engineering and System Safety, 59, 1998, 239-242.

Scott JE, and Vessey I, Managing Risks in Enterprise Systems Implementations, Communications of the ACM, 45 (4), 2002, 74-82.