*International Journal of Engineering & Technology*, 7 (2.23) (2018) 510-515

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# A Framework for Enhanced Tropos Goal-Driven Risk Assessment in Requirements Engineering

**ShankarNayak Bhkukya[1]*, Dr.Suresh Pabboju[2],**

*[1]Ph.D. Research Scholar (External) Faculty of Computer Science and Engineering*
*OSMANIA UNIVERSITY, Hyderabad, Telangana, India*
*bsnaik546@gmail.com*
*[2]Professor,CBIT, Osmania University, Hyderabad, Telangana State,India*
**Corresponding Author E-Mail: plpsuresh@gmail.com*

**Abstract**

Every process model used by software industry has different phases including requirement engineering. This is the crucial phase as it is preceded by other phases and provides valuable inputs to the design phase. Risk assessment made in this phase can help avoid wastage of time, effort, cost and budget overruns and even missed delivery deadlines. Traditionally risks are analyzed in terms of technical aspects like failures in the working system, unavailability of certain services, and fault intolerances to mention few. The identified risks are used to have countermeasures. However, it causes the life cycle of the system to be repeated right from the requirements engineering. On the contrary, risk analysis in the requirements engineering phase can prove fact that a stitch in time saves nine. Therefore early detection of risks in the system can help improve efficiency of software development process. Goal-oriented risk assessment has thus gained popularity as it is done in the requirements analysis phase. Stakeholder interests are considered to analyze risks and provide countermeasures to leverage quality of the system being developed. In this paper, a formal framework pertaining to Tropos goal modelling is enhanced with quantitative reasoning technique coupled with qualitative ones. Towards this end we used a conceptual framework with three layer such as asset layer, event layer and treatment layer. We used a case study project named Loan Origination Process (LOP) to evaluate the proposed framework. Our framework supports probability of satisfaction (SAT) and denial (DEN) values in addition to supporting qualitative values. The Goal-Reasoning tool is extended to have the proposed quantitative solution for risk analysis in requirements engineering. The tool performs risk analysis and produces different alternative solutions with weights that enable software engineers or domain experts to choose best solution in terms of cost and risk. The results revealed the performance improvement and utility when compared with an existing goal-driven risk assessment approach.

***Keywords***: *Requirements analysis, Tropos goal-driven risk assessment, goal-oriented requirements engineering*

## 1. Introduction

Requirements engineering (RE) is part of software development life cycle and software engineering (SE). In this phase it is crucial to analyze and understand the completeness of the requirements elicited. However, it is one of the most challenging and task among difficult SE challenges. When requirements are not analyzed to discover risk, it leads to missing requirements [6]. Many risk analysis approaches came into existence. Additionally, many goal-oriented methodologies such as Tropos [35], GBRAM [36], i* [37] and KAOS [38] are being used in the world. Tropos is the methodology used to develop software with goal-oriented approach. According to this goals of stakeholders are analyzed to determine the better combination of goals to achieve desired solution.

The Tropos goal model is extended in [16] for better approach with three layers namely goals, events and treatments. As shown in Figure 1 these layers are used to have a goal-risk model. The gaols have associated events. Events are nothing but risk occurrences that need appropriate response in the form of treatments. There is cost involved in the treatments as well. For instance processing loan application is the goal which needs an event to have a valid identity proof but customer provided fake one that leads to risk. To handle such risk, there might be countermeasure which is known as treatment which incurs cost again. This phenomenon is presented with a real world case study known as Loan Originating Process collected from banking domain as illustrated in section 4. We proposed an enhanced Tropos goal risk model to support probabilistic values to SAT and DEN attributes instead of using Full (F), Partial (P) and None (N). The quantitative analysis of these attributes provides more permutations and combinations in the solution space. That is the objective of this paper. Out contributions of the paper are as follows.

- We proposed an enhanced goal-risk model that uses Tropos Goal Risk model with three layers namely goal layer, event layer and treatment layer. The proposed methodology makes use of probabilistic values for SAT and DEN attributes to have better combinations with low risk.
- We proposed an algorithm known as Quantitative Risk Analysis (QRA) that takes goal risk model and acceptable risk as input and produce a set of optimized solutions from which stakeholders can choose best solution. The goal risk model used as input encapsulates all goals, events and treatments along with the relations and AND/OR compositions at the top level of layers.
- We built a prototype application that is domain independent and supports case studies collected from different software applications in terms of requirements. Since it deals with RE

to analyze risk and provide goal based risk analysis the prototype helps finding optimized candidates from which best one can be chosen. Due to quantitative approach the optimized candidates can have further combinations based on risk to choose most optimal solution.

The remainder of the paper is structured as follows. Section 2 provides review of literature. Section 3 presents problem definition. Section 4 presents LOP dataset used. It is the real cases study considered for empirical study. Section 5 presents the proposed methodology. Section 6 provides prototype implementation and experimental results. Section 7 concludes the paper besides providing directions for future enhancements.

## 2. Related Work

This section provides review of literature on risk analysis in requirements engineering. Especially the research on Tropos goal models is given importance. Morandini et al [14] explored Tropos SE methodology. Another natural extension to Tropos SE is found in [25]. Morandi et al. [15] proposed Tropos4AS which is meant for adaptive systems to have requirements engineering. Matulevicius et al. [1] focused on extending a goal-oriented language known a Secure Tropos in order to model security risks in requirements engineering phase. They enhanced Tropos syntax and semantics to improve its utility. Ahmed et al. [2] focused on a model known as Information Systems Security Risk Management (ISSRM) and proposed a methodology to convert misuse cases into secure Tropos using model transformation. In [3] investigation is made to understand and achieve alignment between enterprise models and goal models. Their methodology has three phases known as elicitation phase, harmonization phase and alignment phase. Sharma and Kumar [4] proposed goal oriented risk analysis model that could prioritise risk to make decisions early in the life cycle of software development. They proposed a methodology based on Tropos goal-risk model. Sharma and Kumar [5] also studied enhanced Tropos goal risk model to obtain optimized candidate solutions in requirements engineering phase.

Cailliau and Lamsweerde [6] assessed risks associated with requirements by analyzing probabilistic goals and possible obstacles. They focused on both risk analysis and obstacle analysis by presenting a probabilistic framework. They analyzed the severity of goals and obstacles. As they used ambulance dispatching system, they considered obstacles as well. Similar kind of work is made in [32]. Munante et al. [7] on the other hand explored risk analysis in the context of Model Driven Engineering (MDE). Beckers et al. [8] proposed a conceptual framework for security requirements engineering and risk analysis compatible with ISO 27001 and analyzed many security requirements, documentation and techniques. Nhlabatsi et al. [9] make a review of evolving software systems in terms of security requirements engineering. Li and Horkoff [10] studied security requirements of socio-technical systems. They employed a holistic approach with three-layered security framework.

Souag et al. [11] studied domain ontologies and requirements for analysis of the requirements by using heuristic production rules. Data semantics and ontology approaches in modelling can be found in [19]. Onwubiko [12] proposed a goal-oriented risk analysis model that leverages the usage of system requirements and situation awareness. Horkoff [13] presented a solution through interactive and iterative analysis of agent-goal models in order to perform requirements engineering early. Asnar et al. [16] extended Tropos goal modelling with new techniques using a case study in banking domain. Letier and Lamsweerde [17] studied requirements analysis for partial goal satisfaction with reasoning in design engineering. Sangiovanni-Vincentelli and Sifakis [18] focused on compositional modelling in SE. Ansar et al. [20] focused on Tropos goal model by extending it to have better risk analysis. Reasoning is focused in [21] to analyze key performance indicators.

More on requirements processing is found in [22]. Identifying security requirements early in the development is the focus of [23]. Non functional requirements in the design with the help of patterns is analysed in [24] for improving software quality. Privacy and security issues are considered in RE in [26]. Security analysis in the early phases of system development is done in [27]. More details on the non-functional requirements in UML modelling are found in [28]. Requirements analysis with business processes of IT systems is the focus of [29]. Security risk analysis is explored in [30]. Analyzing misuse cases and eliciting requirements is made with certain use cases in [31]. Goal driven requirements analysis is made in [33] for achieving secure design. Security analysis of requirements for service-oriented system is made in [34]. The review of literature found that there is further scope for improving Tropos goal risk model with probabilistic risk analysis and quantitative approach for improving quality of solutions.

## 3. Problem Formulation

Risk analysis is very crucial in SE. Especially in the RE phase it is important to unearth any discrepancies to save time and effort in software development besides achieving more accurate solution. To analyze risks in the RE phase using goal-oriented approach many solutions came into existence. As explored by Asnar et al. [16] goal oriented RE analyzes goals of stakeholders and it leads to alternative sets of functional requirements that can help software development companies to save time and money besides providing accurate software to clients. Many goal-oriented methodologies such as Tropos [35], GBRAM [36], i* [37] and KAOS [38] came into existence. Out of them Tropos model is widely used and many invariants of it are available. Tropos goal oriented framework proposed by Asnar et al. focuses on risk analysis in RE. However, it has used goal satisfaction and denial values in qualitative approach. Extending this approach with probabilistic of quantitative approach can lead to better alternative solutions. This is the problem to be addressed. This is the motivation behind this paper.

## 4. Dataset Description

This dataset used in this paper is pertaining to loan origination process which has specific requirements.

**Table1:** Goals, events and treatments of LOP dataset This dataset containing goals, events and treatments is subjected to Enhanced Tropos Goal-Risk model for more effective analysis of risks associated with requirements collected in a select project.

| Goals | Events | Treatments |
|---|---|---|
| G01-Earn More Income | E01-Increase Interest Rate of Loan | T01-Use Digital Signature |
| G02-Earn from Loan Interest | E02-Forge Electronic Application | T02-Have Digital Signature Inf. |
| G03-Charge High Fee for LOP | E03-Forgery from External Attack | T03-Install Public Key Inf. |
| G04-Receive Loan Application | E04-Forgery from Internal Breach | T04-Employ Intrusion Det. Sys. |
| G05-Receive Hard-copy App. | E05-Cust Fails to Fulfil Loan Schedule | T05-Employ Strict Access Control |
| G06-Receive Electronic App. | E06-Fake Identity Document | T06-Hire Underwriter |
| G07-Ensure Repayment of Loan | E07-Fake Application | T07-Verify ID doc with Gov. DB |
| G08-Ask Mortgage | E08-Credit Bureau Ignorance | T08-Assign Liaison Officer for CB |
| G09-Monitor Usage of Loan | E09-Mispredict Monetary Cond. | T09-Train Internal Actuary |
| G10-Handle Loan Application | E10-Collusion Customer-Clerk | T10-Assess App. Anonymously |
| G11-Verify Loan Application | E11-Cust. Unemployment | |
| G12-Assess Application | E12-Economic Crisis | |
| G13-Assessed by Credit Bureau | | |
| G14-Assessed by In-house | | |
| G15-De?ne Loan Schema | | |
| G16-Proposed by Customer | | |
| G17-De?ned by Bank | | |
| G18-Approve Loan Application | | |
| G19-Approved by Clerk | | |
| G20-Approved by Manager | | |

The dataset is originally collected from www.serenity-project.org. The case study we use in this thesis is originated within the European project SERENITY2 and focuses on a typical Loan Origination Process (LOP) that starts with the receiving a loan application and ends, possibly, with the loan approval. The dataset contains stakeholders' goals, associated events and treatments.

## 5. Proposed Extended Tropos Goal Risk Model

The original Tropos methodology is found in [35]. It is the methodology to guide software development process. It is in fact a goal-oriented early requirements analysis model that analyzes goals of stakeholders and provides alternative goals so as to reduce risk in the requirements phase. In this paper we extend it to have more comprehensive analysis of risk associated with RE. The goal risk model at basic level is similar to that of [16] but our approach extends the denial and satisfaction of goals probabilistically to have better alternative solutions with less risk. Figure 1 shows the three layers in the goal-risk model.

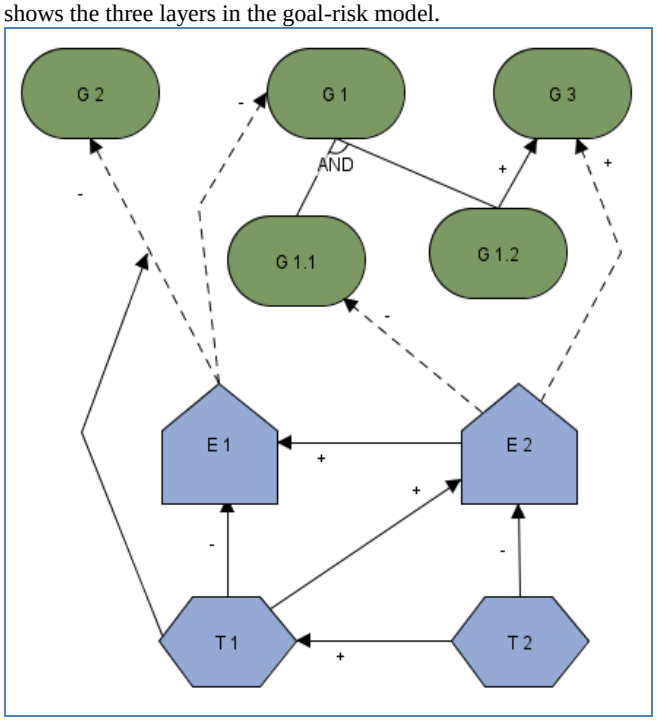



**Figure 1:** Goal-risk model with three layers

The top layer is known as asset layer or goal layer where goals of stakeholders are presented. The middle layer is known as event layer while the bottom layer is known as treatment layer. In the top layer the goals of stakeholders are presented and analyzed to know inter-relationship among all the goals. There might be AND/OR decomposition of goals into sub goals. The event layer shows set of events associated with the system in question. An event may be a potential incident that may cause harm or loss. The goal-risk framework projects events with two attributes such as severity and likelihood. Likelihood of an event can be qualitatively expressed as SAT and DEN for satisfaction and denial respectively. On the other hand severity can be expressed in the form of either negative or positive impact relation. Treatment layer contains a set of treatments that are required to handle events and mitigate risks. The treatments are also known as countermeasures that can support AND/OR decomposition. A treatment can have its influence on the risk in two ways such as reducing it or increase its severity. In order to alleviate likelihood, it is possible to use contribution relation to have denial evidence associated with an event.

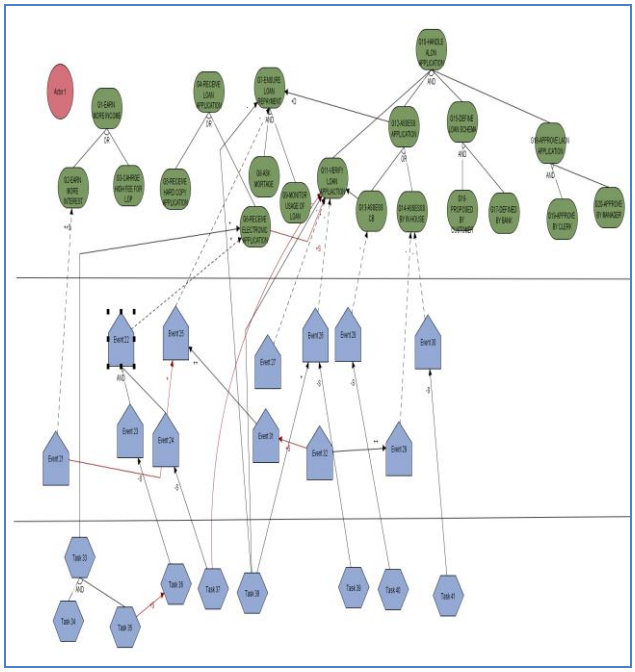


**Figure** 2: Goal-risk model for banking software module LOP

As shown in Figure 2, it is evident that the LOP dataset from banking domain presented in section 4 is visualized using goal-risk framework shown in Figure 2. The three-layered approach is shown for efficient risk analysis. As there are three layers, the mathematical model of goal-risk framework is denoted as {N, R, I}. All the nodes in the three layers are denoted as N. As there are relations among them, they are denoted as R. There are impact relations among the nodes denoted as I. The severity of a relation can have four levels such as -, --, + and ++. Double sign represents stronger positive (++) or negative (--) relation. Since goals are interests to stakeholders, they are subjected to risk analysis and alternative solutions are provided. Before analyzing further it is important to understand the meaning of the layers in this case study. Verify load application is the goal of bank which gets affected by an event known as fake identity document. Thus goal is subjected to denial (DEN) while there is no possibility of satisfaction (SAT) in this case. The qualitative values for SAT and DEN are full (F), partial (P) and none (N) and they satisfy the condition F>P>N.

In this paper we extended the SAT and DEN values to be probabilistic or quantitative. The values are thus can be expressed between 0 and 1. For instance 1 means fully denial or fully satisfactory while 0 indicates no satisfaction or denial. The values between 0 and 1 provide probabilistic values for them. Therefore in the proposed work we take 9 values instead of three values for getting better accuracy and compare with the existing system. We take 9 values those are None, None partial, None full, Partial none, Partially partial, Partial fully, Fully null, Fully Partial, Full. These values are taken respectively from 0.1 to 0.9. And also the values are taken from left to right with comparison the values of none is 0.1 and highest values is 0.9. We are taking these values to improve the performance nearly 30% improvements to compare the existing system. The probabilistic solution is based on Dempster-Shaffer theory. Based on that we are calculating likely hood values. The likelihood is defined qualitatively and can take the following values: (L) likely, (O) occasional, (R) rare and (U) unlikely, with intended meaning L>O>R>U.

To test our approach and its implementation, we ran a number of experiments with the loan origination process scenario which is a simplification of Serenity e-Business scenario. The GR framework supports risk analysis during the very early phases of software development consequently. It reduces the risk of requirements revision, and consequently the cost of development. These frameworks has been tried for analyzing requirements and risks at various critical information systems (e.g., business, safety, and mission critical).We are follow the risk assessment flow diagram to

finding the risk factors. For these to follow there are the three steps. Those are 1) Find the alternative solutions 2) Risk assessment & evaluation 3) Identification of the treatments. Find out the possible treatments and calculate cost for the possible treatment values. From that we are taking the values of total risk and costs of alternative solutions and draw the graph based on these values. For the solution of future work we are use the risk model diagram is used. From that draw the graph we are taking the values of total risk and cost for possible solutions.

### 5.1 Quantitative Risk Analysis (QRA) Algorithm

This algorithm takes goal model and acceptable risk as input and produces a set of optimized solutions. The goal model contains the details of complete model as presented in Figure 2. The LOP goals, events, treatments and relations are encapsulated in the goal risk model variable.

**Algorithm:** Qualitative Risk Analysis

**Inputs:** Goal Model GRM, Acceptable Risk ar

**Output:** Optimized Solutions OS

1 Initialize cost vector C

2 Initialize risk vector R

3 Initialize candidate solutions vector CS

4 CS = GetCandidates(GRM)

5 C = GetCosts(GRM)

6 R=GetRisks(C,GRM)

7 For each solution in CS

8 risk=ComputeRisk(solution)

9 cost=ComputeCost(solution)

10 IF risk is compatible with ar THEN

11 add solution to OS

12 END IF

13 End For

14 Return OS

**Algorithm** 1: Qualitative risk analysis

This algorithm analyses cost and risk and based on the acceptable risk provides a set of alternative and optimized solutions that exhibit minimal risk. Risk analysis focuses on the possibilities of satisfying top goals of stakeholders with acceptable level of risk. Alternative modalities are available with top goals due to OR-decomposition. Each alternative can have different cost and risk thus producing more choices to choose best one. Thus risk is mitigated and appropriate treatments that can handle risk are used. However, the treatments can cause additional cost that need to be considered. Thus the proposed model uses the costs associated with treatments as well.

## 6. Prototype Implementation and Results

We built a prototype application to demonstrate proof of the concept. The application is domain independent. It does mean it can handle case studies in any domain. We used banking domain with LOP software module. However, it can allow loading any dataset that contains stakeholder goals, events and treatments with relations.

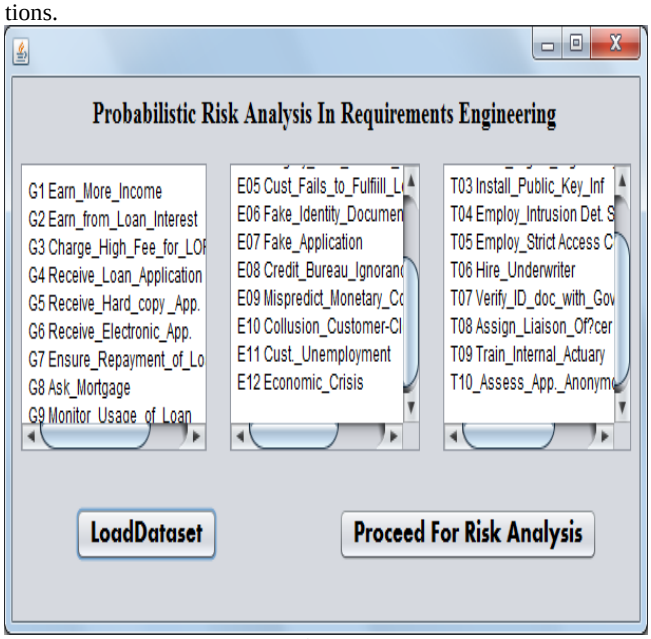



**Figure 3:** Main UI of the prototype application

As shown in Figure 3, it is evident that the application has provision for dynamically loading any dataset that is compatible with goal risk model (the three layer approach). Once the dataset is loaded, it can proceed for risk analysis. With respect to the LOP case study the candidate solutions are as presented in Figure 4. The candidate solutions are subjected to cost and risk analysis and finally the risk is prioritized to have low risk solutions. Optimal candidate solutions and final optimal solutions are also presented. Figure 5 shows the cost of treatment considered for the LOP case study.

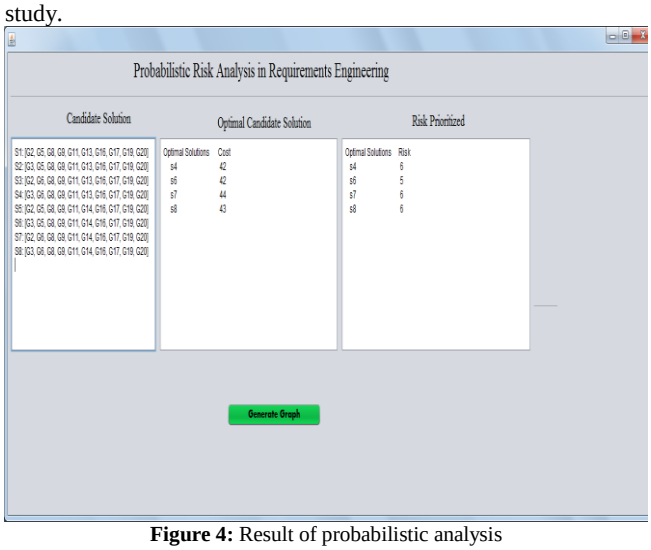
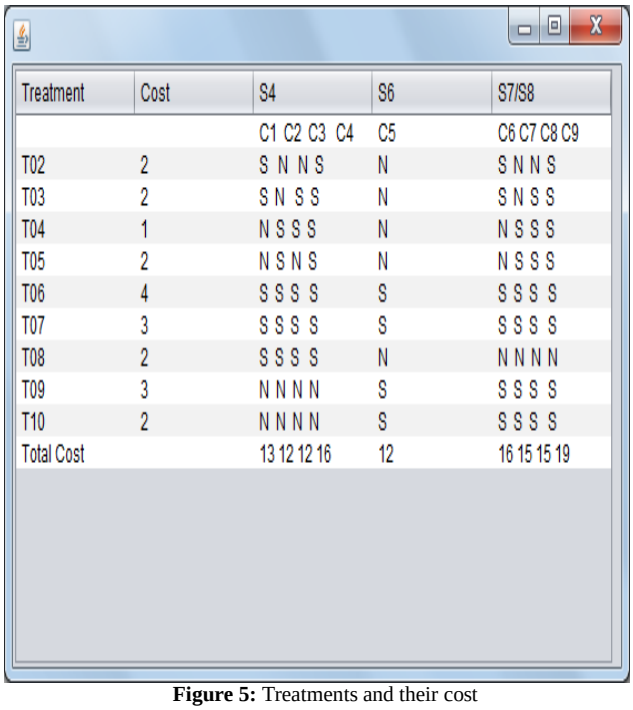



**Figure 4:** Result of probabilistic analysis

As shown in Figure 4, it is evident that the cost and risk analysis results are presented and there is provision for graphical analysis of risks associated with final optimized solutions.



| Treatment | Cost | S4 | S6 | S7/S8 |
|---|---|---|---|---|
| | | C1 C2 C3 C4 | C5 | C6 C7 C8 C9 |
| T02 | 2 | S N N S | N | S N N S |
| T03 | 2 | S N S S | N | S N S S |
| T04 | 1 | N S S S | N | N S S S |
| T05 | 2 | N S N S | N | N S S S |
| T06 | 4 | S S S S | S | S S S S |
| T07 | 3 | S S S S | S | S S S S |
| T08 | 2 | S S S S | N | N N N N |
| T09 | 3 | N N N N | S | S S S S |
| T10 | 2 | N N N N | S | S S S S |
| Total Cost | | 13 12 12 16 | 12 | 16 15 15 19 |

**Figure 5:** Treatments and their cost

The treatments considered are used to have assessment of total cost and risk. This can lead to better optimized solutions. Table 2 shows the solutions with cost and total risk.

**Table 2:** Shows solutons with associated cost and risk

| Solution Name | Cost | Total Risk |
|---|---|---|
| S4+C1 | 43 | 6 |
| S4+C2 | 42 | 6 |
| S4+C3 | 42 | 6 |
| S4+C4 | 46 | 6 |
| S6+C5 | 42 | 5 |
| S7+C6 | 45 | 6 |
| S7+C7 | 44 | 6 |
| S7+C8 | 44 | 6 |
| S7+C9 | 48 | 6 |
| S8+C6 | 44 | 6 |

After risk prioritization as shown in Figure 4, it is evident that there are four solutions that provide minimal risk. They are known as S4, S6, S7 and S8. Out of them S7 and S8 have equal risk possibilities. Therefore both will have same result when used finally. Based on this fact the values of cost and risk are presented appropriately in Table 2.

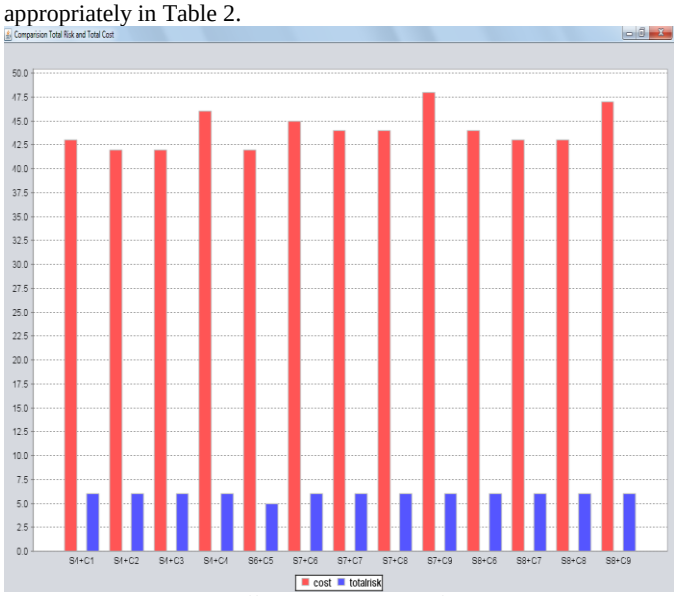



**Figure 6:** Shows different combinations of the 4 solutions

As presented in Figure 6 each solution can be understood in terms of cost and total risk. The results revealed that S6 and C5 combination provided optimized solution. Therefore S6 can be selected as highly optimal solution. Thus the proposed goal risk model which enhanced Tropos model can have probabilistic analysis to provide more choice to choose from.

## 7. Conclusion and Future Work

In this paper we proposed an enhanced goal risk framework based on the Tropos goal risk model. It is a goal oriented risk analysis model which employs both qualitative and quantitative risk analysis to provide better optimal solutions. The proposed model has three layers namely goals, events and treatments. We used LOP dataset collected from banking domain ass explored in Section 4. This dataset is used with additional domain knowledge to model it in extended Tropos goal model. The goal risk model is built in such a way that it encapsulates the presence of goals of stakeholders, corresponding events and treatments. It also models relations among the nodes besides decomposition at top level nodes. These relations provide sufficient information to analyze the cost and risk of the candidate solutions to optimize them based on the proposed risk analysis approach. We proposed an algorithm known as Qualitative Risk Analysis (QRA) to analyze risk and alleviate due to the determination of quantitative values for SAT and DEN attributes. We built a prototype application to demonstrate proof of the concept. Experimental results revealed the utility of the proposed method as it provides more alternatives among the optimized solutions based on the quantified risks associated. In future we intend to extend the proposed methodology to support Software Product Line (SPL) systems for risk analysis in RE phase.

## References


[1]. Raimundas Matulevi˘cius,Haralambos Mouratidis and Nicolas Mayer, Eric Dubois. (2012). Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management. *Journal of Universal Computer Science*. 18 (6), p816-844.

[2]. Naved Ahmed , Raimundas Matulevi˘cius and Haralambos Mouratidis. (2011). A Model Transformation from Misuse Cases to Secure Tropos, p1-8.

[3]. VITÓRIA. (2009). OTHE ALIGMET BETWEEGOAL MODELS AD ETERPRISE MODELS WITH AOTOLOGICAL ACCOUT, p1-208 .

[4]. K.Venkatesh Sharma and PV Kumar,Ph.D. (2013). An Efficient Risk Analysis based Risk Priority in Requirement Engineering using Modified Goal Risk Model. *International Journal of Computer Applications*. 73 (14), p15-25.

[5]. K.Venkatesh Sharma and Dr P.V.Kumar. (2013). A Method to Risk Analysis in Requirement Engineering Using Tropos Goal Model with Optimized Candidate Solutions. *International Journal of Computer Science Issues*. 10 (6), p250-259.

[6]. Antoine Cailliau and Axel van Lamsweerde. (2013). Assessing requirements-related risks through probabilistic goals and obstacles. *Springer*, p1-19.

[7]. Denisse Mu˜nante, Vanea Chiprianov, Laurent Gallon and Philippe Aniort. (2016). A Review of Security Requirements Engineering Methods with Respect to Risk Analysis and Model-Driven Engineering. *International Cross-Domain Conference and Workshop on Availability*, p1-17 .

[8]. Kristian Beckers, Stephan Faßbender, Maritta Heisel, Jan-Christoph K¨uster and Holger Schmidt. (2009). Supporting the Development and Documentation of ISO 27001 Information Security Management Systems Through Security Requirements Engineering Approaches, p1-8.

[9]. Armstrong Nhlabatsi,Bashar Nuseibeh and Yijun Yu. (2012). Security Requirements Engineering for Evolving Software Systems: A Survey, P1-3.

[10]. Tong Li and Jennifer Horkoff. (2010). Dealing with Security Requirements for Socio-Technical Systems, A Holistic Approach, p1-15.

[11]. Amina Souag, Camille Salinesi, Isabelle Wattiau and Haralambos Mouratidis. (2013). Using Security and Domain ontologies for Security Requirements Analysis. *The 8th IEEE International Workshop on Security*, p1-8.

[12]. Cyril Onwubiko. (2012). Modelling Situation Awareness Information and System Requirements for the Mission using Goal-Oriented Task Analysis Approach, P1-3.
[13]. Jennifer Marie Horkoff . (2012). Iterative, Interactive Analysis of Agent-Goal Models for Early Requirements Engineering, P1-449.
[14]. Mirko Morandini, Fabiano Dalpiaz, Cu Duy Nguyen, and Alberto Siena. (2011). The Tropos Software Engineering Methodology, P1-31.
[15]. Mirko Morandini · Loris Penserini AND Anna Perini · Alessandro Marchetto. (2012). Engineering Requirements for Adaptive Systems. *Requirements Engineering*, P1-28 .
[16]. Yudistira Asnar , Paolo Giorgini and John Mylopoulos. (2011). Goal-driven risk assessment in requirements engineering. *Springer*, p101–116.
[17]. Emmanuel Letier and Axel van Lamsweerde. (2004). Reasoning about Partial Goal Satisfaction for Requirements and Design Engineering. *ACM*, p1-11.
[18]. G. Goos, J. Hartmanis, and J. van Leeuwen. (2002). Lecture Notes in Computer Science. *Springer*, p1-432 .
[19]. G. Goos, J. Hartmanis, and J. van Leeuwen. (2003). Lecture Notes in Computer Science. *Springer*, P1-244.
[20]. Yudistira Asnar , Paolo Giorgini and John Mylopoulos. (2011). Goal-driven risk assessment in requirements engineering. *Springer*, p101–116.
[21]. Daniele Barone, Lei Jiang, Daniel Amyot and John Mylopoulos. (2011). Reasoning with Key Performance Indicators. *International Federation for Information Processing*, p 82–96.
[22]. SUZANNE ROBERTSON. (2009). MASTERING THE REQUIREMENTS PROCESS, P1-4.
[23]. Lawrence Chung. (1993). Dealing with Security Requirements During the Development of Information Systems. *5th Int. Conf. on Advanced Info. Sys. Eng*, p234-251.
[24]. Daniel Gross and Eric Yu. (2001). From Non-Functional Requirements to Design through Patterns. *Springer*, p18–36.
[25]. Haralambos Mouratidis , Paolo Giorgini , Gordon Manson and Ian Philp. (2002). A Natural Extension of Tropos Methodology for Modelling Security, P1-13.
[26]. Lin Liu, Eric Yu and John Mylopoulos. (2002). Security and Privacy Requirements Analysis within a Social Setting, P1-11 .
[27]. David Hutchison. (2005). Foundations of Security Analysis and Design III. *Springer*, p1-279.
[28]. Alfonso Rodríguez a , Eduardo Fernández-Medina b, Juan Trujillo c and Mario Piattini. (2011). Secure business process model specification through a UML 2.0 activity diagram profile. *elsever*, P446–465.
[29]. Peter Herrmann and Gaby Herrmann. (2006). Security requirement analysis of business processes. *Springer*, p305–335.
[30]. Michael Armstrong. (1999). $WWDFN 7UHHV UXFH 6FKQHLHU, P1-60.
[31]. Guttorm Sindre , Andreas L and Opdahl. (2005). Eliciting security requirements with misuse cases, p34–44.
[32]. Axel van Lamsweerde and Emmanuel Letier. ( 1998). Handling Obstacles in Goal-Oriented Requirements Engineering. *IEEE*, p1-29 .
[33]. Haralambos Mouratidis and Jan Jurjens. (2006). From Goal-Driven Security Requirements Engineering to Secure Design, P1-26 .
[34]. Michael Menzel,Ivonne Thomas and Christoph Meinel. (2009). Security Requirements Specification in Service-oriented Business Process Management. *IEEE*, p1-8. 11 tropos [35], 1 gram [36], i* 44 [37], kaos 17 [38]
[35]. Bresciani P, Perini A, Giorgini P, Giunchiglia F, Mylopoulos J (2004) Tropos: an agent-oriented software development methodology. J Auton Agent Multi Agent Syst 8(3):203–236.
[36]. Anton AI (1996) Goal-based requirements analysis. In: Proceedings of the 2nd IEEE international conference on requirements engineering (ICRE'96), IEEE Computer Society Press, Washington, DC, USA, p 136.
[37]. Yu E (1995) Modelling strategic relationships for process engineering. PhD thesis, University of Toronto, Department of Computer Science.
[38]. Dardenne A, van Lamsweerde A, Fickas S (1993) Goal-directed requirements acquisition. Sci Comput Program 20(1–2):3–50.