ISSN 2563-7568

RESEARCH ARTICLE

Financial Risk Assessment using Machine Learning Engineering (FRAME): Scenario based Quantitative Analysis under Uncertainty

Krishna Mohan Kovur[1,2*], Medha Gedela[2], Arjun M Rao[2]

[1]*University of Alberta, Edmonton, Canada*
[2]*Banking Labs Inc, Toronto, Canada*

Abstract

Risk management functions, under uncertainty, in the Banking Industry have been changing and will continue to change with the recent advancements and innovations. Embracing uncertainty and working with measurable risk becomes critical, therefore quantitative risk severity assessment is critical for sustainable financial excellence. In this paper, the authors propose Financial Risk Assessment using Machine Learning Engineering (FRAME) based on artificial intelligence (AI) and machine learning (ML), which has two significant contributions. Firstly, adoption of machine learning models for banking towards risk quantification and secondly, granularity that emphases on customized logic via multi-factor analysis modeling at different levels of abstraction connecting machine learning models. These contributions will help Financial Institutions (Fis) that will gain the most benefits and opportunities. In a nutshell, the framework analysis presented in this paper is intended as a step towards building a framework of risk modeling from qualitative to quantitative, viewed at different levels of abstraction to access risk severity in the banking applications.

Key Words: *Risk assessment; Quantitative analysis; Granularity; Machine learning; Banking; Analytic Hierarchy Process (AHP)*

***Corresponding Author**: Krishna Mohan Kovur, University of Alberta, Edmonton, Canada; E-mail: Krishnamohan.Kovur@bankinglabs.com*

***Received Date**: November 28, 2023, **Accepted Date**: December 12, 2023, **Published Date**: December 15, 2023*

***Citation:** Kovur KM, Gedela Medha, Rao AM. Financial Risk Assessment using Machine Learning Engineering (FRAME): Scenario based Quantitative Analysis under Uncertainty. Int J Auto AI Mach Learn. 2023;3(1):1-13.*

1. Introduction

In recent banking trends, operational and strategic uncertainties have significantly increased for number reasons including failing to understand high risk scenarios under uncertainty and an ever-changing organizational dynamic that makes it difficult for control mechanisms aligning the speed and agility. To address new risks emerging with changing business requirements under uncertainty, the paper introduces a new quantitative risk management framework in banking via machine learning in conjunction with multi-factor analysis. It is therefore necessary to develop a risk management model that prioritizes uncertainties and quantifies their degree. Our paper introduces the concept of granularity (or granularity) for understanding the depth of uncertainty through related risk severities and their associated risk influencing variables. As such, to provide a detailed analysis of the application problem via granularity (varying levels of abstraction), we need a robust methodology for risk quantification for performing a detailed analysis. In our proposed risk model framework, risk severity is quantified at different levels of abstraction, facilitating decision makers' estimations and evaluations of the concerned application decision problem. The purpose of this paper is therefore to the first multi-criteria (multi-factored) based risk framework that has been applied to risk management in banking domain area at the Banking Labs.

The following benefits apply to our proposed quantitative risk management framework over qualitative risk analysis.

- Express results at different abstraction levels and rationalize the outcome with added objectivity.
- Assess the greatest factors affecting the application at various abstraction levels by comparing the results among risk factors.
- Enhance risk management by accumulating assets and creating tools and utilities.
- Provides prospective feasibility analysis, such as cost, benefit, and opportunities, for the considered application and increases return on investment (ROI).
- Added granularity enhances the proposal's numerical superiority with respect to other methods of assessing risk severity.

The purpose of this paper is to examine how risk management is applied in the banking sector, as well as in the financial sector. As a result, it aims to compile the relevant literature on a comprehensive risk assessment of banking application projects (BAPs) that takes multiple factors into account. Furthermore, the paper discusses risk management models analysis and proposes a multi-criteria decision-making approach to assess specific risks related to core BAP.

2. Background

2.1. Banking risk management

As a result of our literature review [1-11] on banking risk management analysis and assessment, it has been noted that various aspects of uncertainty prevailing in financial institutions have changed over the past few decades. This led us to identify gaps in general and a need for a greater emphasis on quantitative analyses, especially big data analytics, as the basis for our current research. Based on the findings of the survey [1-11], the following

Figure 1, provides a brief outline of some of the key risks associated with the banking sector on a day-to-day basis.

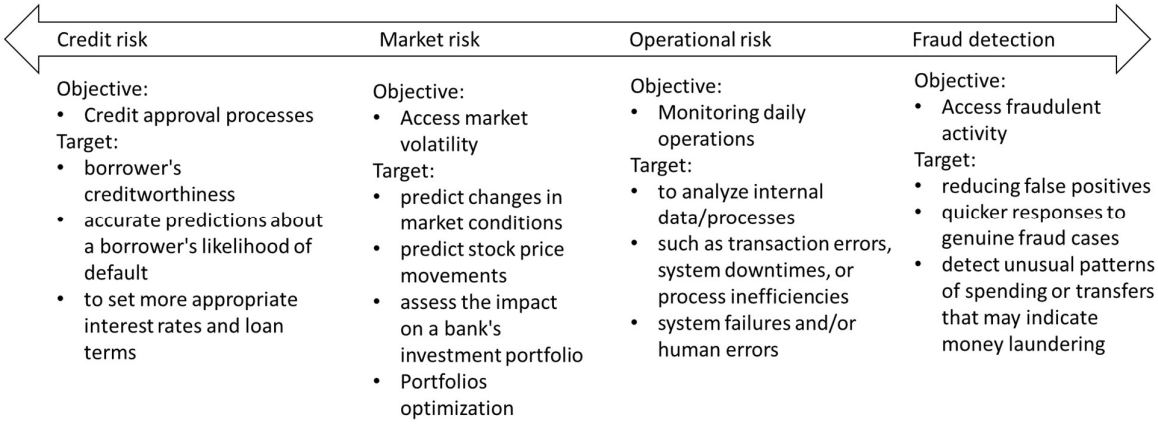

Figure 1: *Summary of various banking risk models' overview.*

To summarize, credit risk, market risk, operational risk, as well as fraud detection and detection tools are all critical components of risk management. Managing these risks can ensure financial stability, asset protection, and compliance by understanding, measuring, and mitigating them. It is essential to develop robust risk management practices that reduce the likelihood of unforeseen events negatively impacting stakeholders. The paper attempts and analyses the risk implications of various possible scenarios on big data analytics to address various shortcomings and enhance decision-making capabilities.

2.2. Multi Criteria Decision-making Approaches (MCDA)

An MCDA offers a formal, quantitative way to evaluate decisions while taking a variety of factors into account. In the literature, MCDA applications [12-21] often involve large numbers of stakeholders or stakeholder groups in policy-based decision making. The AHP [13], the analytical network process (ANP) [20], the grey relational analysis (GRA) [14], and goal programming have become prominent methods of multiple criteria decision-making. For banking decision makers, the main advantage of MCDA is its ability to help determine which applications to consider against the economic, political, technological, environmental, and social aspects. As well as suited for multiple conflicting goals, time-variant real-world applications; provides an opportunity for discussion over complex decisions from the point of view of a variety of stakeholders. For example, comfort and quickness of calculations; flexibility to accommodate complex relationships; cause/effect relationships; and the ability to directly model the effects of different decisions on outcomes are some of the differences between these models. There is no study of how risk severity differs across applications involving multiple risk factors in any of these models.

2.3. Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process is a multiple-criteria decision-making methodology developed by Saaty to deliver a flexible and easy way to deal with complex decisions [12-21]. The purpose of it is to assist decision makers in reaching conclusions regarding different options in the process of risk management. The process involves the formulation of a vector

of preferences in order to perform a quantitative analysis. It is generally accomplished in four major stages: (i) pyramiding the model in hierarchical form, (ii) calculating the weight vectors, (iii) aggregating the weigh vectors according to the pyramiding structure, and (iv) conducting the final mathematical analysis.

2.4. Granularity

Granular computing [22] is an approach of perceiving data as information granules that are well defined at divergent and distinct levels of abstraction. A granule is defined as a piece of information at varying degrees of perception representing a single problem at multiple levels. In other words, granular computing represents a process of problem solving that signifies a focal point of observation. In the proposed methodology, a focal point of observation is a measure of risk severity (low, medium and high) at an objective level, as well as at the levels of risk factors and sub-factors. Information granules are defined at divergent and distinct levels of abstraction that provides useful information [22]. The underlying formalism relies on the way in which information granules are represented and characterized in a real time application. In this paper, the evaluation of risk severity with consistent granularity has been applied at multiple levels of abstraction or granulation of the hierarchy. Different levels of granularity allow us to notice and examine a given application problem considering all information (overall view) or selected pieces of information (individual level views). During the overall view more detailed information is analyzed and whereas, at individual level consider only part of the information or focus on specific information, ignoring other information. This means that we treat an application problem at multiple levels of abstraction and apply a multi-view analysis.

3. Problem Formulation and Objective

To analyze granular quantitative approach that can be adopted towards the evaluation of the uncertainty with a focus on how coarseness enhances decision-making capability in the banking area. Thus, the paper answers directly or indirectly with respect to banking risk management which can be expressed by underlying set of questions to create a platform with regards to:

- To quantify the banking application projects risks considering several factors that affect the risk severity at multiple levels of abstractions - what type of models must be created to capture the prevailing uncertainty?
- What are the tools and techniques available to assess risk in a multi criteria decision-making environment regarding core BAP applications? Which methods of assessment are conducive for application in various banking project scenarios?
- What are the various issues faced in general in risk evaluation, highlighting the characteristic features specific to the solution methodologies mapped with banking applications?

4. Quantitative Risk Assessment (QRA) and Modeling Requirements: A Preamble

Quantitative Risk Assessment (QRA) [23-35] is a methodology for evaluating the risks associated with complex real-time business processes and applications through a systematic

and comprehensive approach. The purpose of this section is to provide a detailed analysis of the modeling requirements for QRA, with a focus on critical factors that must be taken into account in order to ensure accurate and reliable results. The study discusses the importance of defining clear and specific targets for the assessment, which forms the basis for all QRA activities. It emphasizes the need for comprehensive data collection and analysis, including historical data, expert judgments, and relevant research findings. The section also highlights the significance of selecting appropriate risk assessment models and tools that are suitable for the precise context and objectives of the considered study. A crucial part of any model development process is model selection, which is often dependent on the nature of the problem, the data available, and the granularity of the desired outcome. The series of steps will help practitioners enhance the credibility and effectiveness of QRA and enhance risk management and categorization of risk modeling designs and assessments by following the customized modeling requirements outlined below.

Step 1: Selection of risk models, approaches, and tools.

- The underlying aspects of uncertainty (randomness) and certainty (uniqueness) associated with inputs must be addressed for healthy computations - stochastic and deterministic approaches should be selected appropriately.
- The use of formal methods, multiple-criteria decision-making methods, soft computing methods, etc.
- In addition, there are some quantitative assessment tools, such as Monte Carlo simulation, decision trees, and mathematical equations for calculating and analyzing the risks (these tools assist in estimating the overall exposure and potential outcomes).

Step 2: Key characteristics of risk elements (factors Interdependencies).

Analyze how different risk influencing factors may interact or depend on one another. In addition, some of them may be correlated, so their combined impact should be considered. Among the factors, a comprehensive investigation should be conducted with regard to (i) dependent or independent, (ii) linear or non-linear, and (iii) the complexity of the network.

Step 3: Choice of data.

Depending on the availability of the data, there are three options: some data source you have access to with expert input, historical data plus expert input (for data that is missing), historical data alone must consider for the data modeling of the considered application problem.

Step 4: Risk Sensitivity Analysis, Risk Tolerance, and Baseline scenario.

- Perform sensitivity analyses to determine how input parameters (e.g. probability distributions, consequences) affect the outcome. In this way, the most influential factors and their impact on overall risk can be identified.
- Defining risk tolerance levels and criteria is essential in determining the acceptable level of risk, which is a measure of what level of risk is tolerable. As a result of these criteria, risk mitigation strategies are developed, and decisions are made.
- A baseline scenario or reference case demonstrates what would happen if risk mitigation efforts were not implemented.

5. Application of Machine Learning Risk Modeling in Banking: An Overview

The field of risk modeling is experiencing a great deal of change due to the emergence of machine learning (ML) models as the traditional methods of modeling risk are often unable to cope with the volumes and complexity of data. A number of new tools have been developed for analyzing and predicting future risks as well as for increasing their accuracy by ML. Risk modeling involves identifying and quantifying diverse risks that might impact an organization or system. It has been proved through machine learning that it is possible to analyze large datasets and uncover patterns and relationships that would not normally be visible to analysts, making it an excellent tool for data mining since it can handle large and complex datasets with ease. As a result, machine learning algorithms are capable of processing enormous amounts of information and identifying designs and relationships that may not be obvious to human predictors. In doing so, organizations will be able to make better informed decisions about the risks they may face and take the necessary steps to minimize them. A further advantage of machine learning is its ability to adapt to changing risk circumstances and update on a regular basis to improve performance as new data is available. The importance of this is particularly noticeable in areas where risks are constantly evolving, such as cybercrime applications.

As a result of artificial intelligence (AI), machine learning (ML) is revolutionizing the banking industry by providing new and efficient ways of assessing and mitigating risk. The role of risk modeling plays an integral part in the operations of all banks, as it helps them to understand and manage the risks associated with their range of financial products and services. By using machine learning techniques, banks can build models that are able to predict and identify potential risks, ultimately allowing them to make better decisions about their investments. The last section of this section concludes with the overview steps of how to address problems across various risk application categories.

Step 1: Identify the target output: binary classification (risky or not), multi-class classification (low, medium, high risk), regression (risk score), etc.

Step 2: Performing data preprocessing: dealing with outliers, missing values, and inconsistencies.

- Missing data/values imputations: (1) Uni-Variant Imputation Techniques and (2) Multivariate A number of different methods of imputation can be used for missing data/values, such as (1) Univariate Imputation Techniques and (2) Multivariate Imputation of Chained Equations (MICE) Technique.
- Feature engineering: Create features that may be relevant to risk prediction.
- Ensure that all features are scaled equally by normalizing/standardizing the data.
- The data should be divided into three categories: training, validation, and testing.

Step 3: The most appropriate features to use for the prediction task (the target variable) should be selected.

- A number of statistical tests, recursive feature addition, recursive feature elimination, random shuffling, or models such as Lasso that perform feature selection can be used in conjunction with these techniques.

Step 4: Model Selection: The ML algorithm to choose will be based on the data and the problem being addressed. Decision trees or random forests, for example, could be effective in solving non-linear problems with multiple categorical variables.

Step 5: Model Training: Using the validation set, tune hyperparameters and prevent overfitting by training the chosen models on the training dataset.

Step 6: Test set evaluation: Compare performance between the model and the test set.

- Based on the problem definition, choose the appropriate metrics (e.g. accuracy, ROC-AUC (test and train data sets), F1 score, R2 (train and test data sets), and CV (Cross validation).
- Verify the model's performance under different scenarios or subgroups to ensure it is not biased.

Step 7: For end-user testing, hold-out data sets should be tested at the customer's/client site.

6. Proposed Scenario based Granular Analysis and Application to Case Study

The scenario-based granular analysis examines individual components or variables that can affect outcomes to examine possible future outcomes. It is especially useful when dealing with complex systems or uncertain environments in which multiple factors can interact in unpredictable ways. It allows the contributory role of each component to be determined in detail, allowing for a thorough understanding of a larger situation. In this paper, we present granular analysis of the machine learning (ML) model by utilizing AHP model across various stages of ML model development. This Figure 2 illustrates various components of the proposed scenario based granular analysis framework, and quantitative risk assessment within Banking Labs.

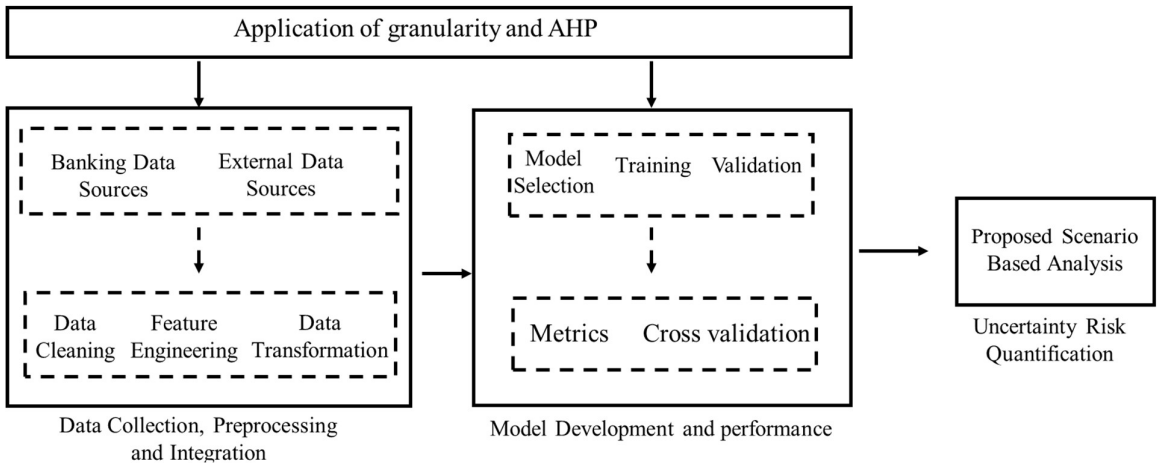

Figure 2: *Proposed scenario based granular analysis framework: quantitative risk assessment.*

As part of the granular approach, external factors are also evaluated, including regulatory changes, economic shifts, and technological advances, each in its context and influence on the success of the product. The scenario can be viewed from an assembly of perspectives to anticipate challenges and opportunities. The use of scenario-based granular analysis enables an understanding of the individual components of a situation, their interactions, and the risk they pose, facilitating strategic decision-making and risk management. In the banking sector, AHP can be applied for a granular analysis of various scenarios such as credit risk assessment, investment decisions, and customer satisfaction evaluations. The AHP follows the following generic steps which are summarized below.

Step 1: Objective with respect to multi criteria evaluation and problem formulation. Defining or revealing the overall objective or goal of the application problem.

Step 2: Risk factors and risk sub-factors. Identifying the risk elements from the application problem as risk factor and risk sub-factor on various levels of abstraction (granularity).

Step 3: Options & possible outcomes. It is the last level in the hierarchy representing different levels, in our case it is risk severity assessment outcome.

Step 4: Decision matrix. Forming relative importance of the elements at each level of the hierarchy in the form via formation of pair-wise judgement matrices using a nine-point scale [14].

Step 5: Evaluation of decision matrix. Evaluation of each judgement matrix (step 4) is performed to evaluate normalized eigenvector associated with its principal eigenvalue (largest eigenvalue) [15], and a consistency check [15].

Step 6: Weight vector/priority vector. Overall weights for options/possible outcomes (risk severity in our application) are found through the aggregation of weights via aggregation matrix.

- comparison among risk factors in the first level, results in one matrix
- comparison among the risk sub-factors in respect to every risk sub-factor from the second level, results in multiple matrices equal to number of sub-risk factors
- comparison of likeliness of severity of risk: low, medium, high for every risk sub-factor, results in various matrices equal to number of risk sub-factors.

Step 7: Risk analysis. The detailed risk analysis is performed based on computed priority vectors of the final decision matrix (from step 6) with various tasks ("what-we-do") and results obtained (what-we-get) in granular perspective. This constitutes a key benefit over any qualitative analysis.

Step 8: Decision. Based on the analysis results from step 7, risk treatment plans and implementation decisions are being made.

Step 9: Communication & review. With the results obtained from step 8, communication and review among stakeholders takes place, depending on the review, model can be revisited if required.

Based on literature review we have formulated a case study that consists of two modules. First one module being in general to the risk management in banking application projects (BAP) projects that has been studied. Whereas second module, we have considered specific risks related to core BAP. Based on the proposed risk management framework, we have identified and classified the risk factors and risk sub-factors for the respective modules.

The formulated case study in respect to first module with the following factors [1-11] and sub-factors [1-11] are as follows: The risk factors are: Technical risk (RG_1); Financial and Economic risk (RG_2); Organizational risk (RG_3)

- sub-factors under the factor RG_1 are: Change in Scope (RG_{11}), Implementation methodology (RG_{12}), Selection of Technology (RG_{13}), Equipment risk (RG_{14}); Change in Engineering and design (RG_{15}), Risk due to material (RG_{16})
- sub-factors under the factor RG_2 are: Inflation risk (RG_{21}), Local law changes (RG_{22}), Fund risk (RG_{23}), Inappropriate estimate (RG_{24}), Changes due to government policies (RG_{25})
- finally, sub-factors under the factor RG_3 are Proficiency of owner's project group (RG_{31}), Consultant's skill (RG_{32}), Vendor's competence (RG_{33}), Capability of Contractor's ability (RG_{34})

Similarly, second module with the following factors [1-11] and sub-factors [1-11] are as follows: The risk factors are: Credit risk including counterparty credit risk (RS_1); Market risk (value at risk (VaR)) (RS_2); Operational risk (RS_3); Liquidity risk (RS_4); Insurance risk (RS_5)

- sub-factors under the factor RS1 are: Exposure to households and small business enterprises (SMEs) (RS_{11}), Exposure to large corporations and institutions (RS_{12})
- sub-factor under the factor RS_2 are: Equity Risk (RS_{21}), Interest Rate Risk (RS_{22}), Exchange Rate Risk (RS_{23}), Commodity Risk (RS_{24})
- sub-factors under the factor RS_3 are: Internal fraud (RS_{31}), External fraud (RS_{32}), Employment practices and workplace safety (RS_{33}), Clients, Products and business practices (RS_{34}), Execution, delivery and process management (RS_{35}), Damage to physical assets (RS_{36}), Systems and data failure (RS_{37}), Information technology security (RS_{38}), Model Risk (RS_{39})
- sub-factors under the factor RS_4 are: Cash-flow risk (RS_{41}), Asset/product risk (RS_{42})
- finally, sub-factors under the factor RS_5 are: Financial and Non-Financial Risks (RS_{51}), Pure and Speculative Risks (RS_{52}), Fundamental and Particular Risks (RS_{53})

Figure 3 depicts in specific implementation of the case study attributes with presented framework in this paper (refer to Figure 2) for details.

Other potential applications of the proposed framework include multi-factor quantitative risk analysis for credit, market, operational, and fraud detection, which can be used to address the following question formulations:

- Has the False Positive rate of blocked transactions monitoring increased?
- Have money laundering patterns changed over the past two years, or have they remained the same?

- Has the number of incidents of asset misappropriation gone down or up from last quarter?
- What is the accounting fraud rate for this year? Is it higher or lower than last year??
- What is the trend in the number of cybercrimes over the last year? Did it decrease or increased?

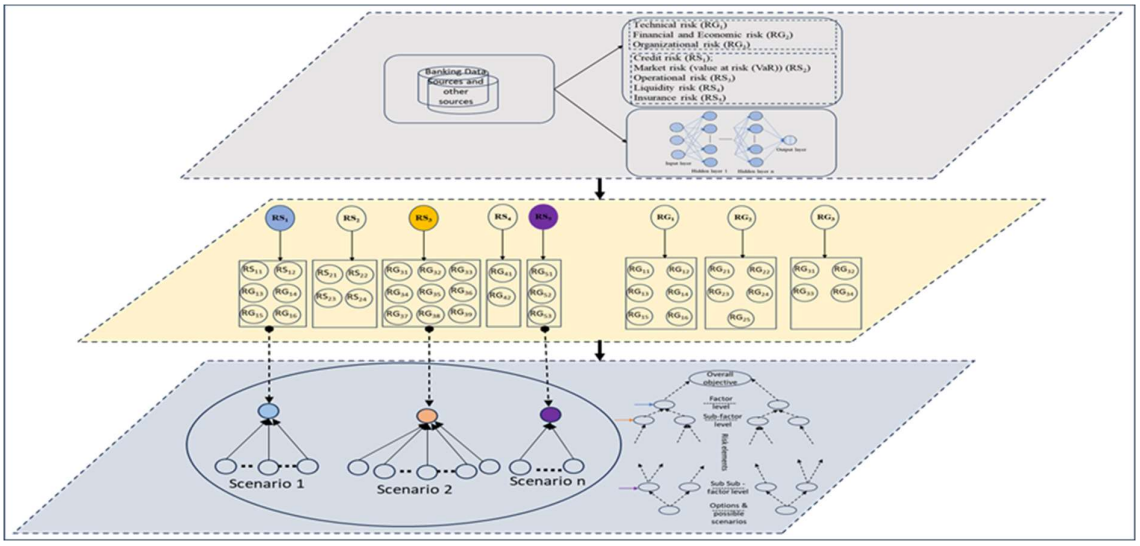

Figure 3: *Specific implementation of the case study attributes with presented framework.*

The proposed framework is confined and introduces the conceptual methodology associated with quantitative model analysis, granularity, and machine learning model. Banking Labs' R&D and development teams are currently working on various scenarios for the proposed framework, including assessing it, validating its models, and evaluating its applicability.

7. Conclusion

The paper proposes a scenario-based machine learning approach to granular analysis through multifactored analysis of scenarios for risk quantification. We have introduced general modeling requirements for quantitative risk assessment, with an emphasis on identifying appropriate risk models, identifying key characteristics of risk elements, providing data sources, and maintaining model stability; and then analyzed machine learning risk models in banking. Thus, an introduction to granularity and a quantitative approach to machine learning models is presented in the paper. The aim of this study is to develop an innovative framework for scenario-based granular analysis that examines individual components or variables that can affect future outcomes to evaluate possible uncertainties. The Financial Risk Assessment using Machine Learning Engineering (FRAME) presented here serves as a scenario-based quantitative analysis under uncertainty for several banking applications, including credit, market, technical, and fraud detection, to quantify risk assessment at a variety of abstraction levels.

Acknowledgement

Authors are thankful to Higher Education Department, University of Alberta, Edmonton, Banking Labs Inc, Toronto, Canada for providing lab facilities.

References

1. Oualid A, Hansali A, Balouki Y, et al. Application of machine learning techniques for credit risk management: a survey. Lect Notes Netw, 2022;357:180-91.

2. Khatri S, Arora A, Agrawal AP. Supervised machine learning algorithms for credit card fraud detection: a comparison. 10th International Conference on Cloud Computing, Data Science & Engineering, Noida, India. 2020.

3. Lestari NI, Hussain W, Merigo JM, et al. A survey of trendy financial sector applications of machine and deep learning. In: Jan MA, Khan F (eds), Application of Big Data, Blockchain, and Internet of Things for Education Informatization, Springer, Cham. 2023. pp.619-33.

4. Tavana M, Abtahi AR, Di Caprio D, et al. An artificial neural network and Bayesian network model for liquidity risk assessment in banking. Neurocomputing. 2018;275:2525-54.

5. Tae CM, Hung PD. Comparing ML algorithms on financial fraud detection. Proceedings of 2nd International Conference on Data Science and Information Technology, Seoul, Republic of Korea. 2019.

6. De Roux D, Perez B, Moreno A, et al. Tax fraud detection for under-reporting declarations using an unsupervised machine learning approach. Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, London, UK. 2018.

7. Xia Y, Liu C, Da B, et al. A novel heterogeneous ensemble credit scoring model based on bstacking approach. Expert Syst Appl. 2018;93:182-99.

8. Monamo P, Marivate V, Twala B. Unsupervised learning for robust Bitcoin fraud detection. Information Security for South Africa (ISSA), Pretoria, South Africa. 2016.

9. Awoyemi JO, Adetunmbi AO, Oluwadare SA. Credit card fraud detection using machine learning techniques: a comparative analysis. International Conference on Computing Networking and Informatics (ICCNI), Royal Holloway, England. 2017.

10. Sanford A, Moosa I. Operational risk modelling and organizational learning in structured finance operations: a Bayesian network approach. J Oper Res Soc. 2015;66:86-115.

11. Keswani B, Khanna A, Gupta D, et al. Adapting machine learning techniques for credit card fraud detection. International Conference on Innovative Computing and Communications, Singpore. 2020.

12. Acze J, Saaty TL. Procedures for synthesizing ratio judgements. J Math Psychol. 1983;27:93-102.

13. Saaty TL, Vargas LG. Models, Methods, Concepts & Applications of the Analytic Hierarchy Process. (2ndedn), Springer, USA. 2012.

14. Saaty TL. Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World. RWS Publications, Pittsburgh, USA. 2001.

15. Saaty TL. Decision-making with the AHP: why is the principal eigenvector necessary. Eur J Oper Res. 2003;145:85-91.

16. Mohan KK, Srividya A, Verma AK. ANP based software reliability prediction using PoCs and subsequent employment of orthogonal defect classification measurements for risk mitigation during prototype studies. Int J Syst Assur Eng Manage. 2010;1:8-13.

17. Saaty TL. The Network Hierarchy Process. RWS Publications, Pittsburgh, USA. 1996.

18. Saaty TL, Vargar LG. Decision Making with Analytic Network Process. Springer, Pittsburgh, USA. 2006.

19. Prashanthi K, Mohan KK, Antić Ž, et al. Multiple ratiometric nanothermometry using semiconductor $BiFeO_3$ nanowires and quantitative validation of thermal sensitivity. Micro Nano Syst Lett. 2022;10:1-12.

20. Saaty TL. Decision Making with Dependence and Feedback: The Analytic Network Process. RWS Publications, Pittsburgh, USA. 2001.

21. Mohan KK, Prashanthi K, Hull R, et al. Risk assessment of a multiplexed carbon nanotube network biosensor. IEEE Sens J. 2018;18:4517-28.

22. Mohan KK, Reformat MZ, Pedrycz W. Analytic hierarchy process and granularity: assessment of risk severity on livestock wellness. Proceedings of IEEE 2012 Annual Meeting of the NAFIPS, Berkeley, CA, USA. 2012.

23. Mohan KK, Srividya A, Gedela RK. Quality of service prediction using fuzzy logic and RUP implementation for process oriented development. Int J Reliab Qual Saf Eng. 2008;15:143-57.

24. Giray G, Bennin KE, Köksal Ö, et al. On the use of deep learning in software defect prediction. J Syst Softw. 2023;195:111537.

25. Mohan KK, Verma AK, Srividya A. An effective early software reliability prediction procedure for process oriented development at prototype level employing artificial neural networks. Int J Reliab Qual Saf Eng. 2011;18:237-50.

26. Kovur KM, Gedela RK. An Integrated Approach of BOCR Modeling Framework for Decision Tool Evaluation. In: Karanki D, Vinod G, Ajit S (eds), Advances in RAMS Engineering. Springer, Cham. 2020;pp.109-48.

27. Mohan KK, Srividya A, Verma AK. Prototype dependability model in software- an application using BOCR models. Int J Syst Assur Eng Manage. 2016;7:167-82.

28. Gedela RK, Mohan KK, Prasad VK. Application of BOCR models in service oriented architecture (SOA): study on model validation through quantification for QoS considerations. Int J Syst Assur Eng Manag. 2018;9:1346-54.

29. Lee AH, Chang HJ, Lin CY. An evaluation model of buyer–supplier relationships in high-tech industry—The case of an electronic components manufacturer in Taiwan. Comput Ind Eng. 2009;57:1417-30.

30. Mohan KK, Verma AK, Srividya A. Early software reliability prediction using ANN for process oriented development at prototype level. 20th International Symposium on Software Reliablity Engineering (ISSRE), Mysuru, Karnataka, India. 2009.

31. Mohan KK, Shaik HU, Srividya A, et al. White-Box and black-box reliability modeling framework: integration through analytical model and user profile validation via deep learning—a practitioner's approach. Int J Reliab Qual Saf Eng. 2021;28:2140007.

32. Mohan KK, Verma AK, Srividya A. Early qualitative software reliability prediction and risk management in process centric development through a soft computing technique. Int J Reliab Qual Saf Eng. 2009;16:521-32.

33. Mohan KK, Verma AK, Srividya A, et al. Early quantitative software reliability prediction using petri-nets. The Third International Conference on Industrial and Information Systems, Kharagpur, India. 2008.

34. Mohan KK, Verma AK, Srividya A, et al. Integration of black-box and white-box modeling approaches for software reliability estimation. Int J Reliab Qual Saf Eng. 2010;18:261-73.

35. Mohan KK, Verma AK, Srividya A. Software reliability estimation through black box and white box testing at prototype level. 2nd IEEE International Conference Reliability, Safety and Hazard Risk-Based Technologies and Physics of Failure Methods, Mumbai, India. 2010.