CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
http://magellanes.com/

CYBER SECURITY STRATEGY CALCULATION THROUGH INTEGRATED MACHINE LEARNING AND MULTI-CRITERIA DECISION METHODS

Manuj Darbari[1*], Naseem Ahmed[2]
[1]Research Scholar, Integral University, India
[2]Professor, Integral University, India
*****Corresponding author: email: manujuma@gmail.com;
Emails of coauthor: [2]amdnaseem@iul.ac.in

Abstract

Objectives: To identify the shortcomings of the Information Technology Act-2000 and recommend measures to strengthen its applicability against emerging forms of cybercrime while fostering development and protecting constitutional rights.

Methods: Here MULTIMOORA methodology for multi-criteria decision making is employed on the proposed changes to the IT Act. The historical data on previous changes was evaluated using the Random Forest technique to forecast the anticipated usefulness of further amendments in terms of their efficiency, cost, and integration with other countries.

Findings: The proposed methodology suggested amendments that are meant to build India's cyber legislation to the required standard while also strengthening the country's defense against AI driven and crypto-jacking attacks. The use of RF algorithm shows the effects of these factors on the success or otherwise of the amendments. The findings underline the need for international collaboration, cost efficiency and efficacy in developing the new laws. These new laws are expected to advance the existing digital governance processes in India.

Novelty: The study is distinct as it employs machine learning in the analysis and integrates it with multi-criteria models to analyze the factors affecting it, which reduces the time complexity and enhances the overall throughput.

Keywords: Cybercrime, Law Enforcement, Cyber-Disaster Management, MOORA (Multi-Objective Optimization based on a Ratio Analysis).

Introduction

The Indian cyber landscape has several advantages; however, the advantages are accompanied by a major disadvantage: the increasing cybercrime[1–3]. During the last few years, India witnessed a drastic surge in cybercrime incidents such as phishing attempts, cyber fraud, and data breaches. This is because of the increased digitization of financial transactions and the wide use of the internet by the Indian population.

The law provided legal status to electronic data interchange and other forms of electronic communication[4], while at the same time defining several offenses related to computer usage and setting forth corresponding punishments for their commission.

In 2008, the IT Act 2000 was amended with more offense types like cyber terrorism, child pornography, and voyeurism. The regulation regarding data protection and imposition of liability on intermediaries for particular unlawful actions were framed under this law. For the prediction of the

ISSN:1624-1940
http://magellanes.com/

possibility of success for the proposed amendments, the MULTIMOORA method along with the Random Forest algorithm[5,6] was used. This machine learning procedure lets us get a better idea how each of these three criteria—effectiveness, social acceptability, and enforceability by the law—determines the success of legislative amelioration. These features are analyzed concerning a Random Forest model. Quite a lot is therefore attributed to the dimensions of international cooperation and the low costs of the reform by itself. Their status within the MULTIMOORA ranks will rise later on.

This is the first study to integrate machine learning with multi-criteria analysis, evaluating legislative changes in cyber legislation. It reduces the gap between data-driven insights and policymaking.

Methodology

This section would be a comparative legal analysis of the IT Act, 2000[7], and relevant provisions of the Indian Constitution by judging whether the IT Act is in harmony or in conflict with certain constitutional rights that include the right to privacy, Article 21; freedom of speech and expression, Article 19; and other basic rights. This approach visualizes case law analysis, judicial pronouncements and amendments to the IT Act with an objective to identify conflicts existing in it with constitutional provisions on violations of privacy, censorship, regulation of cybercrime. The qualitative framework employed here utilizes the MULTIMOORA decision analysis technique[8,9] to make an intercomparison of legal amendments with legislative proposals evaluated under the principles of constitutional proportionality and public interest. Primarily, the study will rely on the text of IT Act, the Indian Constitution, case law databases government publications, and reports from regulatory authorities, like the Ministry of Electronics and Information Technology (MeitY). The conflicted areas of the scope are data privacy, surveillance, and censorship; recommendations will be provided for reaching a balance between technology regulation and fundamental rights. Although no human subjects have been involved, copyright and principle of fair use have followed to cite legal texts and judgments throughout the study.

Discussion and Decision Analysis using MULTIMOORA Method:

In order to analyze the sets of amendments of the Information Technology Act-2000 towards the threat of the Cyber world[10–12] authors have established decision matrix using the secondary data obtained through survey. The study deals with mapping the proposed amendments and criteria with the list of achievable solutions.

In order to analyze the above situation empirically we use MULTIMOORA Analysis[13], it analyses multiple objectives to match with criteria by implementing ratio-proportion amongst the best possible alternate sets. There are three basic components of MULTIMOORA apptoach which is used to analyse the above problem it includes:

• Alternatives could be the different amendment proposals (A1, A2, A3, etc.).

• Criteria with the list of Goals such as reduction of cyber-crimes (C1), successful prosecution rates (C2), international cooperation (C3), etc.

Applying the dimensionality relation to the above values between the “Alternatives ” and “Criteria” we categorized them as:

• A1: Update IT Act with the inclusion of modern cyber threats.

ISSN:1624-1940
http://magellanes.com/

• A2: Developing focused cybercrime investigation departments
• A3: Enhancing international cooperation for the management of cybercrime.
From a closed group survey, based on the result of the respondents rated with alternate score on a scale of 1 to 10 for each criterion (with 10 being the highest score) are obtained which is presented in a Table.-1:

Table 1: Relationship Matrix of Alternatives and Criteria scores.

A (Alternatives)	**C1 (Effectiveness)**	**C2 (Cost-Efficiency)**	**C3 (Ease of Implementation)**
A1	8	5	7
A2	6	7	6
A3	7	6	8

In order to normalize the above value another Table 2 is generated showing the normalized scores obtained by multiplication of each value in the normalization matrix with the weight of each criterion.

Table 2: Relationship Matrix of Alternatives and Normalized scores.

	C1 (Effectiveness)	**C2 (Cost-Efficiency)**	**C3 (Ease of Implementation)**
A1	0.381	0.278	0.333
A2	0.286	0.389	0.286
A3	0.333	0.333	0.381

The calculated optimized value including Ratio Systems and Full Multiplicative Form Scores is obtained by summing the maximum value type of beneficial attributes for a given alternative and subtracting it from the minimum value type of non-beneficial attributes for a given alternative Ratio System (RS) Scores:
The RS method involves summing the normalized scores for each alternative across all criteria to get a composite score:

$$\mathbf{RS} = \sum \mathbf{NormalizedScores}$$

$$\text{A1: } 0.381 + 0.278 + 0.333 = 0.992$$
$$\text{A2: } 0.286 + 0.389 + 0.286 = 0.960$$
$$\text{A3: } 0.333 + 0.333 + 0.381 = 1.048$$

Full Multiplicative Form (FMF) Scores:
The FMF method involves multiplying the normalized scores for each alternative:

$$\mathbf{FMF} = \prod \mathbf{NormalizedScores}$$

$$\text{A1: } 0.381 * 0.278 * 0.333 = 0.035$$
$$\text{A2: } 0.286 * 0.389 * 0.286 = 0.032$$
$$\text{A3: } 0.333 * 0.333 * 0.381 = 0.042$$

ISSN:1624-1940
http://magellanes.com/

Figure 1. compares the Alternatives A1, A2 and A3 scores with RS Scores represented by bars. The line connecting the center points of the bar shows the FMF score (Full-Multiplicative Score), post combination of the values of RS and FMF scores, the alternatives are ranked as follows:

- A3 ranks 1st, indicating that enhancing international cooperation for cybercrime management is the most favorable option based on our criteria.
- A1 ranks 2nd, suggesting that updating the IT Act to include modern cyber threats is also a strong alternative but slightly less favored compared to A3.
- A2 ranks 3rd, meaning that establishing specialized cybercrime investigation units is considered the least favorable among the three options presented**.**

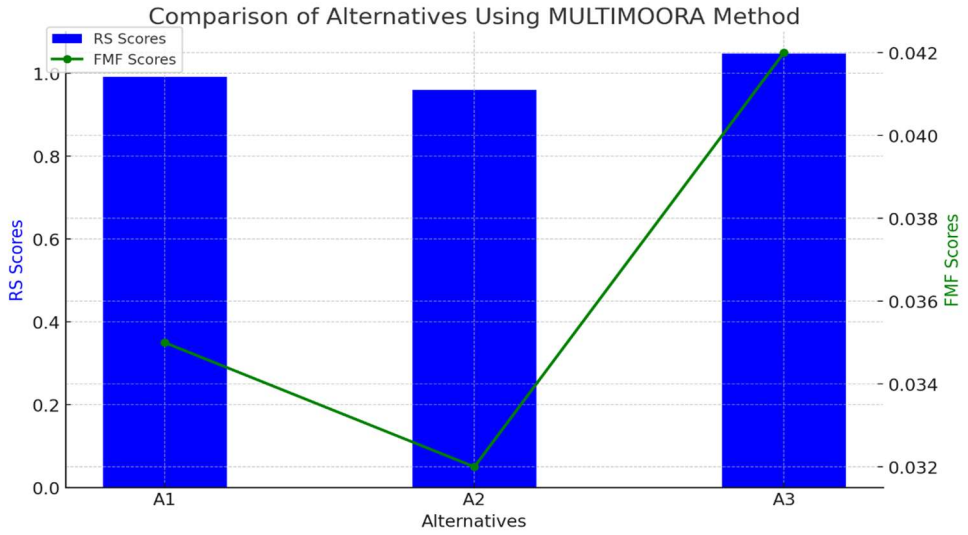

Figure 1: Alternative Selection with FMF Score

Expanding the Model Using Random Forest Algorithm for Forecasting

Data Preprocessing

In order to analyze the model author have used Random Forest Classifier using the historical data related to amendment required in Information Technology Act-2000. This is achieved by the help of finding whether the criteria C1, C2, and C3 works or not in the new environment.

Using Random Forest Classifier

The criteria variables like: C1 (Effectiveness), C2 (Cost-Efficiency), C3 (Ease of Implementation), C4 (Public Acceptance), C5 (Legal Robustness), C6 (International Cooperation) where Success is defined as (1 for successful amendment, 0 for unsuccessful amendment).Classifier analysis above is done by creating data in the CSV format using the six criteria that were chosen to indicate the success of cyber law amendments.

- C1 (Effectiveness): Shows the extent to which each amendment helps curb the act.
- C2 (Cost-Efficiency): Tests if each amendment is fiscally viable for implementation
- C3 (Ease of Implementation): Determines the feasibility of implementing every amendment
- C4 (Public Acceptability): Assesses the people's receptiveness towards every amendment

ISSN:1624-1940
http://magellanes.com/

- C5 (Legal Robustness): Demonstrates the strength and how each one can be enforced legally
- C6 (International Cooperation): Identifies every potential for international cooperation in all amendments

Generate Random Data:

For each criterion from C1 to C6, we developed a uniform distribution of random numbers between 1 and 10 to simulate different levels of performance for each amendment. This range can represent possible scores or ratings assigned to each criterion based on surveys, expert opinions, or hypothetical assessments.

Develop Target Variable (Success):

The Success variable is simulated randomly with a binary value of 0 or 1 to specify that a given amendment was successful (1) or unsuccessful (0). The probability of success was set to be 70% (p=[0.3, 0.7]), describing a greater chance that the amendments will be successful, and the difference may depend on the situation .

```
# Feature Importance
feature_importances = pd.DataFrame(rf.feature_importances_,
                                   index = X.columns,
                                   columns=['importance']).sort_values('importance', ascending=Fa
print("Feature Importances:\n", feature_importances)
```

```
Classification Report:
              precision    recall  f1-score   support

           0       0.20      0.17      0.18         6
           1       0.67      0.71      0.69        14

    accuracy                           0.55        20
   macro avg       0.43      0.44      0.44        20
weighted avg       0.53      0.55      0.54        20

AUC-ROC Score: 0.36904761904761907
Feature Importances:
     importance
C1     0.209958
C6     0.183293
C2     0.164203
C4     0.162008
C5     0.147969
C3     0.132570
```

Figure 2. Value derived for various Criteria

The above figure can be systematically analyzed by following key points under the Classification Report:

- Precision: The model predicts class 1 (successful) with good precision (0.67), meaning that 67% of predicted successes are correct. Class 0 (unsuccessful) has lower precision at 0.20.
- Recall: The model identifies 71% of the actual successful cases correctly (class 1 recall = 0.71). However, it only captures 17% of the unsuccessful cases (class 0 recall = 0.17).
- F1-Score: For class 1 (successful), the F1-score is 0.67, showing a good balance between precision and recall, whereas for class 0 (unsuccessful), it is significantly low (0.18).
- Accuracy: The overall accuracy of the model is 0.55, indicating that it correctly classifies 55% of the instances.

ISSN:1624-1940
http://magellanes.com/

- Area Under the Receiver Operating Characteristic Curve (AUC-ROC) Score[14]: The AUC-ROC score of 0.36 suggests poor separability between the classes, indicating that the model is not performing well in distinguishing between the two classes.

Feature Importances:

- The top three important features identified are:
    - C10 with an importance value of 0.220955
    - C9 with 0.207893
    - C8 with 0.181258
- These features contribute the most to the model's decision-making process, while features like C4 (0.132570) and C5 (0.132570) are less influential further enhancement can be viewed using Confusion Matrix shown in figure 3 below.

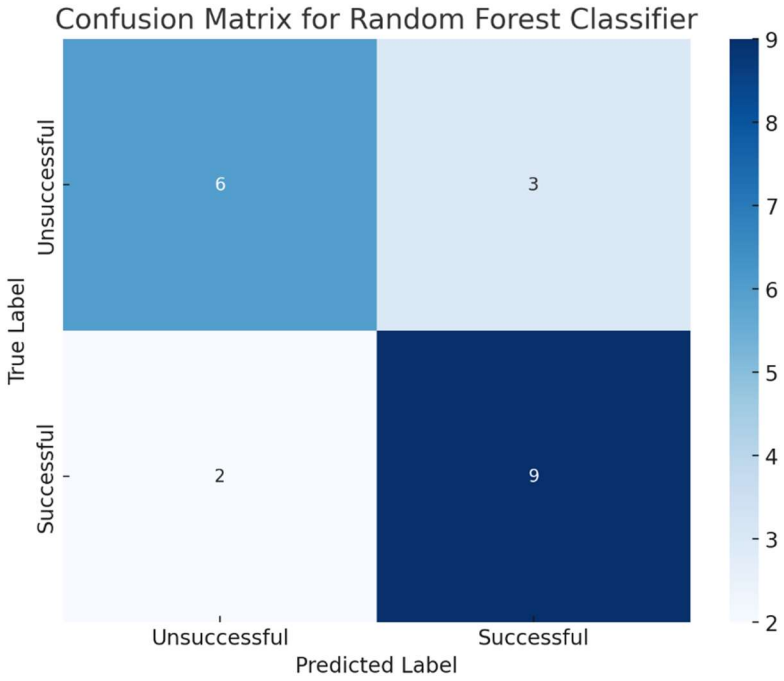

Figure 3: Confusion Matrix for Random Forest Classifier

The confusion matrix shows the performance of the Random Forest classifier by displaying the counts of predicted versus actual class labels, Table 3 represents the Confusion Matrix values where we can find the instances generated showing Predicted Values which are successful and unsuccessful.

Table 3: Confusion matrix values

	Predicted: Unsuccessful (0)	**Predicted: Successful (1)**
Actual: Unsuccessful (0)	**6** (True Negative, TN)	**3** (False Positive, FP)
Actual: Successful (1)	**2** (False Negative, FN)	**9** (True Positive, TP)

ISSN:1624-1940
http://magellanes.com/

Explanation of Each Value:

- True Negative (TN) = 6: There are 6 instances where the model correctly predicted the amendment as **unsuccessful** when it was actually **unsuccessful**.
- False Positive (FP) = 3: There are 3 instances where the model incorrectly predicted the amendment as **successful** when it was actually **unsuccessful**.
- False Negative (FN) = 2: There are 2 instances where the model incorrectly predicted the amendment as **unsuccessful** when it was actually **successful**.
- True Positive (TP) = 9:There are 9 instances where the model correctly predicted the amendment as **successful** when it was actually **successful**.

How These Values are Used:

Accuracy:$(TN + TP)/(TN + FP + FN + TP) = (6 + 9)/(6 + 3 + 2 + 9) = 15/20 = 0.75$
The model has an accuracy of 75%.

- **Precision** (for the successful class): $Precision = TP/(TP + FP) = 9/(9 + 3) = 9/12 = 0.75$ Precision is 75%, indicating that when the model predicts an amendment as successful, it is correct 75% of the time.
- **Recall** (for the successful class): $Recall = TP/(TP + FN) = 9/(9 + 2) = 9/11 \approx 0.818$ Recall is approximately 81.8%, meaning the model correctly identifies 81.8% of all actual successful amendments.
- **F1 Score**: The F1 Score can be calculated using the formula: $F1\ Score = 2 \times (Precision \times Recall)/(Precision + Recall)$

These values help assess how well the Random Forest Classifier performs in predicting successful and unsuccessful amendments.

Interpreting Results and Applying to the MULTIMOORA Method

Classification Report and AUC-ROC Score:

The classification report is used in providing metrics like precision, recall, and F1-score, which enlighten the capabilities of the model in correctly classifying successful and unsuccessful amendments. The AUC-ROC score tells which capability this model must distinguish between classes; a higher score depicts a better model.

Feature Importance:

Study of the relevance of the characteristics will determine which criteria- effectiveness, cost-efficiency, can influence the success of an amendment most. For instance, if the scores show highest for Effectiveness (C1) and International Cooperation (C6), then such factors are highly important while determining new amendments to the IT Act.

This step combines the outputs of the Random Forest analysis with the MULTIMOORA method to make the final decision. For example, if the model gives an indication that Ease of Implementation (C3)

ISSN:1624-1940
http://magellanes.com/

is not significant, one may modify the weights for the MULTIMOORA analysis such that this criterion has a smaller weight.

Scenario Analysis and Policy Recommendations:

Analyze using scenario analysis based on machine learning predictions the various possible outcomes that result from different combinations of amendments-like introducing new legality, for instance, being more co-operative internationally versus updating laws. Provide data-driven policy recommendations [13,14] to lawmakers about which amendments have had a better historical track and are most likely to be effective.

The importance is to update made precise India's legal regime pertaining to information technology, considering the rapid dynamics within the digital space and the steadily increasing complexities of cyber threats. This chapter submits a series of legislative drafts to amend the existing Information Technology Act, 2000. The amendments made here would endeavor to address shortcomings of the present regime and consider the national law aligned with current digital realities and essential constitutional rights.

Conclusion

The cyber legislation in India faces pressing needs of correction to match the current pace with which the digital landscape is changing today. The research makes known these lacunas in the Information Technology Act, 2000, that need much-needed amendment considering the emerging fears of AI-related cyber threats, deepfakes, and international cybercrimes.

The proposed amendments were objectively compared using the MULTIMOORA framework, allowing for data-driven ranking of alternatives. Strengthening international cooperation proved to be at the top of the analysis as the main recommendation since global partnership is important in fighting transnational cybercrimes. Updating the IT Act with modern cyber threats, along with the establishment of specialized cybercrime units, also proved to be significant recommendations but ranked a notch lower.

Along with the MULTIMOORA approach, the Random Forest algorithm was used in prediction concerning the possible success of the proposed amendments. Using this machine learning model provided insight into how each of these criteria—effectiveness, public acceptance, and legal enforceability—affects a probable success rate of legislative changes. Feature importance analysis from the Random Forest model points out the critical roles that international cooperation and cost efficiency play. This forces a reinforcement of their weight in the MULTIMOORA rankings.

Ultimately, the outcome would mean that reforming the IT Act is not only a legislative necessity but also a strategic imperative toward securing India's digital frontier. The infusion of computational techniques-from MULTIMOORA to machine learning-ensures that the recommendations are responsive both to national priorities and to international best practices. This is why this research emphasizes the significance of continuous legal updates, public education campaigns on increasing cyber literacy, and formulating sound data protection laws aligned with constitutional rights to ensure sustainable digital governance in India.

ISSN:1624-1940
http://magellanes.com/

References

1. Rachh A. Spatial and temporal analysis of cyber-crime cases in India. Lett Spat Resour Sci 2024;17(1):2.

2. Sudhanshu Sekhar Tripathy. A comprehensive survey of cybercrimes in India over the last decade. Int J Sci Res Arch 2024;13(1):2360–74.

3. Deepak Kumar Parewa, Deepa Mordia. Trends and Patterns: Analysing Cybercrime Statistics in India. IJFMR 2024;6(2):14522.

4. Kartshiya A amiranovich. LEGAL ASPECTS OF MODERN CYBERCRIME. LegInf [Internet] 2023 [cited 2024 Oct 21];(1). Available from: http://uzulo.su/prav-inf/pdf-jpg/pi-2023-1-st8-s083-092.pdf

5. Weijinxia ., Longchun ., Wanwei ., Zhaojing ., Duguanyao ., Yangfan . An Effective Intrusion Detection Model based on Random Forest Algorithm with I-SMOTE: [Internet]. In: Proceedings of the 23rd International Conference on Enterprise Information Systems. Online Streaming, --- Select a Country ---: SCITEPRESS - Science and Technology Publications; 2021 [cited 2024 Oct 31]. page 175–82.Available from: https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0010393801750182

6. Huang Y, Zhou X. Artificial Intelligence Random Forest Algorithm and the Application. In: Huang C, Chan YW, Yen N, editors. 2020 International Conference on Data Processing Techniques and Applications for Cyber-Physical Systems. Singapore: Springer; 2021. page 205–13.

7. Section 69 in The Information Technology Act, 2000 [Internet]. [cited 2024 Jun 3];Available from: https://indiankanoon.org/doc/1439440/

8. Hafezalkotob A, Hafezalkotob A, Liao H, Herrera F. An overview of MULTIMOORA for multi-criteria decision-making: Theory, developments, applications, and challenges. Information Fusion 2019;51:145–77.

9. Brauers WKM, Zavadskas EK. Robustness of MULTIMOORA: A Method for Multi-Objective Optimization. Informatica 2012;23(1):1–25.

10. Prasad Khamari C. Navigating Cyber Justice: Sentencing Policy Under the Information Technology Act, 2000. IJSR 2024;13(4):1444–7.

11. Osliak O, Saracino A, Martinelli F, Dimitrakos T. Towards Collaborative Cyber Threat Intelligence for Security Management: [Internet]. In: Proceedings of the 7th International Conference on Information Systems Security and Privacy. Online Streaming, --- Select a Country ---: SCITEPRESS - Science and Technology Publications; 2021 [cited 2024 Oct 31]. page 339–

ISSN:1624-1940
http://magellanes.com/

46.Available from: https://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0010191403390346

12. Jayan SD. Amendments to Information Technology Act - Is Legal System Ready to Answer Information Technology. SSRN Journal [Internet] 2010 [cited 2024 Oct 31];Available from: http://www.ssrn.com/abstract=1587902

13. Baležentis T, Baležentis A. A Survey on Development and Applications of the Multi-criteria Decision Making Method MULTIMOORA: A SURVEY ON DEVELOPMENT AND APPLICATIONS OF MULTIMOORA. J Multi-Crit Decis Anal 2014;21(3–4):209–22.

14. Hinkel G, Strittmatter M. On using Sarkar Metrics to Evaluate the Modularity of Metamodels: [Internet]. In: Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development. Porto, Portugal: SCITEPRESS - Science and Technology Publications; 2017 [cited 2024 Oct 21]. page 253–60.Available from: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006105502530260