JOSTIR Publication 2025 | ISSN: 1118-3896

Special Issue December 2025 | 458-465

Journal of Science, Technology and Innovation Research
Volume 1 Special Issue | December 2025

Evaluating Digital Security Solutions for Online Gender-Based Violence Using a Multicriteria Decision-Making Approach

*[1]Aliu F. M. and [2] Bode M. A.

[1]Elizade University, Ilara-Mokin, Ondo State, Nigeria
[2]Engineering Materials Development Institute, KM 4 Ondo Road, Akure, Nigeria

Correspondence: folasade.aliu@elizadeuniversity.edu.ng, bode.moyinoluwa@emdi.naseni.gov.ng

ABSTRACT

Digital security solutions are technologies and processes that help people stay safe online. Online gender-based violence (OGBV) is a major hindrance to online participation and security, especially among women and girls. The prevalence of cyber harassment, doxing, nonconsensual image sharing, and online stalking necessitates the urgent need for specific, gender-sensitive information security measures. The Preference ranking organization method for enrichment evaluation (PROMETHEE-II), a multi-criteria decision-making method was applied in this research to create an organized decision-support framework for evaluating and ranking possible online gender-based violence options. In order to ensure privacy, accessibility, and usability for victims and vulnerable users, five practical alternatives were chosen for evaluation: end-to-end encryption tools, AI-based content moderation systems, anonymous reporting platforms, digital literacy training programs, and emergency support applications. These alternatives were evaluated based on five factors: effectiveness, ease of use, anonymity, cost, and speed of response. The study evaluated solutions and produced a thorough rating using PROMETHEE-II, which applies preference functions and stakeholder-defined weights. The findings reveal that digital literacy awareness programs and emergency support apps had the best net flow scores of 0.160416667 and 0.045833333, demonstrating their greater capacity to strike a balance between user privacy, efficacy, and cost. The quantitative and replicable methodology used in this study can be used by policy makers, technologists, and digital rights advocates to evaluate gender-sensitive information security strategies and to rank and choose solutions that reduce OGBV and promote inclusive online safety.

Keywords: Online Gender-Based Violence (OGBV), Multi-Criteria Decision Making (MCDM), Information Security, PROMETHEE-II, Gender Equity

Introduction

Human association and interaction have been positively affected by the digital age, but it has also introduced new forms of threats, especially to girls and women. Online Gender-Based Violence (OGBV), which includes systematic abuse, doxing, bullying, cyberstalking, and non-consensual image sharing, has become a serious global issue (Almenar 2021, Ostadtaghizadeh *et al*. 2023). United Nations and World Health Organization report that one in three women has been the victim of online abuse, which immensely affects disadvantaged groups (UN 2024, WHO 2024). These infringements deter people from getting fully involved in social life, educational activities, and online spaces because such individuals are emotionally and psychologically traumatised

doi.org/10.51459/jostir.2025.1.Special-Issue.0239

(Bansal *et al.,* 2024, Dunn 2020).

Even though information security deals with the protection of confidentiality, availability, and integrity of digital systems, it is little-studied in the implementation of OGBV tools. Tools like end-to-end encryption, content-filtering and authentication mechanisms protect against common cyber threats, but frequently lack the gender-sensitive design required to address social vices (Hofstetter and Pourmalek 2023). Several multidisciplinary studies have highlighted the need for feminist and people-centred cybersecurity strategies that put an emphasis on contextual privacy, user autonomy, and inclusive design (Bansal *et al.,* 2024). Nevertheless, there are still several disjointed strategies and few frameworks for methodically evaluating their cost, inclusivity, effectiveness, and usability.

Several literatures cover a diversity of societal and technological responses to OGBV (Santos and Pourmalek 2022). The protection of digital assets is implemented by technological solutions like encryption and AI-based content monitoring such as Perspective API, which makes use of machine learning to moderate real-time digital contents and the effect on a conversation. However, such solutions face challenges like algorithmic bias and accessibility (Pasipamire 2024). For victims, emergency support applications and anonymous reporting platforms offer reactive solutions, while digital literacy awareness works to enforce proactive, self-protective behaviours. The need for thorough evaluation methods that take into account the practical choices victims may make when choosing or relying on these technologies has been emphasized by academics (Al-Alosi 2020, Barter and Koulu 2021).

Contemporary strategies to OGBV include community reporting, cybercrime laws, digital literacy awareness programs, and content moderation with secure messaging (Jahan Antara *et al.,* 2025, Setyaningsih *et al.,* 2024). Nevertheless, several frameworks for assessing these solutions based on several, frequently incompatible criteria, including usability, affordability, privacy, and effectiveness, are still lacking. Multi-criteria decision-making (MCDM) methods provide a structured approach to assist with the assessment of these solutions (Sahoo and Goswami 2023). In particular, Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE-II) uses pairwise comparisons and preference functions to enable a robust ranking of alternatives (Goswami 2020). Although it has been used in fields like cybersecurity policy (Torbacki 2021), urban planning (Babaei *et al.,* 2018), and environmental sustainability (Wątróbski 2023), its application to gender-sensitive information security is relatively under-explored.

In order to bridge this gap, this research evaluates and ranks five OGBV prevention strategies using a multi-criteria decision-making (MCDM) technique called PROMETHEE-II. This study offers a methodical, empirical method for ranking gender-sensitive cybersecurity solutions based on five criteria: effectiveness, ease of use, anonymity, cost, and response speed. Ultimately, the study contributes to a more secure and unbiased digital landscape by incorporating knowledge from gender studies, information security, and decision science to improve platform design, policy, and digital safety education.

Methodology

Multicriteria Decision Making Method

This research uses PROMETHEE-II to evaluate and rank online solutions that address gender-based violence. By computing net preference flows that account for the benefit and drawbacks of each alternative in relation to the others, PROMETHEE-II allows for the systematic comparison of options when several, frequently incompatible criteria are present (Isa *et al.,* 2021).

Selection of Alternatives

A number of possible solutions were initially identified, then thoroughly compressed based on the following inclusion criteria: namely, usability, clear relevance to OGBV, and the necessity of information

security within technological platforms. The assessment of these modern online safety and gender-based violence mitigation tools and techniques led to the identification of five practicable and attainable solutions:

End-to-end encryption (E2EE): This solution ensures safe connection and protects user data from unwanted access and interruption (Blaise *et al.,* 2021). It prevents a third party from accessing a message between a sender and a receiver during transmission.

AI-Based Content Moderation: This system recognizes and removes hostile gender-based content from the internet through machine learning (Ahmed and Khan 2024). It identifies tone and contexts of online conversations.

Anonymous Reporting Platforms: With these tools, users can report incidents without revealing their identities (Messman *et al.,* 2024).

Digital Literacy and Cyber Hygiene Training: This empowers users with the skills to identify, avoid, and report online abuse (Kostiantyn 2025).

Emergency Support Apps: These are mobile phone application programs that provide one-tap notifications and direct links to advocacy groups or crisis intervention services (Srinivasan and Dharani 2025). With these apps, users can get help on time and submit evidences of harassments without fear of being traced.

These solutions were selected because they are applicable, available, and represent both technological and educational strategies for OGBV response and deterrence.

Evaluation Criteria

Five evaluation yardsticks were identified through literature study and expert opinion, focusing on practical issues in digital safety solutions:

1. Effectiveness (C1): This describes how well an intervention can reduce or prevent OGBV. It is how well the solution can produce the desired outcome.

2. Ease of Use (C2): It describes how usable and accessible it is to all kinds of users. It is the level to which a user can make use of a tool with minimal guide or stress.

3. Anonymity (C3): It is the degree to which the user's identity is protected by the solution. It ensures that the personal information of a user is not exposed.

4. Cost (C4): This defines the financial affordability and sustainability. It is simply cost-effectiveness and simplicity of use.

5. Speed of Response (C5): This is the rate at which the solution recognizes, stops, or responds to threats.

Each criterion was assigned a weight reflecting its perceived importance, as shown in Table 1.

Table 1. Criterion Weights

Criterion	Weight
Effectiveness	0.25
Ease of Use	0.20
Anonymity	0.25
Cost	0.10
Response Speed	0.20

Alternatives were scored on a 1–5 scale for each criterion based on hybrid approach of consultations with a cybersecurity researchers, gender-right advocates, and OGBV survivors as shown in Table 2. These raw scores were then normalized using min-max normalization to ensure comparability across criteria.

Table 2. Decision Matrix

Alternatives/ Criteria	Effectiveness	Ease of use	Anonymity	Cost	Response Speed
E2EE	4	3	3	3	4
AI Content Moderation	3	4	5	4	3
Anonymous Reporting	4	4	5	5	2
Digital Literacy	5	5	3	3	3
Emergency Support	4	4	3	3	5

Promethee-II Procedure

Step 1: Standardize the decision matrix (evaluation matrix) using the formulas from equations 1 and 2.

Beneficial Criteria:

$$R_{ij} = \frac{[x_{ij} - \min(x_{ij})]}{[\quad]} \quad (i = 1,2, \dots, m; j = 1,2, \dots, n) \qquad (1)$$

Non-beneficial Criteria:

$$\acute{R}_{ij} = \frac{[\max(x_{ij}) - x_{ij}]}{[\max(x_{ij}) - \min(x_{ij})]} \qquad (2)$$

where x_{ij} is the value of each criterion, $\min(x_{ij})$ is the minimum score for each criterion, and $\max(x_{ij})$ is the maximum score for each criterion.

Step 2: Calculate the evaluation differences between the i^{th} choice and the other alternatives using equation 3.

$$D = R_{aj} - R_{bj} \qquad (3)$$

where R_{aj} is the normalized score of a criterion, a, and R_{bj} is the normalized value of a criterion, b.

Step 3: Utilizing equation 4, compute the preference function, $P_j(a, b)$.

$$P_j(a,b) = \begin{cases} 0, & \text{if } R_{aj} \leq R_{bj} \\ D, & \text{otherwise } R_{aj} > R_{bj} \end{cases} \qquad (4)$$

Step 4: As stated in equation 5, construct a function $\pi(a, b)$ that aggregates preferences.

$$\pi(a,b) = \left[\sum_{j=1}^{n} w_j P_j(a,b)\right] \Big/ \sum_{j=1}^{n} w_j \qquad (5)$$

where w_j represents the weights displayed in Table 1.
Step 5: Compute the leaving (positive) outranking flow and the entering (negative) outranking flow, φ^+ and φ^- respectively. The positive flow describes the value of preference of an alternative over the others while the negative flow describes how much all other alternatives are preferred over it. The higher the positive flow, the better. They are stated in equations 6 and 7.

$$\varphi^+ = \frac{1}{m-1}\sum_{b=1}^{m} \pi(a,b) \qquad (a \neq b) \qquad (6)$$

$$\varphi^- = \frac{1}{m-1}\sum_{b=1}^{m} \pi(b,a) \qquad (a \neq b) \qquad (7)$$

where m represents the number of options.

Step 6: Determine the net outranking flow for every alternative as expressed in equation 8.

$$\varphi(a) = \varphi^{+}(a) - \varphi^{-}(a) \quad (8)$$

Step 7: Decide which alternatives should be considered first, based on the values of φ(a).

Sensitivity Analysis

Sensitivity analysis was used to examine the consistency of the generated ranks by changing the weight values and observing the resulting net flow values and overall ranking. The stability of a ranking procedure is well understood when the criteria weights are systematically varied (Kabassi and Martinis 2021). The stability of the ranking was evaluated by varying the weights allotted to the two most important criteria. While altering any weight, modification of other weights must be done proportionately to ensure that the overall sum of weights is still exactly one.

Results and Discussion

Five selected OGBV interventions were ranked in order of performance based on five weighted criteria, using the PROMETHEE-II method. Table 3 shows the leaving flow (φ^{+}), entering flow (φ^{-}) and net preference flow (φ) values which provide a numerical basis for assessing the relative importance of each option. These values were obtained using equations 1 to 8.

Table 3. PROMETHEE-II Ranking of OGBV Solutions

	Leaving Flow	Entering Flow	Net Preference Flow	Rank
E2EE	0.135416667	0.297916667	-0.1625	5
AI Content Moderation	0.241666667	0.26875	-0.027083333	4
Anonymous Reporting	0.24375	0.260416667	-0.016666667	3
Digital Literacy	0.335416667	0.175	0.160416667	1
Emergency Support	0.227083333	0.18125	0.045833333	2

The results give basic insights into how digital security solutions can be used to reduce or prevent online gender-based violence. Among the five interventions, digital literacy performed best among the five criteria with the highest net preference flow of 0.160416667, followed by emergency support apps, with a net preference value of 0.045833333. Digital literacy equips possible victims of OGBV with skills to stay safe online through safety awareness while emergency support apps provide a platform for quick response in times of danger. On the other hand, end-to-end encryption has the lowest ranking, revealing that it is not as effective as the other OGBV solutions. The ranking of the solutions showed a mild variation as a result of the sensitivity analysis and the adjustment of the weights assigned to effectiveness and anonymity criteria. Digital literacy maintained the highest ranking, no matter the weights assigned to the 'effectiveness' criterion. This observation shows its excellent durability and stability. Increasing the weight value of effectiveness above 0.25 shifted Emergency Support Apps to the second position in the ranking, thereby declining the position of Anonymous Reporting. This can be as a result of the high ratings on effectiveness assigned to both Digital Literacy and Emergency Support Apps. The outputs of the sensitivity analysis varying the weights attributed to effectiveness are displayed in Tables 4.

In addition, a slight variation occurs the weights assigned to anonymity criterion is adjusted. The capability of digital literacy is optimized when the weighting of anonymity remains low to moderate, specifically 0.25 or less. When a weight greater than 0.25 is attributed to 'anonymity', Anonymous Reporting obtains the best ranking. The coefficient assigned to anonymity is a significant factor determining the selection of either Digital Literacy or

Table 4. Sensitivity Analysis (Varying Weights of 'Effectiveness')

Weight of Effectiveness	0.15	0.20	0.25 (Base)	0.30	0.35
Digital Literacy	1	1	1	1	1
Anonymous Reporting	2	2	2	3	4
Emergency Support	3	3	3	2	2
AI Content Moderation	4	4	4	4	3
E2EE	5	5	5	5	5

Table 5. Sensitivity Analysis (Varying Weights of 'Anonymity')

Weight of Anonymity	0.15	0.20	0.25 (Base)	0.30	0.35
Digital Literacy	1	1	1	2	2
Anonymous Reporting	3	2	2	1	1
Emergency Support	2	3	3	4	4
AI Content Moderation	4	4	4	3	3
E2EE	5	5	5	5	5

Anonymous Reporting platforms. The results of the sensitivity analysis, varying the anonymity weights are shown in Table 5.

The necessity of context-sensitive application, gender sensitivity, and user-centred design in digital security technological solutions is strengthened by these findings. Solutions that empower users, hides user identity, and give fast interventions received higher priority above those that involved algorithmic solutions. Software developers, decision makers, NGOs, and other stakeholders can structure these solutions with respect to their various needs and functions through a clear and adaptable multicriteria decision-making method such as PROMETHEE-II. This ensures equity and inclusion in efforts to promote cybersecurity.

The education of users, especially girls and women on digital literacy and secure online activities is effective in preventing cyber threats and attacks. It offers a slower intervention time but it is more economical, adaptable, and more equipping than technological tool.

Conclusion and Recommendations

This research utilized PROMETHEE-II, a multicriteria decision-making method to evaluate and classify five solutions for preventing online gender-based violence. Digital literacy and anonymous reporting platforms were discovered to be the most favourable solutions based on the methodical comparison of five relevant criteria of effectiveness, ease of use, cost, anonymity and speed of response. The weight allocated to anonymity largely determines the most important OGBV solution between Digital Literacy and Anonymous Reporting Apps. Anonymous Reporting Apps will be termed the preferable option if anonymity is the most important requirement. However, Digital Literacy stood out as the optimal solution.

The results show that deterrent, privacy-preserving, and user-empowering solutions are more user-friendly and effective to reduce the adverse consequences

of OGBV. Consequently, evidence-based and analytical choices that meet the needs of several user communities, and improve quick interventions and online safety programs are implemented by this research through a method that is flexible and reusable.

This model may be improved upon in future studies by utilizing PROMETHEE-II in various sociocultural and environmental settings, evaluating hybrid approaches, or integrating subjective data.

References

Ahmed, A. and Khan, M. (2024) *AI and Content Moderation: Legal and Ethical Approaches to Protecting Free Speech and Privacy*.

Al-Alosi, H. (2020) Fighting fire with fire: Exploring the potential of technology to help victims combat intimate partner violence. *Aggression and Violent Behavior, 52*, 101376.

Almenar, R. (2021) Cyberviolence against women and girls: Gender-based violence in the digital age and future challenges as a consequence of Covid-19. *Trento Student Law Review, 3*(1), 167-230.

Babaei, S., Ghazavi, R. and Erfanian, M. (2018) Urban flood simulation and prioritization of critical urban sub-catchments using SWMM model and PROMETHEE II approach. *Physics and Chemistry of the Earth, Parts A/B/C, 105*, 3-11.

Bansal, V., Rezwan, M., Iyer, M., Leasure, E., Roth, C., Pal, P. and Hinson, L. (2024) A scoping review of technology-facilitated gender-based violence in low-and middle-income countries across Asia. *Trauma, Violence, & Abuse, 25*(1), 463-475.

Barter, C. and Koulu, S. (2021) Digital technologies and gender-based violence–mechanisms for oppression, activism and recovery. *Journal of gender-based violence, 5*(3), 367-375.

Blaise, O. O., Awodele, O. and Yewande, O. (2021) An Understanding and Perspectives of End-To-End Encryption. *Int. Res. J. Eng. Technol.(IRJET), 8*(04), 1086.

Dunn, S. (2020) Technology-facilitated gender-based violence: An overview.

Goswami, S. S. (2020) Outranking methods: Promethee i and promethee ii. *Foundations of Management, 12*(1), 93-110.

Hofstetter, J.-S. and Pourmalek, P. (2023) *Gendering Cybersecurity through Women, Peace and Security: Designing Conflict-Sensitive Strategy Documents at the National Level*.

Isa, M. A. M., Saharudin, N. S., Anuar, N. B. and Mahad, N. F. (2021) The application of AHP-PROMETHEE II for supplier selection. in *Journal of Physics: Conference Series*: IOP Publishing. pp. 012062.

Jahan Antara, I., Sultan, M., Novelly, S. N. and Islam, M. (2025) Countering Online Gender-Based Violence: Cyber Security or State Security and the Dilemmas of Policy Engagement.

Kabassi, K. and Martinis, A. (2021) Sensitivity Analysis of PROMETHEE II for the Evaluation of Environmental Websites. *Applied Sciences, 11*(19), 9215.

Kostiantyn, Z. (2025) Cyber hygiene in the context of digital transformation in higher education: challenges and opportunities. in *The 5th International scientific and practical conference "Problems of students in universities and new ways of solving them"(February 04–07, 2025) Paris, France. International Science Group. 2025. 245,* 174.

Messman, E., Heinze, J., Hsieh, H.-F., Hockley, N., Pomerantz, N., Grodzinski, A., Scott, B., Goldstein, N. and Zimmerman, M. (2024) Anonymous reporting systems for school-based violence prevention: A systematic review. *Health Education & Behavior, 51*(1), 62-70.

Ostadtaghizadeh, A., Zarei, M., Saniee, N. and Rasouli, M. A. (2023) Gender-based violence against women during the COVID-19 pandemic: recommendations for future. *BMC women's health, 23*(1), 219.

Pasipamire, N. (2024) Navigating algorithm bias in AI: ensuring fairness and trust in Africa. *Frontiers in Research Metrics and Analytics, 9*.

Sahoo, S. K. and Goswami, S. S. (2023) A comprehensive review of multiple criteria decision-making (MCDM) Methods: advancements, applications, and future directions. *Decision Making Advances, 1*(1), 25-48.

Santos, A. F.-D. and Pourmalek, P. (2022) Preventing violence in

the digital age: Women peacebuilders and technology-facilitated gender-based violence. *GENDER-BASED VIOLENCE, 71*.

Setyaningsih, R., Santoso, D. H. and Nurwahid, A. F. (2024) Digital Literacy of Social Media Users in Preventing Online Gender-Based Violence in Indonesia. *Journal of Ecohumanism, 3*(8), pp. 5886-5894.

Srinivasan, S. and Dharani, S. (2025) Women Safety Android Application.

Torbacki, W. (2021) A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. *Sustainability, 13*(16), 8833.

UN (2024) *One in three women experiences gender-based violence*, Available: https://news.un.org/en/story/2024/11/1157046 [Accessed 04/06/2025 2025].

Wątróbski, J. (2023) Temporal PROMETHEE II—New multi-criteria approach to sustainable management of alternative fuels consumption. *Journal of Cleaner Production, 413*, 137445.

WHO (2024) *Violence against women*, Available: https://www.who.int/news-room/fact-sheets/detail/violence-against-women [Accessed 04/06/2025 2025].