frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 11 November 2024
DOI 10.3389/fcomp.2024.1389223

Check for updates

OPEN ACCESS

EDITED BY
Martin Shepperd,
Brunel University London, United Kingdom

REVIEWED BY
Lidia Fotia,
University of Salerno, Italy
Cheng Yunlong,
Chongqing University of Posts and Telecommunications, China

*CORRESPONDENCE
Olorunjube James Falana
✉ falanaoj@funaab.edu.ng
Amjad Alsirhani
✉ amjadalsirhani@ju.edu.sa

RECEIVED 21 February 2024
ACCEPTED 20 September 2024
PUBLISHED 11 November 2024

CITATION
Falana OJ, Ojeaga T, Naeem H, Aborisade DO, Alsirhani A and Alserhani F (2024) FHG-PR: a hybridized fuzzy-AHP and game theory model for assessing privacy risk on social media platforms.
Front. Comput. Sci. 6:1389223.
doi: 10.3389/fcomp.2024.1389223

COPYRIGHT
© 2024 Falana, Ojeaga, Naeem, Aborisade, Alsirhani and Alserhani. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

FHG-PR: a hybridized fuzzy-AHP and game theory model for assessing privacy risk on social media platforms

Olorunjube James Falana[1]*, Trust Ojeaga[1], Hamad Naeem[2], Dada Olaniyi Aborisade[1], Amjad Alsirhani[3]* and Faeiz Alserhani[3]

[1]Department of Computer Science, Federal University of Agriculture, Abeokuta, Ogun State, Nigeria, [2]Department of Computer Science, College of Computer Sciences and Information Technology (CCSIT), King Faisal University, Al-Ahsa, Saudi Arabia, [3]College of Computer and Information Sciences, Jouf University, Sakaka, Aljouf, Saudi Arabia

Social media platforms have become integral to our daily lives, enabling global connectivity and interaction. Current research provides general solutions for mitigating privacy risks, but it does not focus on particular platforms. However, the voluntary sharing of personal information on these platforms presents considerable privacy risks, highlighting the need for effective risk assessment mechanisms. This study presents a hybrid approach that uses the fuzzy Analytical Hierarchy Process (AHP) and game theory to estimate privacy risks on Meta and X. We used a fuzzy AHP to rank determinant variables based on surveys of social media users and professionals. These weighted criteria were then used in a Multi-Criteria Decision-Making (MCDM) framework using cooperative game theory to discover ways to lower privacy hazards. The model accurately analyzed the privacy threats on Meta and X, recommending alternate techniques for preventing breaches in data privacy. The cooperative game theory method allows stakeholders to collaborate on creating privacy-preserving measures. The findings emphasize the model's ability to address platform-specific privacy threats, as well as its flexibility in other social media settings. The model's potential for real-world application is demonstrated by its ability to provide practical risk reduction measures, which improve privacy protection for social media users.

KEYWORDS

sensitive data, social media, privacy, Analytical Hierarchy Process, game, risk

1 Introduction

Social media platforms have changed the way and manner in which people communicate and interact in their day-to-day activities. Despite the numerous advantages and features that these platforms provide, their massive data collecting and management practices have prompted serious privacy issues. This dilemma has generated the need for strong privacy protection rules and measures (Janssen et al., 2020). This complex issue has resulted in several privacy challenges and advocates for the need to develop privacy-protecting regulations (Kavianpour et al., 2019).

Social media networks collect large quantities of user data, such as personal interests, online behaviours, and comprehensive personal information. This data, often collected without explicit user consent, is used for targeted advertising and shared with third parties, exacerbating privacy risks (Pensa and Di Blasi, 2017).

The rise of artificial intelligence has further intensified these concerns, as AI tools increasingly rely on social media data for training and improvement, sometimes without adequate user consent

(Wiggers, 2023). Previous research has explored various privacy protection mechanisms, such as systems enhancing user control over data (Janssen et al., 2020); privacy threat models that improve information security (Weiss, 2009), and privacy risk analysis using data-driven techniques like sentiment analysis (Saura et al., 2022). However, these approaches often fail to address the complexities and uncertainties specific to different social media platforms. Recent studies have made significant strides in developing privacy risk assessment models, but a focused evaluation of platforms like Meta (formerly Facebook) and X (formerly Twitter) remains lacking (Ahvanooey et al., 2023).

This study aims to close this gap by addressing the following research question: How can we create a comprehensive framework for assessing and mitigating privacy risks on major social media platforms, specifically Meta and X, given the complex and dynamic nature of user data interactions and privacy threats? To address this challenge, a comprehensive privacy risk assessment framework for Meta and X, a hybridised Fuzzy Analytic Hierarchy Process (Fuzzy-AHP), and a cooperative game theory-based Multi-Criteria Decision-Making (MCDM) framework are developed. The research also aims to provide an accurate assessment of privacy risks based on Multi-criteria Decision Making as well as analyse different risk mitigation measures. This work is critical for furthering the present state of study in social media privacy and providing practical solutions for protecting user data on these sites.

The rest of the paper is organized as follows: Section 2 presents background knowledge of privacy risks and related works. Section 3 introduces related works like fuzzy AHP and game theory. Section 4 describes the methodology. Section 5 shows the implementation and describes the experimental analysis. Section 6 debates the practical implications of the research taken for cooperative management areas and lists the limitations of the study.

2 Background and related work

Social media platforms have become an inseparable part of contemporary society, enabling communication and socialisation. The wide acceptability of social media has raised concerns about privacy issues and data protection. This literature review outlines the research related to privacy threats on social media platforms.

2.1 Privacy risks in social media platforms

Privacy and confidentiality are distinct concepts, but they are interconnected. Privacy is the ability to disclose personal information to chosen individuals, while confidentiality is the absolute secrecy of information. People may choose to keep their phone numbers private or list them in a do-not-call registry. There may be differences in perceptions between how information is released in the actual and virtual worlds. According to a study, Social media may be influencing how people see online privacy (Shullich, 2011).

These days, identity theft and impersonation pose a serious threat to privacy on SM. For modern organizations, protecting customer identification is crucial, and part of that responsibility includes teaching consumers how to be secure online and prevent identity theft (AlMudahi et al., 2022; Anderson and Agarwal, 2010). Privacy risk assessments in SM are very essential in building user trust and confidence because they help to safeguard user data and platforms (Cheng et al., 2017; Paliszkiewicz and Koohang, 2016).

2.2 Related work

Research has explored various strategies to address security concerns in decision-making contexts, including the use of fuzzy-AHP and game theory to tackle multi-criteria decision-making (MCDM) challenges. Ahvanooey et al. (2023) used cybersecurity experts to assess privacy risk on social media platforms, providing strategic alternatives for enhancing privacy in the public, commercial, and governmental spheres.

2.2.1 Fuzzy Analytical Hierarchy Process (AHP)

Decision-making, especially in multi-criteria situations, is picking the best option from a group of options based on predetermined criteria. It is critical in collective decision-making to define these criteria before analysing and awarding judgment scores. The Analytic Hierarchy Process (AHP) is a well-known multi-criteria decision-making (MCDM) technique that generates ratio scales through pairwise comparisons, allowing decision-makers to evaluate both tangible and intangible aspects (Saaty, 2010). While AHP is commonly used for calculating priorities, it has certain drawbacks in dealing with the subjectivity and ambiguity inherent in decision-making processes, especially when the choice incorporates ambiguous or inaccurate information.

To overcome these constraints, Laarhoven and Pedrycz (1983) were the first to expand AHP by using fuzzy set theory, resulting in the Fuzzy-AHP (FAHP). Their methodology introduced the use of triangular fuzzy numbers to express subjective judgements, providing a more subtle method of dealing with ambiguity in comparisons. However, their solution was restricted by the complexities of determining ambiguous priorities. Buckley (1985) built on Laarhoven and Pedrycz's work by employing trapezoidal fuzzy numbers for prioritisation, enhancing the use of fuzzy logic in decision-making. Buckley's suggestion made the approach more useful in situations when judgements were very ambiguous. However, the fuzzy priorities obtained were not crisp enough for many actual applications, resulting in uncertainty in the outcomes.

To address this, Chang (1996) proposed a novel method for producing crisp priority vectors from fuzzy judgements, resulting in a crisper, more definitive output. Chang's work was a huge step forward in making Fuzzy-AHP more useful for real-world decision-making situations by minimising the ambiguity of the generated priorities. Buckley et al. (1999) later merged fuzzy logic with AHP approach to create Fuzzy-AHP, which generalizes the computation of the constant ratio into a fuzzy matrix and resulting in a more accurate weight (Buckley et al., 2001; Xu and Liao, 2013; Zhu, 2014).

Recent research, such as Ahvanooey et al. (2023) and Peng et al. (2021), have sought to solve these concerns by offering more efficient fuzzy weight calculation techniques and enhancing fuzzy judgement consistency. Despite these advancements, further research is required to streamline the process and make it more adaptive to complex decision-making contexts, such as those involving privacy issues on social media platforms, where ambiguity and inaccurate data are widespread (Sur et al., 2020; Zhü, 2014).

Abbreviations: TFN, Triangular Fuzzy Number; FPCM, Fuzzy Pairwise Comparison Matrix; SD, Sensitive Data; SM, Social media; MCDM, Multi criteria Decision Making; P, Player; S, Strategy; PF, Play-off; C, Criteria; SC, Subcriteria; CI, Consistency Index; Consistency Ratio, Consistency Ratio.

2.2.2 Game theory

Game theory is used to analyse player behaviour in decision-making processes, notably cooperation and competition. It provides a systematic framework for evaluating strategic options and optimising results (Ahvanooey et al., 2023; Do et al., 2017). Ahvanooey et al. (2023) used cybersecurity specialists to assess privacy risks and provide strategic engagement methods for several management sectors. They created a model that used Fuzzy-AHP and cooperative game theory to better strategic information management in three critical sectors: industrial (developers), social (users), and government (inspectors). The Fuzzy-AHP component was utilised to establish the relative relevance of various criteria, which then fed into the game theory framework for evaluating interactions between these sectors. This combination strategy provided insights into decreasing privacy threats by modelling the strategic behaviour of different stakeholders.

Despite its unique technique, Ahvanooey et al.'s (2023) study included some significant limitations. One significant drawback was the lack of a thorough examination of two prominent social media sites, X and Meta, which are essential to contemporary privacy problems. Furthermore, the study failed to include the hazards posed by third-party marketers, who are becoming an increasingly prominent role in the privacy environment (Bouke et al., 2023). Addressing these gaps is critical to fully comprehending the larger ecosystem of privacy issues in social media.

2.2.3 Privacy risks in social media platforms

Several recent research have made major contributions to detecting and analysing privacy threats on social media sites. Alemany et al. (2019) used criteria like audience size and reachability to estimate privacy hazards associated with network topologies and data flows. Their study established a systematic technique for quantifying risk, but it was largely concerned with network-centric concerns, leaving other social factors untouched. Karusala et al. (2019) addressed the privacy difficulties confronting women in patriarchal countries, emphasising the significance of cultural and gender variables in influencing privacy concerns. Their findings highlighted the importance of more inclusive privacy models that account for social and cultural differences.

Such and Criado (2018) established the notion of multiparty privacy, which is crucial in social media since user data is shared. This research emphasised that privacy is frequently jeopardised when several users engage with shared material, offering the potential for additional investigation into how social media platforms might handle such complexity. More recently, Rivadeneira et al. (2023) investigated user-centric privacy models inside the Internet of Things (IoT) framework and recommended strong consent management techniques to reduce privacy threats. While their research provides useful insights, its relevance to social media platforms warrants more investigation, especially in settings where consent is frequently implicit or concealed.

2.2.4 User perceptions and attitudes

Understanding users' attitudes towards privacy is critical for building successful privacy protection methods. Jacobson et al. (2020) discovered that consumers' comfort with social media marketing is strongly related to their view of the risks and advantages. Their findings suggest that consumers may tolerate some privacy violations provided they see a comparable advantage, but the study did not look into how these perceptions differed between demographic groups or geographies.

Koohang et al. (2018) expanded the subject by creating a research model that connects consumers' privacy concerns to their risk and trust perceptions. They found a striking link between perceived privacy issues and consumers' trust in social media networks. However, their findings raise unsolved issues about how platforms might re-establish confidence after it has been lost, particularly following data breaches or privacy scandals. More study is needed to better understand the dynamics of trust restoration and how different user groups respond to privacy infractions.

2.2.5 Privacy-preserving technologies and solutions

In reaction to increased privacy concerns, several privacy-preserving methods have been developed. Lockl et al. (2023) investigated the possibility of self-sovereign identities (SSIs) to provide users with greater control over their personal data. Their research showcased the prospect of SSIs, but there are still issues with scalability and widespread adoption.

Dikshit et al. (2023) examined developing technologies such as private relays and encrypted DNS solutions, highlighting their importance in protecting user data. However, they also stated that these solutions have not yet been broadly implemented and face opposition from some service providers, making comprehensive privacy protection challenging.

García-Rodríguez et al. (2024) proposed biometric-bound attribute-based credentials (bb-ABC) to increase security and privacy. These credentials connect biometric data to attribute-based access control, adding an additional layer of security. Despite this improvement, deploying such systems in large-scale, real-world settings remains difficult, and further research is required to solve implementation challenges.

Furthermore, Choi et al. (2020) studied whether blockchain-enabled social media (BSM) systems might solve privacy concerns while boosting social media analytics. Their research found that, while BSM systems have the ability to improve data security and analytics accuracy, they confront challenges such as data privacy violations and assuring the integrity of analytics operations. The challenges of handling correct, privacy-preserving data in the supply chain continue to be a barrier to widespread adoption.

Hiwale et al. (2023) did comprehensive research on the function of federated learning and blockchain in improving the privacy of telemedicine platforms. They highlighted the collaborative concept of federated learning and the immutability of blockchain in protecting patient data. However, problems like as high computing costs and technological interaction with current systems must be overcome before these technologies can be scaled effectively.

Together, these investigations shed light on the development of the suggested privacy risk assessment system. By combining Fuzzy-AHP and game theory, the framework seeks to solve the specific issues given by current social media platforms like Meta and X, notably in addressing privacy concerns involving various parties and sources of uncertainty.

3 Methodology

The proposed FHG-PR framework combines the Fuzzy-AHP method with game theory to assess privacy risks on social media platforms. The approach is divided into four phases: data collection, frequency analysis, pairwise comparison and game theory, as shown in

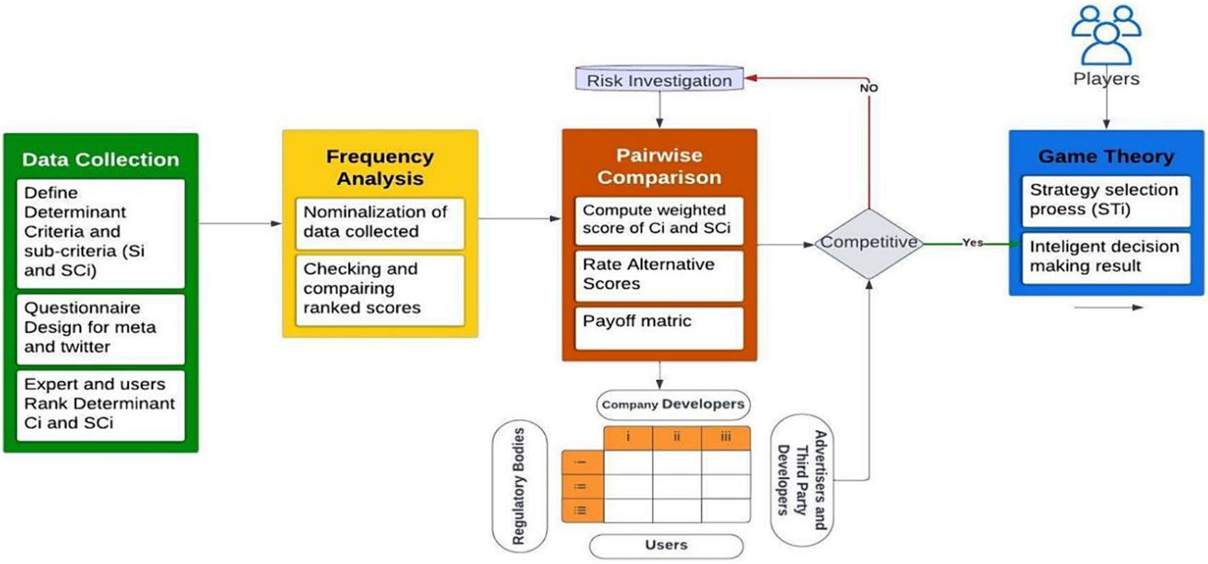

Data Collection
Define Determinant Criteria and sub-criteria (Si and SCi)
Questionnaire Design for meta and twitter
Expert and users Rank Determinant Ci and SCi
Frequency Analysis
Nominalization of data collected
Checking and compairing ranked scores
Risk Investigation
Pairwise Comparison
Compute weighted score of Ci and SCi
Rate Alternative Scores
Payoff matric
NO
Competitive
Yes
Players
Game Theory
Strategy selection proess (STi)
Inteligent decision making result
Company Developers
Regulatory Bodies
i
ii
iii
i
ii
iii
Users
Advertisers and Third Party Developers

FIGURE 1
The general architecture of FHG-PR.

Figure 1. Fuzzy-AHP is useful in overcoming the inherent subjectivity and ambiguity in decision-making by using fuzzy logic. This technique enables more flexible and refined decisions when prioritising privacy risk criteria. Privacy problems, especially in the context of social media, are frequently unclear and complicated. Fuzzy-AHP successfully tackles ambiguity by combining ambiguous and imprecise data, which are typical in circumstances involving social media platforms (Kubler et al., 2016; Ashour and Mahdiyar, 2023). It guarantees that privacy concerns are evaluated systematically, and data-driven, allowing for the ranking of criteria even when the data is imprecise.

On the other hand, game theory simulates the strategic interactions of numerous stakeholders, including users, platform developers, third-party developers, and regulators, all of which may have competing interests in privacy management. Game theory focuses on reaching optimum solutions through collaboration or competition, making it very useful in multi-party decision-making contexts such as platform privacy risk management (Rass and Schauer, 2018). Game theory allows for assessing strategic decisions and proposing strategies that match each entity's diverse objectives by accounting for different stakeholders' cooperative and competitive behaviours. By using the game theory, we can examine all the possible combinations of alternative decisions taken by each stakeholder (P^i). The prioritised weights obtained by Fuzzy-AHP serve as payoff values inside the game theory framework, allowing us to interpret each stakeholder's degree of desire and estimate privacy risks accordingly.

3.1 Data collection

To assess privacy risks on Meta and X, we identified critical factors influencing privacy invasion. We gathered information from privacy policy sites, API documentation, and literature reviews from cybersecurity experts. Key criteria (C_i) and sub-criteria (SC_i) were prioritized through surveys involving social media users and professionals. A questionnaire was created and posted on the LinkedIn, X, and Facebook platforms. The questionnaire was designed to target Cybersecurity experts and X users who will be asked to assign linguistic terms (e.g., 5-point Likert scale) by considering the relation of Triangular Fuzzy Numbers (TFNs) to pairwise comparisons for all C_i/SC_i through the dimension of a hierarchy system. Triangular Fuzzy Numbers (TFNs) are a type of fuzzy number that is represented as a triplet (lower limit, frequent value, upper limit). TFNs are used to represent uncertainty in decision-making processes. They are especially valuable in Fuzzy-AHP for reflecting experts' subjective judgements more flexibly and realistically.

We define the infringement of privacy of users' sensitive data in social media as Multi Criteria Decision Making (MCDM) problem involving a collection of players $P^i = \{P^1, P^2, P^3, P^4\}$ as shown in Table 1. There are four major players:

i Company Developers: This is the social media (SM) platform and the organization that supports it. To prevent misuse, developers must prioritize user consent in data acquisition and properly manage third-party access.

ii Users: This includes Individuals, corporations, media outlets, celebrities, government figures, non-profit organizations, researchers, academics and Bot accounts are all examples of SM users. They utilize SM platforms for a variety of purposes, including opinion sharing, news updates, product promotion, interacting with followers, engaging in public discussions, and publicizing research findings. It is critical to consider the varied viewpoints and interests of SM users when doing a privacy risk assessment.

iii Regulatory bodies: Regulatory bodies play an important role in assessing the privacy risks of SM platforms. They are governmental or non-governmental entities charged with enforcing privacy laws and regulations. The Federal Trade

TABLE 1 Parameters used for determining the privacy invasion risks of users' sensitive data on the SM and their interactions with the players.

Category of P^i	Criteria C_i		Sub-criteria SC_i	
Company developers	C_1	Transparency on data security, privacy policy and Ad targeting	SC_1	Measures against data breach and incident response protocol they use
			SC_2	Transparency in data practice and privacy update frequency
			SC_3	Extent to which user data is being used for personalized advertising
Users	C_2	Users control over the spread and use of their data	SC_4	Users' knowledge over their account security features and encryption protocols
			SC_5	Users' knowledge over data sharing & visibility and clear consent mechanism
			SC_6	User's willingness to report privacy invasion and its consequences on their life
Regulatory bodies	C_3	Companies' compliance to privacy policies and data sharing.	SC_7	Regulatory bodies' concern regarding ensuring adequate security measures to protect user data
			SC_8	Regulatory bodies' practice in privacy transparency requirement considering international laws
			SC_9	Regulatory bodies' knowledge regarding user's privacy invasion report authentication on SM platform
Third-party developers & advertisers	C_4	Considerations for terms and condition accessing users' data on the platform	SC_{10}	Third-party developers' knowledge on the scope of user data access through platform's Application programming interface (API)
			SC_{11}	Advertisers' awareness on the availability of user's data for marketing and business purposes
			SC_{12}	Compliance with the platform's policies and data usage disclosures

Commission (FTC) in the United States, the European Data Protection Board (EDPB) in the EU, the Information Commissioner's Office (ICO) in the United Kingdom, and the Nigeria Data Protection Commission (NDPC) in Nigeria are some significant examples. These organizations monitor and enforce compliance with data protection regulations, investigate privacy violations, and guarantee the platform's user data is secure. Their actions and directives have a significant impact on the privacy policies and practices of SM platforms, making them critical participants in the platform's overall privacy risk assessment.

iv Third-party developers & advertisers: Advertisers and third-party developers, in particular (Meta and X), are major participants in the SM platform's privacy risk evaluation because of their direct engagement in collecting user data and exploiting it for marketing and app development objectives. To maintain user privacy and data security, their access to and use of user data must be rigorously regulated and matched with the SM platform's privacy policies. Company developers, users, regulatory bodies, and third-party developers and advertisers, i.e., each P^i belongs to an independent management sector.

3.2 Fuzzy-AHP

The fuzzy-AHP method helps determine each criterion's weight based on survey responses. This process involves frequency analysis and pairwise comparisons, where participants rate the importance of each factor using a fuzzy scale. The collected data is then processed to calculate the relative weights of the criteria, reflecting their importance in privacy risk assessment.

3.2.1 Frequency analysis

After prioritizing C_i/SC_i, a frequency analysis is done to normalize the ranked scores as detailed in Tables 2, 3. Note that the Likert scale serves as the basis for Triangular Fuzzy Numbers (TFNs), which are as follows: Influential (9), Very Influential (7), Essentially Influential (5), Moderate Influential (3), and Slightly Influential (1).

3.2.2 Fuzzy-pairwise comparison

Compute FPCM by computing priority weights for C_i/SC_i based on the frequency analysis of gathered scores using the fuzzy-AHP model proposed by Chang (1996).

Let $V = \{v_1,v_2,\ldots,v_n\}$be a set of objects for FPCMs related to C_i/SC_i and $U = \{u_1,u_2,\ldots,u_n\}$ be a goal set for each category. The extent analysis approach proposed by Chang (1996) calls for taking each item and doing an extent analysis for each goal, g_i in turn. Consequently, extent analysis values m are acquired for every item shown in Equation 1

$$M_{gi}^{1}, M_{gi}^{2}, \ldots, M_{gi}^{m}, i = 1,2,3,\ldots,n \tag{1}$$

Such that $M_{gi}^{j}\left(j = 1,2,3,..,m\right)$ are TFNs, as shown in Table 4. We adopt the four steps in Chang (1996) extent analysis for each goal:

Step 1: Fuzzy synthetic extent's value S_i with relation to *ith* object is defined using Equation 2:

$$S_i = \sum_{j=1}^{m}\left(M_{gi}^{j}\right) \otimes \left[\sum_{i=1}^{n}\sum_{j=1}^{m}\left(M_{gi}^{j}\right)\right]^{-1} \tag{2}$$

Such that $\sum_{j=1}^{m} M_{gi}^{j}$ is computed using the m extent analysis of a specific matrix by performing the fuzzy addition operation as detailed in Equation 3:

$$\sum_{j=1}^{m} M_{gi}^{j} = \left(\sum_{j=1}^{m} l_i, \sum_{j=1}^{m} m_i, \sum_{j=1}^{m} u_i\right) \tag{3}$$

Note that in Equation 2, the $\left[\sum_{i=1}^{n}\sum_{j=1}^{m} M_{gi}^{j}\right]^{-1}$ is calculated by addition and inverse operations. Following this, Equation 4 computes the inverse operation:

$$\left[\sum_{i=1}^{n}\sum_{j=1}^{m} M_{gi}^{j}\right]^{-1} = \left(\frac{1}{\sum_{i=1}^{n} u_i}, \frac{1}{\sum_{i=1}^{n} m_i}, \frac{1}{\sum_{i=1}^{n} l_i}\right) \tag{4}$$

Step 2: Both x_1 and x_2 are TFNs, therefore the degree of possibility of $x_2 = \left(x_{l2}, x_{m2}, x_{u2}\right) \geq \left(x_{l1}, x_{m1}, x_{u1}\right)$ defined in Equation 5:

$$\beta = \sup\left[\min\left(\mu_{x_1}, \mu_{x_2}\right] = hgx\left(x_1 \cap x_2\right)\right). \tag{5}$$

Where $hgx\left(x_1 \cap x_2\right) = \mu_{x_2(\gamma)}$ such that γ is the highest intersection point between μ_{x_1} and μ_{x_2}. Therefore, x_1 and x_2 can only be ascertained if the requirements $\beta_1\left(,x_2 \geq x_1\right)$ and $\beta_2\left(,x_2 \geq x_1\right)$ are met.

β represents the degree of possibility, which is calculated to evaluate the extent to which one fuzzy number is greater than or equal to another.

Supremum (sup): This is the smallest value that is greater than or equal to every value in a set.

hgx refers to the height of the greatest intersection.

hgx($x_1 \cap x_2$): represents the membership value of the intersection of two fuzzy sets x_1 and x_2. It is used to determine the possibility that one fuzzy number is greater than or equal to another.

TABLE 2 Fuzzy extent analysis for X platform.

FPCM for related to C_{1-4} category classification.					
	C_1	C_2	C_3	C_4	Priority weight
C_1	(1, 1, 1)	(1, 1.5, 2)	(0.5, 0.6, 1)	(1.5, 2, 2.5)	0.2892
C_2	(0.5, 0.6, 1)	(1, 1, 1)	(0.4, 0.5, 0.6)	(0.5, 0.6, 1)	0.1577
C_3	(1, 1.5, 2)	(1.5, 2, 2.5)	(1, 1, 1)	(1.5, 2, 2.5)	0.3612
C_4	(0.4, 0.5, 0.6)	(1, 1.5, 2)	(0.4, 0.5, 0.6)	(1, 1, 1)	0.1919
$\lambda_{\max} = 4.0373$, CI = 0.0124 CR = 0.0138, $\in_r = 0.0675$.					

Step 3: The convex TFN value x_1 are then computed using Equation 6:

$$\beta\left(x \geq x_1, x_2, x_3, \ldots, x_n\right) = min\beta\left(x \geq x_i\right). \tag{6}$$

Such that $\left(i = 1,2,3,..,k\right)$ assume that $d^{'}\left(x_i\right) = min\beta\left(x \geq x_k\right)$ when $k = 1,2,3,\ldots,n; k \neq i$.

Consequently, the weight vector for each v_i is derived through Equation 7:

$$W^{'} = \left(d^{'}\left(x_1\right), d^{'}\left(x_2\right), d^{'}\left(x_3\right), \ldots, d^{'}\left(x_n\right)\right)^{x} \tag{7}$$

Such that $X_i\left(1,2,3,..,n\right)$ are n elements.

Step 4: After normalization and conversion of TFNs to non-fuzzy numbers. Equation 8 outlines the process of obtaining the nomalized weight vectors:

$$W = \left(d\left(x_1\right), d\left(x_2\right), d\left(x_3\right), \ldots, d\left(x_n\right)\right)^{x} \tag{8}$$

To ensure the correctness of the derived weights for Fuzzy Pairwise Comparison Matrices (FPCMs), the Consistency Ratio (CR) must be determined. If the CR is less than 0.10, it means that the FPCMs are consistent. However, if the CR exceeds this level, the pairwise comparison procedure for each ranking based on linguistic norms must be redone and recalculated until the CR falls below acceptable limits. The graded mean integration approach is used to calculate the CR by converting the TFN = (x_{li}, x_{mi}, x_{ui}), of v_i in the FPCMs to the appropriate crisp value Q_{cv} as shown in Equation 9:

$$Q_{cv} = \left[\frac{4x_l + x_m + x_u}{6}\right] \tag{9}$$

After obtaining Q_{cv} we utilize Equations 10–13 to get the values of $\lambda_{\max}$, CI, CR, and $\dot{\partial}_r$.

Saaty (2010) developed the Consistency Index (CI) and the Consistency Ratio (CR) to assess inconsistency in Fuzzy-AHP models.

TABLE 3 Fuzzy pairwise comparison matrix for subcriteria.

FPCM for related to SC_{1-3} category classification				
	SC_1	SC_2	SC_3	Priority weight
SC_1	(1, 1, 1)	(2, 2.5, 3)	(2, 2.5, 3)	0.5439
SC_2	(0.3, 0.4, 0.5)	(1, 1, 1)	(0.5, 0.6, 1)	0.1887
SC_3	(0.3, 0.4, 0.5)	(1, 1.5, 2)	(1, 1, 1)	0.2674
$\lambda_{\max} = 3.0142$, CI = 0.0071, CR = 0.00122, $\varepsilon_r = 0.0387$				

FPCM for related to SC_{4-6} category classification				
	SC_4	SC_5	SC_6	Priority weight
SC_4	(1, 1, 1)	(0.3, 0.4, 0.5)	(0.3, 0.4, 0.5)	0.1593
SC_5	(2, 2.5, 3)	(1, 1, 1)	(1, 1.5, 2)	0.4597
SC_6	(2, 2.5, 3)	(0.5, 0.6, 1)	(1, 1, 1)	0.3810
$\lambda_{\max} = 3.0167$, CI = 0.0083, CR = 0.0144, $\in_r = 0.0387$				

FPCM for related to SC_{7-9} category classification				
	SC_7	SC_8	SC_9	Priority weight
SC_7	(1, 1, 1)	(1.5, 2, 2.5)	(1.5, 2, 2.5)	0.4929
SC_8	(0.4, 0.5, 0.6)	(1, 1, 1)	(1, 1.5, 2)	0.2957
SC_9	(0.4, 0.5, 0.6)	(0.5, 0.6, 1)	(1, 1, 1)	0.2114
$\lambda_{\max} = 3.0128$, CI = 0.0064, CR = 0.0111, $\in_r = 0.0387$				

FPCM for related to SC_{10-12} category classification				
	SC_{10}	SC_{11}	SC_{12}	Priority weight
SC_{10}	(1, 1, 1)	(2.5, 3, 3.5)	(0.3, 0.4, 0.5)	0.3509
SC_{11}	(0.2, 0.3, 0.4)	(1, 1, 1)	(0.2, 0.3, 0.4)	0.1270
SC_{12}	(2, 2.5, 3)	(2.5, 3, 3.5)	(1, 1, 1)	0.5222
$\lambda_{\max} = 3.0510$, CI = 0.0255, CR = 0.0440, $\in_r = 0.0387$				

$$\mathrm{CI} = \frac{\lambda_{\max} - n}{n - 1} \tag{10}$$

where $\lambda_{\max}$ is the maximum eigenvalue and n is the size of FPCM.

$$\mathrm{CR} = \frac{\mathrm{CI}}{\mathrm{RI}} \tag{11}$$

In this case, the Random Index (RI) is a set of random values, and the CI is the average of many randomly generated multiplicative preference relations. If CR = 0.10, W is assumed to be appropriately consistent, and if CI = 0, W is consistent; for example, a CR = 0.10 threshold indicates that the CI is 10%. The Threshold (T) of the biggest eigenvalue may then be computed as follows:

$$\lambda_{\max}^{T} = n + 0.1 \times \left(n - 1\right) \times \mathrm{RI} \tag{12}$$

Where relative error $\in_r$ is defined as:

$$\in_r = \frac{\lambda_{\max}^{T} - n}{n} \tag{13}$$

If the CR > 0.10, indicating that the FPCM is not consistent, the pairwise comparison method of C_i/SC_i must be altered until the CR becomes acceptable (Liu et al., 2017; Ahvanooey et al., 2023).

3.3 Game theory-based MCDM

Cooperative game theory based on Multi-Criteria Decision Making (MCDM) is used to assess strategic decisions by a variety of stakeholders, including firm developers, users, regulatory agencies, and third-party developers. In cooperative game theory, players can benefit from cooperating and forming coalitions, leading to mutually beneficial outcomes. This approach is particularly suitable for our study as it allows us to model the interactions between different stakeholders (e.g., users, social media platforms, third-party applications) with the aim of finding optimal strategies for minimizing privacy risks. It thus identifies the best combination of strategies that ensures a balanced approach to privacy risk management. Unlike in a Zero-sum game in which one player's gain is exactly balanced by the losses of the other player(s).

A Game (G) can be represented as a strategic structured style of notation based on participant activity as defined in Equation 14:

$$G = \left(P, ST, PF\right) \tag{14}$$

Where $PF_i = \{pf_1, pf_2, pf_3, pf_4\}$ is the pay-off function of the ith player, and there exists a set of p^i players inside the game from which the p^i can pick an alternative strategy (st_j) from the set $ST_i = \{st_1, st_2, st_3\}$. A mixed strategy is made using a collection of pure strategies, and a strategy profile is a mixture of selected strategies for the P^i.

PF_i is also the connection between an input space of all possible profiles ($ST = ST_i, i \in P$), and the output space of real values R. According to the Nash equilibrium strategy profile, no P^i can increase its pay-off by changing its behaviours unilaterally if the rest of the options are unchanged. Furthermore, the Nash equilibrium strategy is the optimum reaction of p^i that maximizes their utility while considering the other p^is' equilibrium as shown in Equation 15 (Ahvanooey et al., 2023; Do et al., 2017)

A strategy ψ^* is a Nash equilibrium if it meets the condition outlined in Equation 16:

$$PF_i\left(\varphi^*{}_i, \varphi^*{}_{-i}\right) \geq PF_i\left(st_i, \varphi^*{}_{-i}\right) \forall st_i \in ST_i \tag{15}$$

However, Pareto efficiency, another essential notion, does not necessarily agree with Nash equilibrium. A strategy profile is Pareto-efficient if no player can improve their payoff while reducing the

TABLE 4 Linguistic scale and TFN conversion scheme.

TFN ($\tilde{v}_{iJ}$)	Reciprocal scale			Pairwise comparison of C_i / SC_i rankings based on expert ratings
	x_{li}	x_{mi}	x_{ui}	
(2.5, 3, 3.5)	0.2	0.3	0.4	The evidence favoring a criterion over another is of the highest feasible order of affirmation.
(2, 2.5, 3)	0.3	0.4	0.5	A criterion is strongly favored, and its dominance is exhibited in practice.
(1.5, 2, 2.5)	0.4	0.5	0.6	The judgment essentially favors one criterion over another.
(1, 1.5, 2)	0.5	0.6	1	The judgment moderately favors one criterion over another.
(1, 1, 1)	1	1	1	Two criteria contribute equally to the objective.

payoff of another player, as expressed mathematically in Equation 16 (Ahvanooey et al., 2023; Do et al., 2017).

Suppose that a strategy profile ψ^{p} P is a Pareto efficient outcome if for the φ:

$$\begin{aligned} &\forall_i \ PF_i(\varphi) \geq PF_i\left(\psi^{p}\right), \\ &\exists_i \ PF_i(\varphi) > PF_i\left(\psi^{p}\right). \end{aligned} \tag{16}$$

Where PF_1, PF_2, and PF_3, PF_4 are the pay-off functions for each player in different strategy association games, and $\{st_1, st_2, st_3\}$ are the strategic possibilities of P^1, P^2, P^3 and P^4. The collection of tactics available to the specific player or players is known as the player's ST set. If $\left(\overline{st_1, st_2, st_3}\right)$ is met while taking the following into account:

$$\begin{cases} PF_1\left(\overline{st1}, \overline{st2}, \overline{st3}\right) = \max\limits_{st_1 \in ST_i} PF_1\left(st_1, st_2, st_3\right) \\ PF_2\left(\overline{st1}, \overline{st2}, \overline{st3}\right) = \max\limits_{st_2 \in ST_i} PF_2\left(st_1, st_2, st_3\right) \\ PF_3\left(\overline{st1}, \overline{st2}, \overline{st3}\right) = \max\limits_{st_3 \in ST_i} PF_3\left(st_1, st_2, st_3\right) \\ PF_4\left(\overline{st1}, \overline{st2}, \overline{st3}\right) = \max\limits_{st_4 \in ST_i} PF_4\left(st_1, st_2, st_3\right) \end{cases} \tag{17}$$

Therefore, there is a Pareto-Nash equilibrium in the strategy set $\left(\overline{st_1}, \overline{st_2}, \overline{st_3}\right)$. If no strategy set $\left(st_1, st_2, st_3\right)$ exists for the game set $\left(P^1, P^2, P^3, P^4\right) \in P$ that meets the following requirements:

$$\begin{cases} PF_1\left(\overline{st_1}, \overline{st_2}, \overline{st_3}\right) < PF_1\left(st_1, st_2, st_3\right) \\ PF_2\left(\overline{st_1}, \overline{st_2}, \overline{st_3}\right) < PF_2\left(st_1, st_2, st_3\right) \\ PF_3\left(\overline{st_1}, \overline{st_2}, \overline{st_3}\right) < PF_3\left(st_1, st_2, st_3\right) \\ PF_4\left(\overline{st_1}, \overline{st_2}, \overline{st_3}\right) < PF_3\left(st_1, st_2, st_3\right) \end{cases} \tag{18}$$

Table 5 outlines various alternative strategies, categorized by different stakeholders, which are crucial for mitigating the privacy invasion risk of users' sensitive data on social media platforms. These strategies are part of a game theory model designed to address privacy concerns, where each category of stakeholders has a set of strategies they can adopt to protect user data.

3.3.1 Payoff matrix

The payoff matrix is determined based on these steps:

i Criteria Weighting using Fuzzy AHP
Fuzzy AHP is utilized to determine the relative significance of privacy risk factors to each stakeholder. These criteria weights served as the foundation for determining payoffs.

ii Strategic Interaction via Game Theory
Using these weighted criteria, we simulated player interactions and calculated their payoffs. The payoffs represent the rewards or outcomes that each player (stakeholder) gains by choosing a certain combination of strategies. For each combination of strategies chosen by the players, a corresponding payoff is calculated, indicating how beneficial that combination is in mitigating privacy risks as shown in Equations 17, 18.

Game theory is used to calculate the payoffs based on interactions between the players. Each player's strategy influences the others, and the Nash equilibrium is used to find the optimal set of strategies where no player can unilaterally improve their payoff. Each Player P^i has three ways to reduce the danger of privacy breaches. Each method is mutually exclusive, therefore only one of the three may be chosen. As a result, we have a total of $(3 * 3 * 3 * 3) = 81$ possible player interactions. The full payoff matrix would require listing all 81 strategy combinations (since $3^4 = 81$) and calculating the payoffs for each combination based on the mixed strategy probabilities. The interactions are represented in the form of a three-dimensional pay-off matrix, with one box containing three numbers indicating the outcome of PF_i for each P^i when options are picked as shown in Table 6.

4 Implementation

This section delves into the specifics of the implementation of the proposed FHF-PR. The model was implemented on the MATLAB 2018a platform, including the selection of computational methods used to compute weights and the expert-ranked determinant criteria.

4.1 Data collection

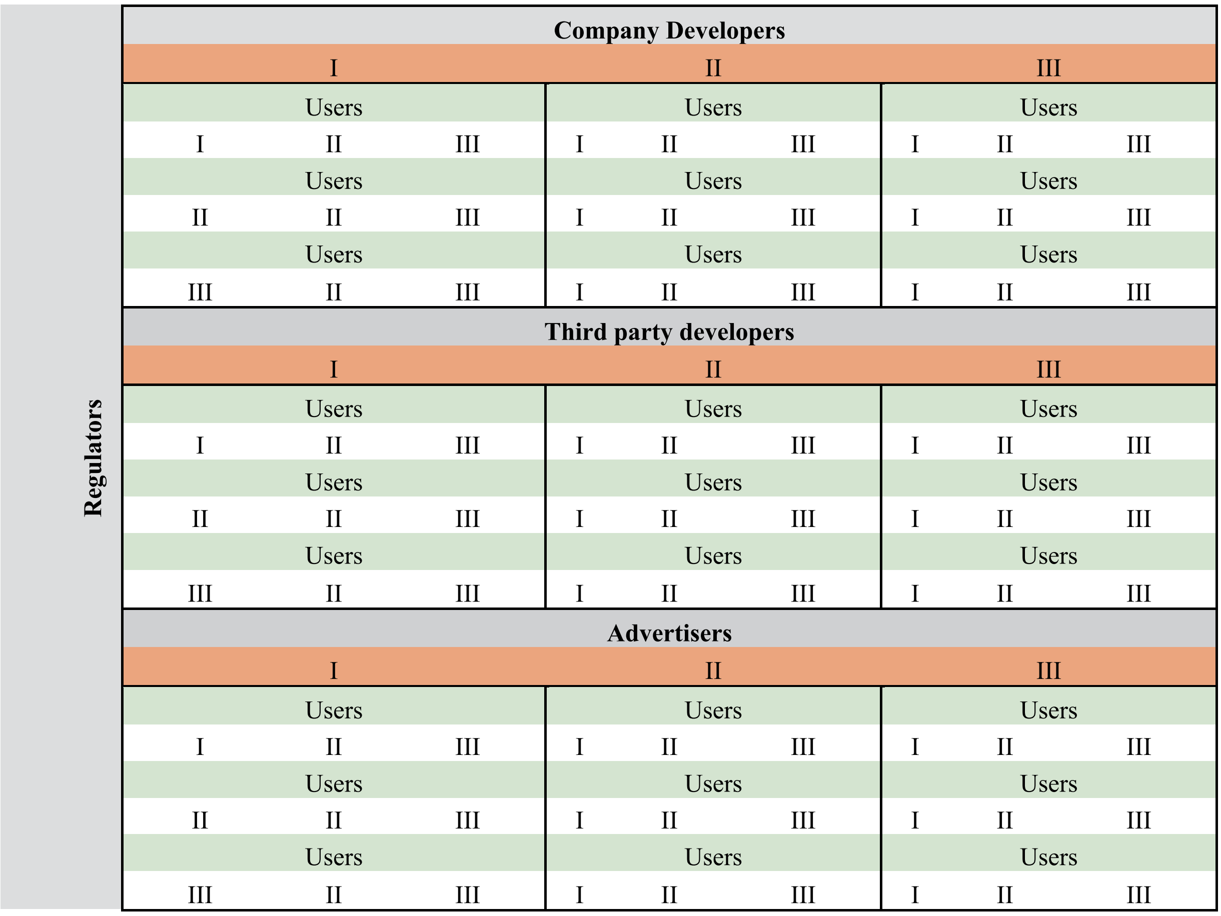
A questionnaire was created using the Microsoft Forms platform and distributed to experts (such as cybersecurity professionals, programmers, cybercrime fighters, and IT specialists) and social media users through LinkedIn, WhatsApp, and X. Out of the 57 responses received, seven were excluded due to incomplete demographic information. The ranked scores from various experts and users were then analyzed, focusing on the determinant criteria and sub-criteria. Tables 7, 8 present the frequency analysis of experts' opinions regarding X (Twitter) and Meta. According to the survey, 36% of respondents identified as programmers, 18% as IT professionals, 4% as cybersecurity experts, and the remaining respondents

TABLE 5 A game theory model for linguistic scale and TFN conversion scheme.

Category of p^i	Criteria C_i		Alternative strategies st_i	
Company developers	C_1	Transparency on data security, privacy policy and Ad targeting	st_1	Implement and develop a Zero Trust Security Model and a comprehensive incident response plan
			st_2	Implementing a Privacy Dashboard and Communication Framework
			st_3	Adopt a Privacy-Centric Advertising Model and Third-party data restrictions
Users	C_2	Users control over the spread and use of their data	st_4	Empowering users with the knowledge and skills needed to protect their accounts and understand encryption technologies
			st_5	Implement a User-centric Data control center
			st_6	Implementing a Comprehensive Privacy Reporting and Support System
Regulatory bodies	C_3	Companies' compliance to privacy policies and data sharing	st_7	Creating a comprehensive and adaptable framework that sets clear guidelines and standards for SM Platforms to follow in safeguarding user data
			st_8	Establish a Global Privacy Standards and Certification Program
			st_9	Implementing a Collaborative Reporting and Verification Network
Third-party developers & advertisers	C_4	Considerations for terms and condition accessing users' data on the platform	st_{10}	Implementing a Developer Education and Certification Program
			st_{11}	Implementing a Transparent Data Access and Usage Education Program for Advertisers
			st_{12}	Develop a robust compliance verification program

Provides alternative strategies st_i in the game theory model that must be taken seriously to mitigate the privacy invasion risk of users' sensitive data (SD) on the social media platforms.

TABLE 6 A payoff matrix based on game theory involving four players.



Regulators	Company Developers								
	I			II			III		
	Users			Users			Users		
	I	II	III	I	II	III	I	II	III
	Users			Users			Users		
	II	II	III	I	II	III	I	II	III
	Users			Users			Users		
	III	II	III	I	II	III	I	II	III
	Third party developers								
	I			II			III		
	Users			Users			Users		
	I	II	III	I	II	III	I	II	III
	Users			Users			Users		
	II	II	III	I	II	III	I	II	III
	Users			Users			Users		
	III	II	III	I	II	III	I	II	III
	Advertisers								
	I			II			III		
	Users			Users			Users		
	I	II	III	I	II	III	I	II	III
	Users			Users			Users		
	II	II	III	I	II	III	I	II	III
	Users			Users			Users		
	III	II	III	I	II	III	I	II	III

TABLE 7 Frequency analysis of prioritized C_i/SC_i for X (Twitter) platform based on expert judgments.

Ranked C_i / SC_i	SM users & professional's opinions on particular C_i / SC_i for X sample size (n = 50)							
	Highly important			Moderately important			Slightly important	
Linkert scale	9	7	%	5	3	%	1	%
C_1	16	17	66	6	8	28	3	6
C_2	7	26	66	6	6	24	5	10
C_3	9	25	68	11	3	28	2	4
C_4	11	25	66	9	5	28	3	6
SC_1	15	22	74	9	3	24	1	2
SC_2	12	21	66	13	4	34	0	0
SC_3	15	19	68	10	3	26	3	6
SC_4	19	19	76	7	3	20	2	4
SC_5	18	23	82	6	2	16	1	2
SC_6	16	25	82	5	1	12	3	6
SC_7	10	27	74	8	4	24	1	2
SC_8	11	26	74	8	3	22	1	4
SC_9	14	22	72	9	3	24	2	4
SC_{10}	11	25	72	10	3	26	1	2
SC_{11}	9	23	65	14	1	30	3	6
SC_{12}	14	24	76	6	4	20	2	4

TABLE 8 Frequency analysis of prioritized C_i/SC_i for Meta platform based on expert judgments.

Ranked C_i / SC_i	SM users & professional's opinions on particular C_i / SC_i for Meta sample size (n = 50)							
	Highly important			Moderately important			Slightly important	
Linkert scale	9	7	%	5	3	%	1	%
C_1	16	21	74	9	2	22	2	4
C_2	12	25	74	6	3	24	1	2
C_3	13	23	72	9	3	24	2	4
C_4	16	22	76	9	1	22	2	4
SC_1	14	25	78	5	4	18	1	4
SC_2	14	22	72	8	3	22	3	6
SC_3	13	24	74	8	3	22	2	4
SC_4	15	22	74	10	1	22	2	4
SC_5	13	25	76	8	1	18	3	6
SC_6	17	20	74	7	2	20	3	6
SC_7	15	21	72	10	2	24	2	4
SC_8	11	24	70	11	2	26	2	4
SC_9	13	20	68	12	3	30	2	4
SC_{10}	15	26	82	6	1	14	2	4
SC_{11}	15	19	68	11	3	28	2	4
SC_{12}	17	19	72	8	4	24	2	4

represented a variety of professions including data analysts, students, civil engineers, project managers, and blockchain developers.

4.2 Computational analysis and results

To compute the priority weights for determinants, the Fuzzy Pairwise Comparison Matrices (FPCMs) were generated using the scaling scheme presented in Table 4, based on the frequency analysis of collected scores in Tables 2, 8. After generating the FPCMs, the consistency ratio was applied to validate the derived weights using the fuzzy-AHP as computed in the MATLAB platform (see Tables 3, 9–11).

Following the computational analysis, valid priority weights were achieved and represented as payoff values in the payoff matrix elements.

In the context of this research, game theory is used alongside Fuzzy-AHP to model privacy risk assessment on social media platforms (Meta and X). The goal is to provide strategic options to mitigate privacy invasion risks by considering various stakeholders (company developers, users, regulatory bodies, third-party developers, and advertisers). Here's how the payoff matrix and strategies are determined:

For Meta platform:

Player 1 (Company Developers):

- Strategy 1 (0.5082): Focuses on implementing the Zero Trust Security Model.
- Strategy 2 (0.1699): Focuses on developing a Privacy Dashboard.
- Strategy 3 (0.3220): Focuses on adopting a Privacy-Centric Advertising Model.

Player 1 is most likely to implement the Zero Trust Security Model, followed by adopting a Privacy-Centric Advertising Model, and least likely to develop a Privacy Dashboard.

Player 2 (Users):

- Strategy 1 (0.1887): Focuses on account security awareness.
- Strategy 2 (0.5439): Focuses on implementing a user-centric data control center.
- Strategy 3 (0.2674): Focuses on implementing a comprehensive privacy reporting system.

Player 2 is most likely to implement a user-centric data control center, while focusing least on account security awareness.

Player 3 (Regulatory Bodies):

- Strategy 1 (0.5326): Focuses on creating adaptable frameworks for data protection.

TABLE 9 Fuzzy extent analysis for Meta platform.

FPCM for related to C_{1-4} category classification.					
	C_1	C_2	C_3	C_4	Priority weight
C_1	(1, 1, 1)	(1, 1.5, 2)	(2, 2.5, 3)	(0.5, 0.6, 1)	0.2930
C_2	(0.5, 0.6, 1)	(1, 1, 1)	(1.5, 2, 2.5)	(0.3, 0.4, 0.5)	0.2094
C_3	(0.3, 0.4, 0.5)	(0.4, 0.5, 0.6)	(1, 1, 1)	(0.3, 0.4, 0.5)	0.1141
C_4	(1, 1.5, 2)	(2, 2.5, 3)	(2, 2.5, 3)	(1, 1, 1)	0.3835
$\lambda_{\max} = 4.0431$, CI = 0.0144, CR = 0.0160, $\epsilon_r = 0.0675$.					

TABLE 10 FPCM for related to SC_{1-3} category classification.

	SC_1	SC_2	SC_3	Priority weight
SC_1	(1, 1, 1)	(2, 2.5, 3)	(1.5, 2, 2.5)	0.5082
SC_2	(0.3, 0.4, 0.5)	(1, 1, 1)	(0.4, 0.5, 0.6)	0.1699
SC_3	(0.4, 0.5, 0.6)	(1.5, 2, 2.5)	(1, 1, 1)	0.3220
$\lambda_{\max} = 3.0305$, CI = 0.0153, CR = 0.0263, $\epsilon_r = 0.0387$				

FPCM for related to SC_{4-6} category classification				
	SC_4	SC_5	SC_6	Priority weight
SC_4	(1, 1, 1)	(0.3, 0.4, 0.5)	(0.5, 0.6, 1)	0.1887
SC_5	(2, 2.5, 3)	(1, 1, 1)	(2, 2.5, 3)	0.5439
SC_6	(1, 1.5, 2)	(0.3, 0.4, 0.5)	(1, 1, 1)	0.2674
$\lambda_{\max} = 3.0142$, CI = 0.0071, CR = 0.0122, $\epsilon_r = 0.0387$				

FPCM for related to SC_{7-9} category classification				
	SC_7	SC_8	SC_9	Priority weight
SC_7	(1, 1, 1)	(2, 2.5, 3)	(2, 2.5, 3)	0.5326
SC_8	(0.3, 0.4, 0.5)	(1, 1, 1)	(1.5, 2, 2.5)	0.3031
SC_9	(0.3, 0.4, 0.5)	(0.4, 0.5, 0.6)	(1, 1, 1)	0.1643
$\lambda_{\max} = 3.0667$, CI = 0.0575, CR = 0.0333, $\epsilon_r = 0.0387$				

FPCM for related to SC_{10-12} category classification				
	SC_{10}	SC_{11}	SC_{12}	Priority weight
SC_{10}	(1, 1, 1)	(2.5, 3, 3.5)	(2.5, 3, 3.5)	0.5771
SC_{11}	(0.2, 0.3, 0.4)	(1, 1, 1)	(0.4, 0.5, 0.6)	0.1464
SC_{12}	(0.2, 0.3, 0.4)	(1.5, 2, 2.5)	(1, 1, 1)	0.2765
$\lambda_{\max} = 3.0035$, CI = 0.0018, CR = 0.0030, $\epsilon_r = 0.0387$				

- Strategy 2 (0.3031): Focuses on establishing a Global Privacy Standards Certification.
- Strategy 3 (0.1643): Focuses on building a collaborative reporting and verification network.

Player 3 is most likely to create adaptable frameworks for data protection, and least likely to focus on collaborative reporting.

Player 4 (Third-party Developers & Advertisers):

- Strategy 1 (0.5771): Focuses on implementing a developer education and certification program.
- Strategy 2 (0.1464): Focuses on transparent data access and usage education.
- Strategy 3 (0.2765): Focuses on developing compliance verification programs.

Player 4 is most likely to focus on developer education and certification, while transparent data access and usage education is the least likely strategy.

For X platform:

Player 1 (Company Developers):

- Strategy 1 (0.5439): Focuses on implementing the Zero Trust Security Model.
- Strategy 2 (0.1887): Focuses on developing a Privacy Dashboard.
- Strategy 3 (0.2674): Focuses on adopting a Privacy-Centric Advertising Model.

Player 1 is most likely to implement the Zero Trust Security Model, followed by adopting a Privacy-Centric Advertising Model, and least likely to develop a Privacy Dashboard.

Player 2 (Users):

- Strategy 1 (0.1593): Focuses on account security awareness.
- Strategy 2 (0.4597): Focuses on implementing a user-centric data control center.
- Strategy 3 (0.3810): Focuses on implementing a comprehensive privacy reporting system.

Player 2 is most likely to implement a user-centric data control center, while focusing least on account security awareness.

Player 3 (Regulatory Bodies):

- Strategy 1 (0.4929): Focuses on creating adaptable frameworks for data protection.
- Strategy 2 (0.2957): Focuses on establishing a Global Privacy Standards Certification.
- Strategy 3 (0.2114): Focuses on building a collaborative reporting and verification network.

Player 3 is most likely to create adaptable frameworks for data protection, and least likely to focus on collaborative reporting.

TABLE 11 Frequency analysis of prioritized C_i/SC_i for Meta platform based on expert judgments.

Alternative strategy	$P^{1'}s$ Payoff (C_1 = 0.2892)
$s_1 \Rightarrow SC_1$ (Best strategy)	0.5439
$s_2 \Rightarrow SC_3$	0.2674
$s_3 \Rightarrow SC_2$	0.1887
User's payoff values as the second player alternatives	
Alternative strategy	$P^{1'}s$ Payoff ($C_2 = 0.1577$)
$s_1 \Rightarrow SC_5$ (Best strategy)	0.4597
$s_2 \Rightarrow SC_6$	0.3810
$s_3 \Rightarrow SC_4$	0.1593
Regulatory bodies' payoff values as the third player alternatives	
Alternative strategy	$P^{1'}s$ Payoff ($C_3 = 0.3612$)
$s_1 \Rightarrow SC_7$ (Best strategy)	0.4929
$s_2 \Rightarrow SC_8$	0.2957
$s_3 \Rightarrow SC_9$	0.2114
Third party developers & advertisers' payoff values as the fourth player alternatives	
Alternative strategy	$P^{1'}s$ Payoff ($C_4 = 0.1919$)
$s_1 \Rightarrow SC_{12}$ (Best strategy)	0.5222
$s_2 \Rightarrow SC_{10}$	0.3509
$s_3 \Rightarrow SC_{11}$	0.1270

Player 4 (Third-party Developers & Advertisers):

- Strategy 1 (0.3509): Focuses on implementing a developer education and certification program.
- Strategy 2 (0.1270): Focuses on transparent data access and usage education.
- Strategy 3 (0.5222): Focuses on developing compliance verification programs.

Player 4 is most likely to focus on developing compliance verification programs.

Figures 2, 3 compared weighted scores calculated using the FHG-PR across different stakeholders for the Meta and X platforms. The graphs demonstrate diverse preferences for strategy implementation. Company Developers will most likely choose the Zero Trust Security Model (Strategy 1), with a Meta rating of 0.5082 and X scoring of 0.5030. At the same time, the Privacy-Centric Advertising Model (Strategy 3) is somewhat probable, with Meta scoring 0.3220 and X scoring 0.2674.

Users choose Strategy 2 (User-Centric Data Control Centre), with a Meta score of 0.5439, whereas X prioritises Strategy 3 (Comprehensive Privacy Reporting System), with a value of 0.3810. Regulatory Bodies like Strategy 1 (Adaptable Frameworks for Data Protection), with a Meta rating of 0.5326 and X scoring of 0.4929, make it the best option. Lastly, third-party developers and advertisers. Lastly, Third-party Developers and Advertisers have a high preference for Strategy 1 (Developer Education and Certification Program), with Meta at 0.5771 and X at 0.5222, whilst Strategy 3 for X, with a score of 0.1270, is the least likely to be implemented by all stakeholders. Strategy 1 tends to prevail across many stakeholders, particularly Meta, with a high possibility of adoption by Third-party Developers and Advertisers, reaching 0.5771. Strategy 3 for X's Third-party Developers & Advertisers, on the other hand, had the lowest score of 0.1270.

Priority weights for criteria and sub-criteria were used to rank players and strategies, and these weights were entered as payoff values in the payoff matrix. Figures 4, 5 show the decision tree illustrating the various strategies used by various stakeholders as well as the possibility of each plan being implemented The fuzzy extent analysis in Tables 2, 3, 8, 9 confirms the consistency of judgments, with a consistency ratio > 0.1 validating the accuracy for both platforms. Using the game theory model, three alternative strategies are available to each player to mitigate privacy invasion risk. Each strategy is mutually exclusive, allowing only one choice per decision-making process, resulting in 81 possible interactions among players (social media users, advertisers, third-party developers, company developers, and regulatory bodies) (see Tables 11, 12).

4.3 Comparison with existing work

Table 13 compares the proposed FHG-PR to previous work by Ahvanooey et al. (2023), which focuses on fuzzy-AHP for social media platforms. Unfortunately, there is little study in this field. The results show the performance of various strategies (St1, St2, St3) among different players (developers, users, inspectors, and third-party entities) on the X and Meta platforms. FHG-PR has a higher priority weight for St1 (0.5439) than the existing work (0.4551), indicating a greater emphasis on Strategy 1 for developers. For consumers, the proposed FHG-PR shifts attention considerably towards St2 (0.4597) and St3 (0.3810). Unlike previous studies, which prioritised St1 (0.5323). Overall, the suggested FHG-PR model places a greater emphasis on specific strategies across distinct actors than in prior studies. This shows that the suggested methodology offers a more sophisticated and diverse approach to reducing privacy issues on social media sites. The experimental results show that the proposed FHG-PR solutions can greatly minimise privacy issues in social media platforms. Figures 6, 7 show interactions between various stakeholders (players) on platforms such as X and Meta, illustrating their methods and how criteria and sub-criteria are prioritised to reduce privacy issues. Figure 8 shows a comparison of game theory models for the X and Meta platforms. It examines how various organisations assess their privacy strategies and decision-making, providing a more in-depth view of how privacy concerns are managed on each platform. These interactions are examined through the framework of Game Theory.

5 Discussion and practical implications

In this section, we analyze the model's key findings and their practical implications for the strategic information management of SM by including managerial sectors.

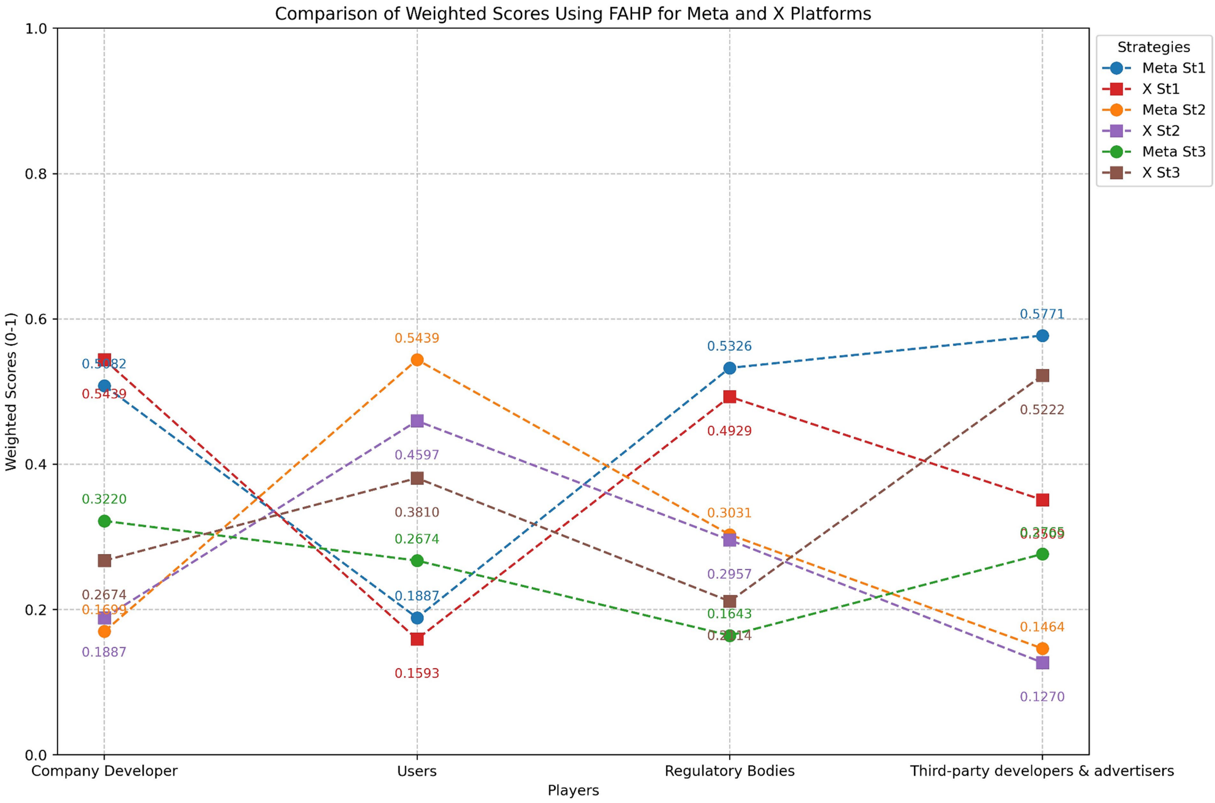


FIGURE 2
Comparison of weighted score using FHG-PR for meta and X platform.

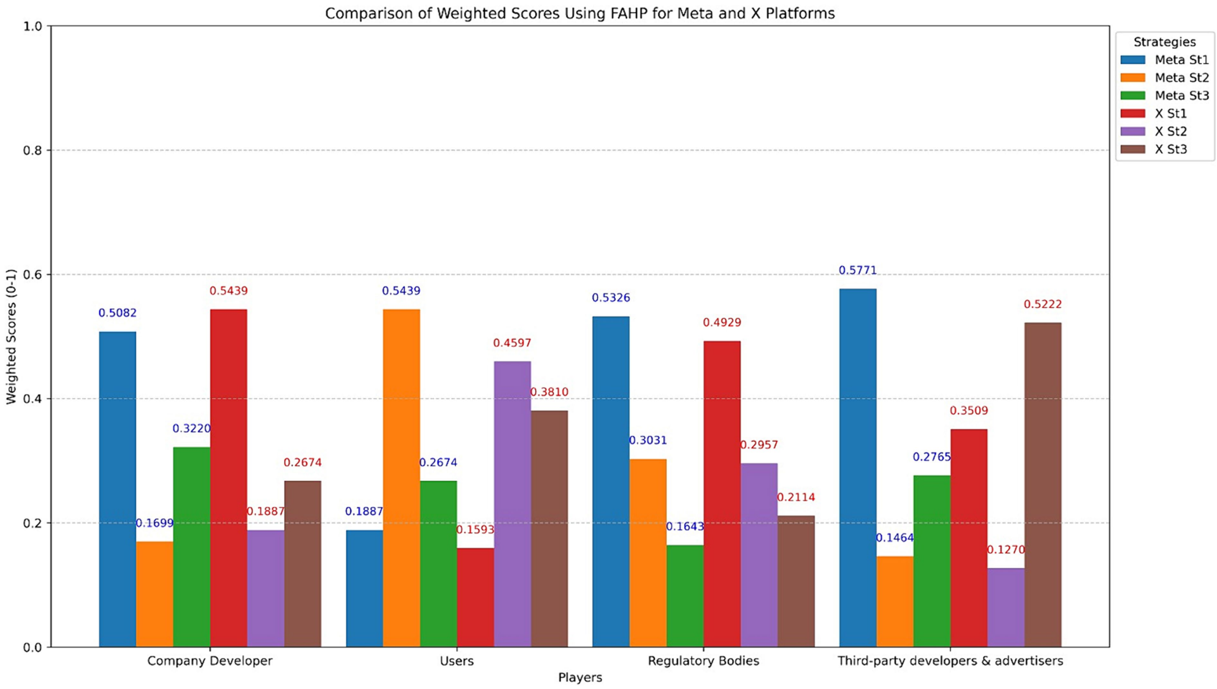


FIGURE 3
A chart of weighted score using FHG-PR for meta and X platform.

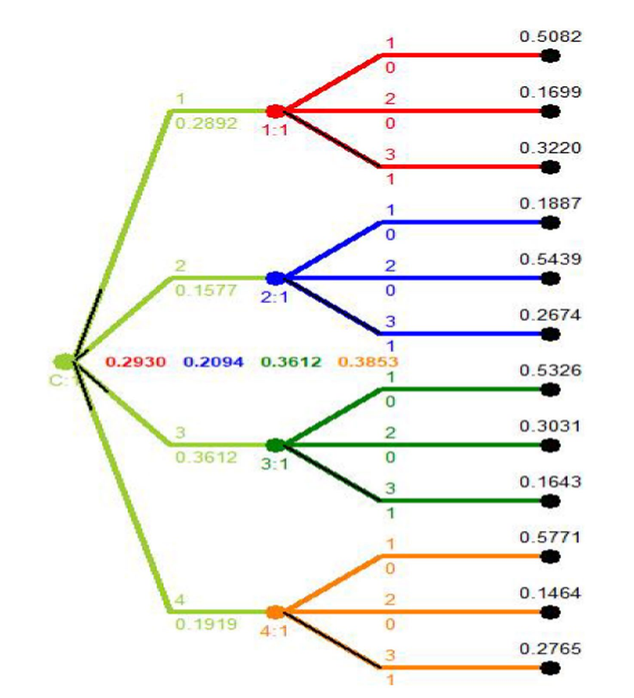


FIGURE 4
The decision tree showing the strategies adopted by different stakeholders on Meta platform based on their respective weights.

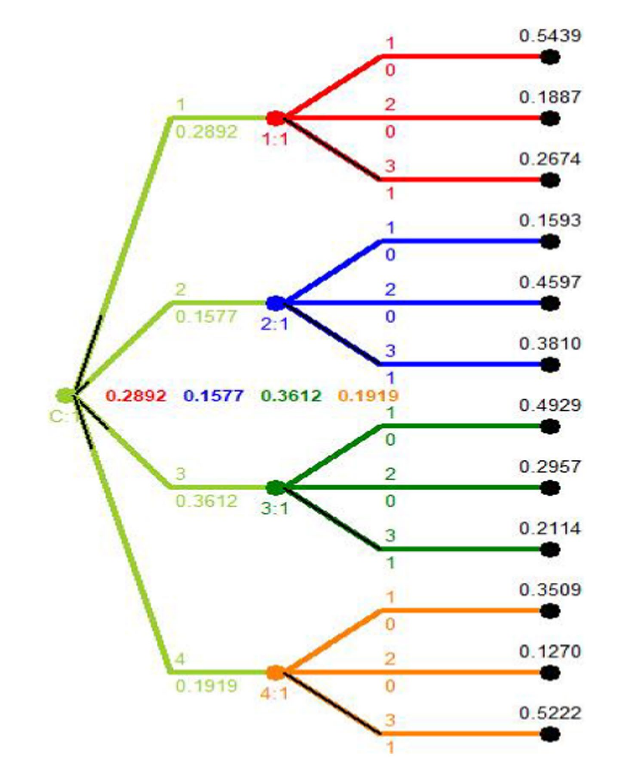


FIGURE 5
The decision tree showing the strategies adopted by different stakeholders on X platform based on their respective weights.

TABLE 12 Frequency analysis of prioritized C_i/SC_i for X Platform based on expert judgments.

Alternative strategy	$P^{1'}s$ Payoff (C_1 = 0.2930)
s_1 => SC_1 (Best strategy)	0.5082
s_2 => SC_3	0.3220
s_3 => SC_2	0.1699
User's payoff values as the second player alternatives	
Alternative strategy	$P^{1'}s$ Payoff (C_2 = 0.2094)
s_1 => SC_5 (Best strategy)	0.5439
s_2 => SC_6	0.2674
s_3=> SC_4	0.1887
Regulatory bodies' payoff values as the third player alternatives	
Alternative strategy	$P^{1'}s$ Payoff (C_3 = 0.1141)
s_1 => SC_7 (Best strategy)	0.5326
s_2 => SC_8	0.3031
s_3 => SC_9	0.1643
Third party developers & advertisers' payoff values as the fourth player alternatives	
Alternative strategy	$P^{1'}s$ Payoff (C_4 = 0.1919)
s_1 => SC_{10} (Best strategy)	0.5771
s_2 => SC_{12}	0.2765
s_3 => SC_{11}	0.1464

TABLE 13 Comparative analysis of FHG-PR with previous work.

Authors	Social media	Players	St1	St2	St3	
Ahvanooey et al. (2023)	X platform	Developers	0.4551	0.3777	0.1673	0.0387
		Users	0.5323	0.3027	0.165	
		Inspector	0.4926	0.2956	0.2118	
Proposed FHG-PR	X platform	Developers	0.5439	0.1887	0.2687	0.0387
		Users	0.1593	0.4597	0.3810	
		Inspector	0.4929	0.2957	0.2114	
		Third party	0.3509	0.1270	0.5222	
	Meta platform	Developers	0.5082	0.1699	0.3220	0.0387
		Users	0.1887	0.5439	0.2674	
		Inspector	0.5326	0.3031	0.1643	
		Third party	0.5771	0.1464	0.2765	

5.1 Key findings

This study can bridge the gap by proposing strategic solutions to address privacy concerns in SM ecosystems. It examines privacy issues in the literature and identifies factors that can be addressed by four corporate management sectors. Data from 50 users and experts is used to rank the relevance of the determinant C_i/SC_i in terms of privacy invasion hazards. The Fuzzy-AHP technique is used to derive the weights of determinants C_i/SC_i. A game theory-based MCDM framework is created to evaluate situations where

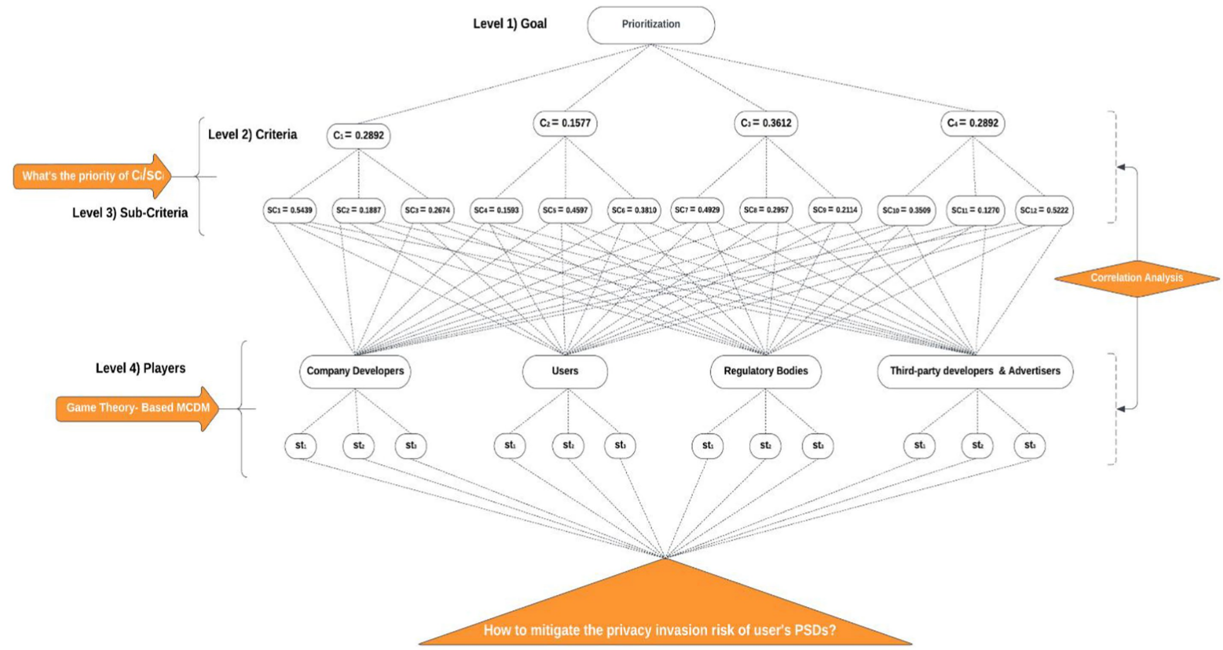


FIGURE 6
The decision tree showing the strategies adopted by different stakeholders on X platform based on their respective weights.

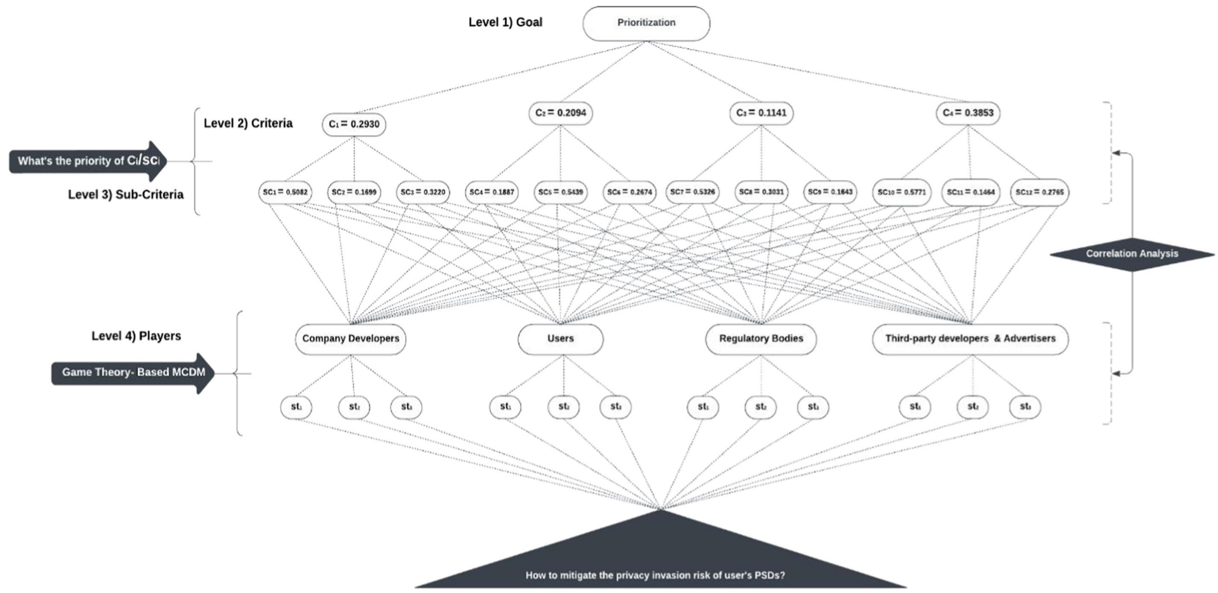


FIGURE 7
The decision tree showing the strategies adopted by different stakeholders on X platform based on their respective weights.

independent players in each management sector make decisions. These tactics can guide active players to adopt real remedies that positively influence SMP privacy improvements. The hybridized fuzzy-AHP and game theory models offer promising measures for mitigating privacy invasion risks.

5.2 Practical implications

The paper explores strategic information management for SM platforms using the fuzzy-AHP model and game theory. It identifies four sectors: technology & development, social, government &

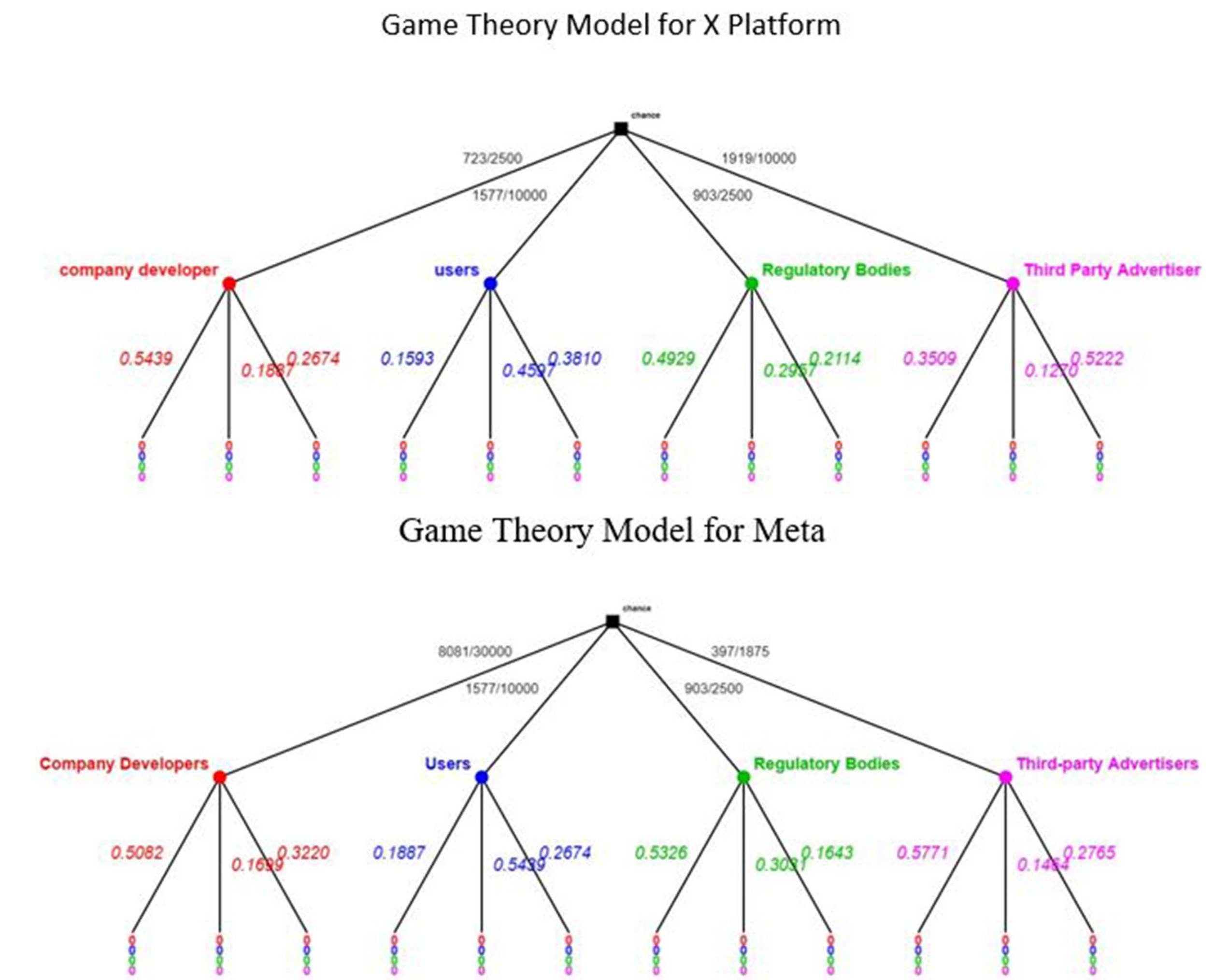


FIGURE 8
Game theory model for X platform and Meta platform.

compliance, and external partners, each working together to reduce privacy invasions of users' sensitive data. The model can guide these sectors in developing safer platforms in the future, addressing privacy invasion risks in social media. The probable consequences of this concept are discussed further below:

- **Technology & development management**: The technology and engineering departments of social media platforms (SMs) often prioritize business profits over privacy-preserving improvements. For instance, platforms like Meta faced cyberattacks in October 2021, revealing leaked user data. Law Enforcement Agencies (LEAs) should mandate SM platforms to deploy cybersecurity specialists and upgrade their systems against cyberattacks like Man in the Middle (MITM) and Sybil. Alternative countermeasures for managing and securing users' PSDs include implementing a Zero Trust Security Model and developing a comprehensive incident response strategy, which can prove to be effective for Meta and X platforms.
- **Social management:** Social departments of organizations like the United Nations Department of Public Information research the worldwide hazards of social media platforms for their members and users. They believe that user data leaks can lead to violence, identity theft, and impersonation. To improve privacy, they recommend that platforms develop a data control center, allowing users to control their data access, deactivate apps, and update their settings. This model can guide social management departments in making strategic choices to limit privacy invasion threats of users' data. This collaboration is crucial to ensuring the safety and security of social media platforms.
- **Governmental and compliance management:** The Nigeria Data Protection Bureau (NDPB), Europol, the FBI of the United States, and Interpol are among the regulatory authorities working together to combat international cybercrime. These bodies are responsible for defending human rights and promoting a peaceful living environment. However, private organizations like SM platforms lack adequate safeguards to guarantee free expression, which is where government authorities come in. They provide independent legal checks, address complaints, and oversee oversight decisions. This responsibility is largely missing from public discussions. Concerns about user privacy on SM platforms worldwide are highlighted, prompting regulatory agencies to adopt new strategies. One such strategy is harmonizing data laws by creating unified privacy standards that align with major international laws, reducing data fragmentation and conflict in data protection regulation. This would make it easier for SM platforms to navigate and comply with multiple jurisdictions. The

model proposes strategic solutions for dealing with user privacy infringement allegations/reports by regulatory organizations. However, further research could expand these proposals to address more specific consumer concerns and limit privacy invasion threats.

- **External partner management:** This sector typically involves various stakeholders and activities related to managing external partnerships and ensuring compliance with privacy standards in the context of SM. SM platforms like Meta and X have integrated third-party apps and services. Users grant permissions to these apps, allowing them to access their data. In the past, some apps have misused this access, leading to privacy breaches. For instance, in 2023, X began to reduce the number of tweets a user could read in a day to counter the unauthorized use of users privately sensitive data by advertisers and third-party developers who used illegal bots to steal people's tweets. These measures seem counterproductive, as users complained about not being able to access and view tweets and were irritated by the sudden change of rules. Hence, this model suggests a strategic alternative for external partner management. For example, X platform can create an external partner department that helps external partners get verified or go through a robust compliance verification process that involves being certified after being verified to use the platform's API for development and advertisement purposes. The model also suggests that external partners should be educated on responsible data access practices, ensuring they have a clear understanding of what data they can access and how to use it appropriately while using the Meta platform.

5.3 Limitations

This study has some limitations that need to be addressed in future research. First, sample size and representativeness are concerns, as the population being analysed may not include all Meta and X users. Instead, it may represent a smaller, more specialised group, such as cybersecurity specialists or developers, limiting the general applicability of the results.

Also, the game theory model utilised in the study assumes that all stakeholders are perfectly rational and have all relevant knowledge. However, in practice, users may be unaware of privacy hazards, and both businesses and regulatory authorities are susceptible to external variables such as legal and operational limits that are not accounted for in the model. In addition, the model provides a static perspective on decision-making, but real-world settings include dynamic changes in information, legislation, and technology improvements. Thus, future research should use a more flexible and thorough approach in order to improve the accuracy and relevance of findings. The frequency analysis identifies knowledge-based aspects, such as the C_i/SC_i determinants, which may contain other factors not explored here. Future research should look at including more factors such as cultural and sentiment analysis. Expanding the scope to include other social media sites, such as TikTok and Snapchat, might improve privacy risk evaluations.

6 Conclusion

This study used a risk assessment methodology based on fuzzy-AHP using some set of determinant criteria to identify and rank potential strategies to limit the danger of privacy invasion of user's Sensitive Data in SM. The investigation found several factors that influence the privacy invasion risks of users' Sensitive Data. Following that, data on the relevance of these characteristics was graded by polling 50 users and experts. Furthermore, based on the collected data, the fuzzy-AHP method was used to assign weights to the criteria, and a cooperative game theory MCDM framework was used to evaluate the possibilities of interactions among players, such as management sectors, and to determine alternative strategies for enhancing privacy in SMs. This study's experimental results indicated that the proposed model works. As such, privacy invasion concerns are expected to be significantly reduced if this model's proposed alternatives are considered and implemented into an organization's operational technology security plans.

Data availability statement

The anonymized data along with the MATLAB code, datasets, and intermediate results, can be accessed in a public repository on GitHub at the following link: https://github.com/osasido/Fuzzy-AHP-risk-assessment-.git.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. Written informed consent from the participants was not required to participate in this study in accordance with the national legislation and the institutional requirements.

Author contributions

OF: Conceptualization, Methodology, Supervision, Writing – original draft, Writing – review & editing. TO: Methodology, Software, Writing – original draft. HN: Data curation, Investigation, Methodology, Software, Supervision, Writing – review & editing. DA: Investigation, Methodology, Validation, Visualization, Writing – review & editing. AA: Formal analysis, Methodology, Software, Supervision, Writing – review & editing. FA: Investigation, Methodology, Software, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. The authors acknowledge the support of Jouf University.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fcomp.2024.1389223/full#supplementary-material

References

Ahvanooey, M. T., Zhu, M. X., Ou, S., Mazraeh, H. D., Mazurczyk, W. and Choo, K. K. R., et al. (2023). AFPr-AM: a novel fuzzy-AHP based privacy risk assessment model for strategic information management of social media platforms. *Comput. Secur.* 130:103263. doi: 10.1016/j.cose.2023.103263

Alemany, J., Del Val, E., Alberola, J. M., and Garćia-Fornes, A. (2019). Metrics for privacy assessment when sharing information in online social networks. *IEEE Access* 7, 143631–143645. doi: 10.1109/ACCESS.2019.2944723

AlMudahi, G. F., AlSwayeh, L. K., AlAnsary, S. A., and Latif, R. (2022). Social media privacy issues, threats, and risks. Paper presented at the 2022 fifth international conference of women in data science at Prince Sultan University (WiDS PSU). 155–159.

Anderson, C. L., and Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *MIS Q.* 34, 613–643. doi: 10.2307/25750694

Ashour, M., and Mahdiyar, A. (2023). A comprehensive state-of-the-art survey on the recent modified and hybrid analytic hierarchy process approaches. *Appl. Soft Comput.* 150:111014. doi: 10.1016/j.asoc.2023.111014

Bouke, M. A., Abdullah, A., ALshatebi, S. H., Zaid, S. A., and El Atigh, H. (2023). The intersection of targeted advertising and security: unraveling the mystery of overheard conversations. *Telemat. Informat. Rep.* 11:100092. doi: 10.1016/j.teler.2023.100092

Buckley, J. J. (1985). Fuzzy hierarchical analysis. *Fuzzy Sets Syst.* 17, 233–247. doi: 10.1016/0165-0114(85)90090-9

Buckley, J. J., Feuring, T., and Hayashi, Y. (1999). Fuzzy hierarchical analysis. Paper presented at the FUZZ-IEEE'99. 1999 IEEE international fuzzy systems. Conference proceedings (Cat. No. 99CH36315). 1009–1013.

Buckley, J. J., Feuring, T., and Hayashi, Y. (2001). Fuzzy hierarchical analysis revisited. *Eur. J. Oper. Res.* 129, 48–64. doi: 10.1016/S0377-2217(99)00405-1

Chang, D.-Y. (1996). Applications of the extent analysis method on fuzzy AHP. *Eur. J. Oper. Res.* 95, 649–655. doi: 10.1016/0377-2217(95)00300-2

Cheng, X., Fu, S., and de Vreede, G.-J. (2017). Understanding trust influencing factors in social media communication: a qualitative study. *Int. J. Inf. Manag.* 37, 25–35. doi: 10.1016/j.ijinfomgt.2016.11.009

Choi, T.-M., Guo, S., and Luo, S. (2020). When blockchain meets social-media: will the result benefit social media analytics for supply chain operations management? *Transp. Res. Part E Logist. Transp. Rev.* 135:101860. doi: 10.1016/j.tre.2020.101860

Dikshit, P., Sengupta, J., and Bajpai, V. (2023). Recent trends on privacy-preserving technologies under standardization at the IETF. *ACM SIGCOMM Comput. Commun. Rev.* 53, 22–30. doi: 10.1145/3610381.3610385

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., et al. (2017). Game theory for cyber security and privacy. *ACM Comput. Surv.* 50, 1–37. doi: 10.1145/3057268

García-Rodríguez, J., Krenn, S., and Slamanig, D. (2024). To pass or not to pass: privacy-preserving physical access control. *Comput. Secur.* 136:103566. doi: 10.1016/j.cose.2023.103566

Hiwale, M., Walambe, R., Potdar, V., and Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthcare Anal.* 3:100192. doi: 10.1016/j.health.2023.100192

Jacobson, J., Gruzd, A., and Hernández-García, Á. (2020). Social media marketing: who is watching the watchers? *J. Retail. Consum. Serv.* 53:101774. doi: 10.1016/j.jretconser.2019.03.001

Janssen, H., Cobbe, J., and Singh, J. (2020). Personal information management systems: a user-centric privacy utopia? *Internet Policy Rev.* 9, 1–25.

Karusala, N., Bhalla, A., and Kumar, N. (2019). Privacy, patriarchy, and participation on social media. Paper presented at the proceedings of the 2019 on designing interactive systems conference. 511–526.

Kavianpour, S., Tamimi, A., and Shanmugam, B. (2019). A privacy-preserving model to control social interaction behaviors in social network sites. *J. Inf. Secur. Appl.* 49:102402. doi: 10.1016/j.jisa.2019.102402

Koohang, A., Paliszkiewicz, J., and Goluchowski, J. (2018). Social media privacy concerns: trusting beliefs and risk beliefs. *Ind. Manag. Data Syst.* 118, 1209–1228. doi: 10.1108/IMDS-12-2017-0558

Kubler, S., Robert, J., Derigent, W., Voisin, A., and Le Traon, Y. (2016). A state-of the-art survey & testbed of fuzzy AHP (FAHP) applications. *Expert Syst. Appl.* 65, 398–422. doi: 10.1016/j.eswa.2016.08.064

Laarhoven, P., and Pedrycz, W. (1983). A fuzzy extension of Saaty's priority theory, fuzzy sets and systems. *Fuzzy Sets Syst.* 11, 1–3.

Liu, D. I., Cao, C., Dubovyk, O., Tian, R., Chen, W., Zhuang, Q., et al. (2017). Using fuzzy analytic hierarchy process for spatio-temporal analysis of eco-environmental vulnerability change during 1990–2010 in Sanjiangyuan region, China. *Ecological Indicators* 73, 612–625.

Lockl, J., Thanner, N., Utz, M., and Röglinger, M. (2023). The paradoxical impact of information privacy on privacy preserving technology: the case of self-sovereign identities. *Int. J. Innov. Technol. Manag.* 20:2350025. doi: 10.1142/S0219877023500256

Paliszkiewicz, J., and Koohang, A. (2016). Social media and trust: a multinational study of university students. Santa Rosa, California: Informing Science.

Peng, G., Han, L., Liu, Z., Guo, Y., Yan, J., and Jia, X. (2021). An application of fuzzy analytic hierarchy process in risk evaluation model. *Front. Psychol.* 12:715003. doi: 10.3389/fpsyg.2021.715003

Pensa, R. G., and Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Syst. Appl.* 86, 18–31. doi: 10.1016/j.eswa.2017.05.054

Rass, S., and Schauer, S. (2018). Game theory for security and risk management. *Springer International Publishing* 10, 978–3. doi: 10.1007/978-3-319-75268-6

Rivadeneira, J. E., Silva, J. S., Colomo-Palacios, R., Rodrigues, A., and Boavida, F. (2023). User-centric privacy preserving models for a new era of the internet of things. *J. Netw. Comput. Appl.* 217:103695. doi: 10.1016/j.jnca.2023.103695

Saaty, T. L. (2010). Mathematical principles of decision making (principia mathematica decernendi). Ellsworth Avenue, Pittsburgh, PA, United States: RWS Publications.

Saura, J. R., Ribeiro-Soriano, D., and Palacios-Marqués, D. (2022). Evaluating security and privacy issues of social networks based information systems in industry 4.0. *Enterp. Inf. Syst.* 16, 1694–1710. doi: 10.1080/17517575.2021.1913765

Shullich, R. (2011). Risk assessment of social media. *Int. J. Electron. Commer.* 2, 103–126.

Such, J. M., and Criado, N. (2018). Multiparty privacy in social media. *Commun. ACM* 61, 74–81. doi: 10.1145/3208039

Sur, U., Singh, P., and Meena, S. R. (2020). Landslide susceptibility assessment in a lesser Himalayan road corridor (India) applying fuzzy AHP technique and earth-observation data. *Geomat. Nat. Haz. Risk* 11, 2176–2209. doi: 10.1080/19475705.2020.1836038

Weiss, S. (2009). Privacy threat model for data portability in social network applications. *International journal of information management.* 29, 249–254.

Wiggers, K. (2023). The current legal cases against generative AI are just the beginning: TechCrunch. Available at: https://techcrunch.com/2023/01/27/the-current-legal-cases-against-generative-ai-are-just-the-beginning/

Xu, Z., and Liao, H. (2013). Intuitionistic fuzzy analytic hierarchy process. *IEEE Trans. Fuzzy Syst.* 22, 749–761. doi: 10.1109/TFUZZ.2013.2272585

Zhü, K. (2014). Fuzzy analytic hierarchy process: fallacy of the popular methods. *Eur. J. Oper. Res.* 236, 209–217. doi: 10.1016/j.ejor.2013.10.034