JST

JOURNAL OF SCIENCE AND TECHNOLOGY
ISSN: 2229-8460 e-ISSN: 2600-7924

Vol. 18 No. 1 (2026) 1-12
https://publisher.uthm.edu.my/ojs/index.php/jst

A Fuzzy Comprehensive Evaluation-Based Information Security Risk Assessment of Online Threats Among Young Individuals: A University Campus Scenario

Aliu Folasade Mercy[1]*

[1] *Department of Mathematics and Computer Science, Elizade University, Ilara-Mokin, Ondo State, NIGERIA*

*Corresponding Author: folasade.aliu@elizadeuniversity.edu.ng
DOI: https://doi.org/10.30880/jst.2026.18.01.001

Article Info

Received: 20 November 2025
Accepted: 19 May 2026
Available online: 30 June 2026

Keywords

Online threats, information security, risk assessment, fuzzy comprehensive evaluation, entropy method, risk matrix

Abstract

This research conducts a comprehensive examination of the online threats encountered by young individuals, particularly students, at a university. Utilizing a detailed information security risk assessment approach, the study identifies and analyzes various online risks faced by students, including cyberbullying, exposure to inappropriate content, online predators, privacy breaches, and device security vulnerabilities. The research employs both quantitative and qualitative methods, such as surveys, interviews, and data analysis, to gain insights into the prevalence, nature, and impact of these online threats on the university's student population. The level of information security risks experienced by students was evaluated using Risk Matrix, Entropy, and Fuzzy Comprehensive Evaluation (FCE) methods. The results indicate that the students' information security risk level falls within the low category among five defined risk levels, with an FCE output of 0.403. Additionally, the study proposes recommendations for enhancing the university's cybersecurity posture and promoting digital safety among students. This case study contributes to the broader discourse on information security risk management in educational institutions and provides practical insights for addressing online threats faced by young individuals in academic settings.

1. Introduction

In the rapidly evolving digital age, the internet has become an integral part of the lives of children and teenagers worldwide [1] [2]. The internet offers a wealth of knowledge and endless possibilities for creativity and exploration. It serves as a powerful tool for education, enabling students to access a world of information with a few clicks. It connects friends and family across vast distances, fostering relationships that transcend borders. It provides a platform for self-expression, allowing teenagers to discover and share their passions with a global audience. From education to entertainment, communication to socialization, the online world offers a vast array of opportunities and experiences for young users. However, with these opportunities come significant information security risks that can affect the well-being, privacy, and future prospects of our youngest digital citizens.

Children and teenagers, by virtue of their age and limited life experiences, are particularly susceptible to a wide range of online threats. From exposure to inappropriate content and cyberbullying to privacy breaches and

identity theft, the risks they face are both numerous and complex. Moreover, the constantly evolving nature of technology presents new challenges, demanding vigilance and adaptability from those responsible for safeguarding young users.

Fuzzy comprehensive evaluation (FCE) is an artificial evaluation technique based on fuzzy mathematics, providing real and accurate evaluation results that are extensively utilized in psychology and other fields [3]. The integration of fuzzy theory with Multiple-criteria decision-making (MCDM) methods is primarily used to address the challenge of dealing with linguistic variables in most MCDM methods [4].

Several researchers have applied fuzzy mathematics and entropy methods to achieve different objectives. For instance, the authors in [5] used the combination of fuzzy mathematics and entropy methods to improve the safety management level of construction sites. The results demonstrated that this hybrid method, which can overcome the shortcomings of each single method, is feasible, practical, and operational in assessing construction site safety. Additionally, Shannon entropy theory, a fuzzy comprehensive method, and an analytic hierarchy process (AHP) have been employed to demonstrate a variable type of weighting for landslide susceptibility evaluation modelling, combining subjective and objective weights. This approach produced more objective and accurate landslide susceptibility maps that leverage original data and reflect expert knowledge and decision-makers' opinions [6].

Further applications of FCE include Ma et al.'s use of FCE to determine the source of water inrush in coalmines, applying F-statistics to allocate weights [7]. Similarly, [8] analysed real estate investment risks and found that FCE provides an effective means for investors to understand risk factors and make forecasts. The research of [9] simulated FCE and Principal Component Analysis (PCA) to assess the water quality of the Nansi Lake Basin, China.

Chang in [3] applied a Genetic Algorithm (GA) to determine corresponding weights for FCE of psychological measurement data on the Likert scale, showing that GA-based FCE is beneficial in psychological measurement and consumer psychology studies. Deng and Xiang in [10] used the FCE method based on the Gray correlation degree to evaluate the stability of loess slopes, proving it reasonable and feasible. The study of [11] applied the FCE method to rate the quality of coal in China, considering six evaluation factors, and concluded that the coal is of good quality. The research of [12] comprehensively evaluated the operational level of energy-intensive Internet-of-Things equipment using integrated FCE and AHP methods. In 2021, [13] assessed the digital readiness level of enterprises in Central and Eastern Europe using MCDM methods and the entropy method to determine the weights of the determinants.

The research of [14] provided a comprehensive understanding of potential risks in oil investment in Central Asia using FCE, demonstrating the causes of these risks and offering a scientific basis for mitigating oil investment risks and improving investment benefits for both host and investing countries. FCE has also been used to evaluate the effect of students' participation in course learning, providing feedback and guidance to improve the teaching process and forming a closed-loop management system in education [15]. In [16], Zhang and Guoqing applied FCE to evaluate the water flooding effect in oilfields using entropy and AHP methods to compute weights. Azim developed an e-Governance security assessment model and used both AHP and FCE to determine the system's security level [17].

One of the most challenging aspects of MCDM is appropriately assigning weights to the criteria for ranking alternatives [18]. There are several methods for determining the weights for FCE, such as AHP, genetic algorithm (GA), TOPSIS, Promethee II, and entropy methods [19]. The entropy method avoids human interference in the weighting of indicators, making the evaluation results more objective. Its main advantage is that it can be applied in any weight determination process [20].

Several risk analytical approaches do not necessarily address the fuzzy and behavioural nature of threats faced by young people but focus on technological tools. There is also a limited integration of objective weighting methods and fuzzy evaluation techniques in analysing online security risks faced by youths. It is therefore necessary to develop a detailed framework that combines risk matrix, entropy and fuzzy comprehensive evaluation methods in evaluating cybersecurity risks among young ones. The objectives of this research are to recognize the online security threats faced by youths; to evaluate and categorize their information security risk levels using risk fuzzy comprehensive evaluation; and to contribute feasible solutions to mitigate the risks. The following sections delve into the multifaceted world of information security risks for children and teenagers using the internet. It explores the types of threats they may encounter and analyses the risk level of these threats through the risk matrix, entropy and FCE methods. The analysis is based on the review of questionnaires filled by the students to determine their probability of exposure to online threats and the likely impacts these threats have on them.

2. Methodology

2.1 Entropy Method

To assign weights to criterion, the Entropy approach is utilized in this research. Entropy weight is a parameter that describes how many different alternatives approach one another with respect to sub-criteria. The concept is

J. of Science and Technology Vol. 18 No. 1 (2026) p. 1-12

taken from transportation mechanics. The steps to calculate the weights using the Entropy technique for the decision matrix, A are as follows.

Step 1: Build the initial decision-making matrix, as can be seen in Equation (1).

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}; i = 1,2, \dots, m; j = 1,2, \dots, n \quad (1)$$

where each a_{ij} is the performance of the i^{th} alternative to the j^{th} criterion, m is the number of alternatives and n is the number of criteria.

Step 2: Normalize the decision matrix using Equation 2.

$$r_{ij} = \frac{a_{ij}}{\sum_{i=1}^{m} a_{ij}} \quad (2)$$

where r_{ij} is the normalized value of each a_{ij}.

Step 3: Compute the entropy, e of the j^{th} criterion using Equation 3.

$$e_j = -h \sum_{i=1}^{m} r_{ij} \ln r_{ij} = \frac{1}{\ln m} \sum_{i=1}^{m} r_{ij} \ln r_{ij} \quad (3)$$

Step 4: Compute the degree of diversification, d_j.

$$d_j = 1 - e_j \quad (4)$$

Step 5: Calculate the weight vector, w_j.

$$w_j = \frac{d_j}{\sum_{j=1}^{n} d_j}, j = 1,2 \dots, n \quad (5)$$

2.2 Fuzzy Comprehensive Evaluation (FCE)

FCE is a process of integrating multiple independent variable scores into a dependent variable score. It is a versatile approach for making decisions when the situation is ambiguous or confusing. FCE is a type of artificial intelligence that delivers an exceptional degree of trust for fuzzy logic-based decision-making [21]. It helps by breaking down large decisions into smaller, more manageable portions known as criterion. Then it employs fuzzy logic to address the fuzziness or ambiguity of our judgments regarding those criteria. Finally, it aggregates all of these ambiguous assessments to produce a clear ranking or decision. The traditional method is to determine the weight by expert scoring, which is subjective. However, the entropy approach, which is an objective method, is employed in this study for weight distribution.

Fuzzy comprehensive evaluation technique is a certain implementation procedure which applies fuzzy mathematics [22]. The procedures are outlined beneath.

Step 1: Identify the domain of the examined object factors.

The object factors, X = {x1, x2,..., xj}, indicate the 'j' assessment factors from which a person should judge the assessed object factor, with x_i representing the i^{th} index. Table 1 shows the risk factors that have been discovered. The fuzzy set X = {X_1, X_2, X_3} contains the risk sub-factors X_{11}, X_{12}, X_{13}, X_{14}, X_{21}, X_{22}, X_{23}, X_{31}, X_{32}, X_{33}.

Table 1 *A model for categorizing online risk factors*

Objective	Risk Factors	Risk Sub-factors
Information Security Risk of Youths Online	Direct Harmful Interaction (X_1)	Cyber-bullying (X_{11})
		Online Predators (X_{12})
		Privacy Breaches (X_{13})
		Social Engineering (X_{14})
	Content-related Risks (X_2)	Inappropriate Contents (X_{21})
		Addictive Behaviours (X_{22})
		Online Frauds (X_{23})
	Security and Reputation Concerns (X_3)	Device Security (X_{31})
		Location Tracking (X_{32})
		Online Reputation Damage (X_{33})

Cyberbullying is the use of internet communication tools to harass, intimidate, or humiliate people. Online predators are people who utilize the web to take advantage of, exploit, or groom minors for sexual harassment or other types of abuse. Privacy breaches occur when unauthorized access to personal information or data result in identity theft, stalking, or other privacy crimes. Social engineering is the manipulation tactics used to trick children into disclosing sensitive information or engaging in risky behaviour. Inappropriate content implies the exposure to improper or dangerous materials, such as violence, pornography, or explicit information. Addictive habits include excessive use of online platforms or digital gadgets, which can lead to addiction, social isolation, or mental health problems. Online frauds are fraudulent schemes or deceptive methods used to fool youngsters into giving up money, private details, or access to their devices. Device security refers to vulnerabilities in devices or software that hackers can exploit to obtain unauthorized access, install malicious software, or compromise personal data. Location tracking is monitoring or tracking a child's physical whereabouts via digital devices or applications, which might jeopardize their safety and privacy. Online reputation damage refers to the negative consequences of inappropriate activity, cyberbullying, or social media posts that might ruin a child's reputation or future possibilities.

The comments set is set up for evaluators to assess the objects, with Y as an assessment index set: Y = {y1, y2... yn}. Because risk is a function of chance and impact, two separate evaluation sets are created. Table 2 illustrates the interpretation of the assessment set $Y_p = \{Y_{p1}, Y_{p2}...Y_{p5}\}$ of the risk factor set X for the risk likelihood, Rp.

Table 2 *Description of the risk likelihood*

Risk Likelihood	Likelihood Description
Y_{p1}	Never
Y_{p2}	Once in a while
Y_{p3}	Often
Y_{p4}	Very often
Y_{p5}	Always

Table 3 displays the assessment set $Y_c = \{Y_{c1}, Y_{c2}...Y_{c5}\}$ of risk factor set X and the implications for risk impact, R_c.

Table 3 *Description of the risk impact level*

Risk Impact	Impact Description
Y_{c1}	Have minimal consequences, often limited to minor inconvenience.
Y_{c2}	They have limited impact but are generally manageable and can be easily addressed.
Y_{c3}	Incidents may result in moderate distress or harm that may require support from parents and educators.
Y_{c4}	Have serious consequences necessitating immediate intervention and support.
Y_{c5}	Have severe and potentially life-threatening consequences requiring urgent intervention and crisis management.

J. of Science and Technology Vol. 18 No. 1 (2026) p. 1-12

Each evaluator is assessed using a questionnaire that measures the likelihood and impact of the risk factors, X, as displayed in tables 2 and 3. In this study, the fuzzy assessment level of each evaluator is calculated using the risk matrix shown in Table 4.

Table 4 *Risk matrix*

Risk	Y_{c1}	Y_{c2}	Y_{c3}	Y_{c4}	Y_{c5}
Y_{p1}	Very Low	Very Low	Low	Low	Medium
Y_{p2}	Very Low	Low	Low	Medium	Medium
Y_{p3}	Low	Low	Medium	Medium	High
Y_{p4}	Low	Medium	Medium	High	Very High
Y_{p5}	Medium	Medium	High	Very High	Very High

Risk matrices are often referred to as probability and effect risk matrices. They are a simple tool for increasing risk visibility and assisting management with decision making. A risk matrix is an image-based instrument that helps enterprises comprehend and estimate the probabilities and gravity of potential threats. It is often employed during risk evaluations to help choose which risks giving preference to and which strategies for risk management to implement [23] [24]. A risk matrix is built around two overlapping factors: the possibility of a risk event happening and the possible consequence of that event. The possibility of risks occurring is often displayed along the Y-axis of the grid. The amount of risk is calculated by multiplying the likelihood and consequence.

Standards-setting agencies and occupational safety researchers have expressed concerns about subjectivity and inconsistency of risk matrices [24] [25]. Therefore, combining fuzzy methods with risk matrix will produce a more accurate result because it will capture uncertainties not captured by the risk matrix [26].

Step 2: Evaluate a single element and create the fuzzy relationship grid, P.

Single-factor fuzzy evaluation requires assessing an element separately while determining its membership degree set ('Y'). One hundred and ten (110) young individuals were brought in to assess the information security risk. These students independently verified the level of the analysed factors in respect to the information security risk. Considering each x_j, p_{ij} denotes the degree of dependency on x_j to v_i.

$$\mathrm{p_{ij}} = \frac{\mathrm{n}}{\mathrm{z}} \tag{6}$$

where n is the sample size of x_j and z is the sum of the experts. P is the fuzzy array of element x_j on grade v_i as seen in equation 7.

$$P = \begin{bmatrix} p_{11} & \cdots & p_{15} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{m5} \end{bmatrix} \tag{7}$$

Step 3: Calculate the fuzzy weight values of the examined factors.

To determine the fuzzy level of each element, the weight w_i *(i = 1, 2..., n)* given to the elements of *'X'* must satisfy the condition that $\mathrm{w_i} \geq 0; \sum \mathrm{w_i} = 1$, representing the i^{th} element weights and constituting the fuzzy weight set, *'W'* for each of the element weights. The weights used in FCE have a significant impact on the ultimate result of the evaluation. In this work, entropy is used to calculate the weights.

Step 4: Get comprehensive results.

The weight, W, multiplies the fuzzy matrix, P, to generate the FCE output vector, B, for each assessed object element. The FCE model is shown in equation 8.

$$\mathrm{B = W \cdot P^T} = (\mathrm{w_1, w_2, \ldots, w_m}) \begin{bmatrix} \mathrm{p_{11}} & \mathrm{p_{21}} & \cdots & \mathrm{p_{n1}} \\ \mathrm{p_{12}} & \mathrm{p_{22}} & \cdots & \mathrm{p_{n2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{p_{1m}} & \mathrm{p_{2m}} & \cdots & \mathrm{p_{nm}} \end{bmatrix} = (\mathrm{b_1, b_2, \ldots, b_n}) \tag{8}$$

Step 5: Determine the conclusion of the result.

The concept of highest integration is used to reach a conclusion about the whole assessment. That is, the evaluation will be according to the greatest value of B. The outputs of B are categorized into the five risk levels as expressed: very low (< 0.26), low ($0.26 \leq \mathrm{B} < 0.42$), medium ($0.42 \leq \mathrm{B} < 0.62$), high ($0.62 \leq \mathrm{B} < 0.78$) and very high ($0.78 \leq \mathrm{B} \leq 1$).

3. Results and Discussion

The rapid development of the internet and social media has fundamentally altered how people interact, communicate, and show themselves online. Understanding the impact of online presence on different aspects of life is critical, especially for university students who are frequent users of digital platforms. This study gives the results of a systematic questionnaire with both quantitative and qualitative questions designed to assess the potential risks of online presence on young people from various fields. The questionnaire includes demographic questions such as age and gender, as well as questions about the frequency with which people use social media platforms and their awareness and attitudes regarding data privacy and security. The survey included 110 students, who represented a broad sample in terms of age, gender, and academic background. This diversity ensures that the findings provide a comprehensive view of the influence of online presence among university students. Table 5 displays the complete results from the demographic portion of the questionnaire, providing an extensive overview of the influence of online presence on the participating students.

Table 5 *Demographic information for internet presence*

Characteristics	Sub-Characteristics	Percentage Value
Gender	Male	63.6%
	Female	36.4%
Age	12-15years	2.7%
	16-19years	70.9%
	20-24 years	26.4%
Age of first access to the internet without adult supervision	4-6 years	4.5%
	7-10 years	20.9%
	11-12 years	25.5%
	13-15 years	33.6%
	Above 16 years	15.5%
Frequency of antivirus update	0-12 months	32.7%
	1-3 years	25.5%
	Above 3 years	1.8%
	Not at all	22.7%
	Do not have	17.3%
Frequency of viewing social media daily	Less than an hour	7.3%
	1-3 hours	30.9%
	4-6 hours	36.4%
	7-11 hours	17.3%
	12-18 hours	8.2%
Frequency of post on social media daily	Less than an hour	61.8%
	1-3 hours	10.9%
	4-6 hours	6.4%
	7-11 hours	2.7%
	12-18 hours	18.2%
Level of parental involvement	Never	28.2%
	Occasionally	47.3%
	Often	15.5%
	Very often	4.5%
	Always	4.5%

J. of Science and Technology Vol. 18 No. 1 (2026) p. 1-12

According to table 5, majority of them are in their late teens; they began using the internet unsupervised in their early teens; they often update their antivirus software; and spend an average of five hours each day on social media. However, majority of them post information on social media platforms for less than an hour each day. Furthermore, just a couple of parents get involved with their children's internet activities. Table 6 displays the students' risk evaluation reports based on the probability and impact of the risk factors.

Table 6 *Evaluator's risk assessment level*

Risk Factors/ Risk Level	Very Low	Low	Medium	High	Very High
Cyberbullying	54	46	8	2	0
Online Predators	54	42	10	3	1
Privacy Breaches	59	36	12	2	1
Social Engineering	45	46	19	0	0
Inappropriate Content	29	42	32	6	1
Addictive Behavior	1	35	46	19	9
Online Scams	38	36	30	6	0
Device Security	53	39	16	2	0
Location Tracking	43	46	18	1	2
Online Reputation Damage	10	18	35	12	35

Table 6, for example, shows that majority of them have a very low risk of cyberbullying, online predators, privacy breaches, and device security. Table 6 was constructed using the risk matrix shown in Table 4. The output from table 6 was utilized to compute the fuzzy matrix, P, for each single-level factor using equations 6 and 7.

The single-factor risk evaluation matrices are:

$$P_1 = \begin{bmatrix} 0.491 & 0.418 & 0.073 & 0.018 & 0 \\ 0.491 & 0.382 & 0.091 & 0.027 & 0.009 \\ 0.536 & 0.327 & 0.109 & 0.018 & 0.009 \\ 0.409 & 0.418 & 0.173 & 0 & 0 \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 0.264 & 0.382 & 0.291 & 0.055 & 0.009 \\ 0.009 & 0.318 & 0.418 & 0.173 & 0.082 \\ 0.345 & 0.327 & 0.273 & 0.055 & 0 \end{bmatrix}$$

$$P_3 = \begin{bmatrix} 0.482 & 0.355 & 0.145 & 0.018 & 0 \\ 0.391 & 0.418 & 0.164 & 0.009 & 0.018 \\ 0.091 & 0.164 & 0.318 & 0.109 & 0.318 \end{bmatrix}$$

The associated fuzzy weight values were calculated using the entropy approach, as shown in equations 2 to 5. The following fuzzy weights were generated by applying the entropy approach, as specified in equations 2 to 5.

$$W = [0.586 \quad 0.236 \quad 0.178]$$
$$W_1 = [0.275 \quad 0.233 \quad 0.241 \quad 0.251]$$
$$W_2 = [0.322 \quad 0.322 \quad 0.356]$$
$$W_3 = [0.476 \quad 0.413 \quad 0.111]$$

Table 7 shows the detailed weights obtained for each risk factor and sub-factors.

Table 7 *Entropy weights for the risk factors*

	Weight	Overall Weight
Sub-factor Layer		
Cyberbullying	0.275	0.142
Online Predators	0.233	0.120
Privacy Breaches	0.241	0.124
Social Engineering	0.251	0.130
Inappropriate	0.322	0.074
Addictive Behavior	0.322	0.074
Online Scams	0.356	0.082
Device Security	0.476	0.121
Location Tracking	0.413	0.105
Online Reputation	0.111	0.028
Main Factors		
Direct Harmful	0.586	
Content-related Risks	0.236	
Security & Reputation concerns	0.178	

The values in the second column represent the weights of the sub-factors in relation to their respective main factors. For example, cyberbullying has a weight of 0.275 when compared to the primary factor of direct harmful interactions. Additionally, the component of direct harmful interactions carries more weight than the other key variables. Furthermore, the results of the overall weights suggest that cyberbullying causes the most concern among the other sub-factors. The weights of the sub-factors will be used to conduct the single-factor evaluation, while the weights of the main factors will be used for the multi-factor assessment. To obtain the FCE outputs, these weights are multiplied by their corresponding fuzzy matrices, as shown in equation 8.

The outputs for the single-factor FCE are:

$$B_1 = [0.4813 \quad 0.3878 \quad 0.1108 \quad 0.0158 \quad 0.0043]$$
$$B_2 = [0.2107 \quad 0.3419 \quad 0.3255 \quad 0.0926 \quad 0.0293]$$
$$B_3 = [0.4010 \quad 0.3597 \quad 0.1721 \quad 0.0245 \quad 0.0427]$$

The multi-factor assessment outputs are derived by multiplying the risk factor weights, W, with the single-factor evaluation matrix, P. The matrix, P, is produced using equation 9.

$$P = \begin{bmatrix} B_1 \\ B_2 \\ B_3 \end{bmatrix} \tag{9}$$

$$\therefore B = [0.403 \quad 0.372 \quad 0.172 \quad 0.036 \quad 0.017]$$

The final stage is to use the maximal membership principle to draw conclusions about the entire assessment. The risk's maximum membership is 0.403. This shows that the overall risk level of the students' online presence falls in the low category. Several variables could have contributed to the students' low degree of online risk exposure. These elements may include some level of parental supervision and guidance, digital literacy knowledge, and school workshops and seminars that promote safe online behaviour.

To evaluate the outcome of the FCE, a different set of weights were applied. These weights were obtained using the Analytic Hierarchy Process (AHP). AHP is a MCDM tool used to rank alternatives based on pair-wise comparisons. It involves several steps as seen in the following steps.

Procedure 1: Build the hierarchy. This is displayed in Table 1.

Procedure 2: Generate the pairwise comparison matrix as shown in equation 10. This was decided by two stakeholders.

J. of Science and Technology Vol. 18 No. 1 (2026) p. 1-12

$$A = \begin{bmatrix} 1 & \frac{w_1}{w_2} & \cdots & \frac{w_1}{w_n} \\ \frac{w_2}{w_1} & 1 & \cdots & \frac{w_2}{w_n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{w_n}{w_1} & \frac{w_n}{w_2} & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad (10)$$

where w_1 = weight of element 1, w_2 = weight of element 2, w_n = weight of element n.

Procedure 3: Normalize the matrix as expressed in equation 11.

$$X_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \quad (11)$$

Procedure 4: Calculate the weight vector as shown in equation 12.

$$W_{ij} = \frac{\sum_{j=1}^{n} X_{ij}}{n} \quad (12)$$

Procedure 5: Check the consistency of the judgments by computing the consistency index and the consistency ratio using equations 13 and 14 respectively.

$$CI = \frac{\lambda_{max} - n}{n-1} \quad (13)$$

where n is the order of matrix and λ_{max} is the eigen value.

$$CR = \frac{CI}{RI} \quad (14)$$

The value of RI, random index is seen in the standard random consistency index displayed in Table 8.

Table 8 *Random Consistency Index* [27]

n	1	2	3	4	5	6	7	8	9	10
RI	0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49

If CR ≤ 0.1, then the judgment is suitable, else the judgment should be re-examined.

The pair-wise comparison matrices for the risk subfactors are represented by A_1, A_2 and A_3. The resultant weight and consistency ratio for each are also given.

$$A_1 = \begin{bmatrix} 1 & 5 & 7 & 3 \\ \frac{1}{5} & 1 & 2 & \frac{1}{4} \\ \frac{1}{7} & \frac{1}{2} & 1 & \frac{1}{6} \\ \frac{1}{3} & 4 & 6 & 1 \end{bmatrix}$$

$$W_1 = [0.558 \quad 0.095 \quad 0.057 \quad 0.290]$$

$$CR_1 = 0.044$$

$$A_2 = \begin{bmatrix} 1 & \frac{1}{5} & 3 \\ 5 & 1 & 7 \\ \frac{1}{3} & \frac{1}{7} & 1 \end{bmatrix}$$

$$W_2 = [0.188 \quad 0.731 \quad 0.081]$$

$$CR_2 = 0.068$$

$$A_3 = \begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{6} \\ 2 & 1 & \frac{1}{5} \\ 6 & 5 & 1 \end{bmatrix}$$

$$W_3 = [0.102 \quad 0.172 \quad 0.726]$$

$$CR_3 = 0.03$$

The decision matrix of the risk factors is represented by A.

$$A = \begin{bmatrix} 1 & \frac{1}{5} & \frac{1}{3} \\ 5 & 1 & 3 \\ 3 & \frac{1}{3} & 1 \end{bmatrix}$$
$$W = [0.105 \quad 0.637 \quad 0.258]$$
$$CR = 0.04$$

The consistency ratios for the sub-risk factors and risk factors are less than 0.1, which indicates that the judgments are acceptable.

These AHP weights are applied to the fuzzy matrices to generate the AHP-FCE outputs using equations 8 and 9.

The outputs for the single-factor AHP-FCE are:

$$B_1 = [0.4698 \quad 0.4095 \quad 0.1055 \quad 0.0138 \quad 0.0014]$$
$$B_2 = [0.0842 \quad 0.3309 \quad 0.3825 \quad 0.1409 \quad 0.0615]$$
$$B_3 = [0.1824 \quad 0.2269 \quad 0.2740 \quad 0.0826 \quad 0.2341]$$

Therefore, the multi-factor assessment for the AHP-FCE is:

$$B = [0.1500 \quad 0.3123 \quad 0.3254 \quad 0.1125 \quad 0.0997]$$

Based on the principle of maximum membership, the highest value is 0.3254, which also falls in the low category. The outcome of the AHP-FCE validates the Entropy-FCE approach.

4. Conclusion

This study developed a strategy for categorizing online risk elements and analyzing the information security risk level of young people's online presence, using a university campus as an instance of study. Three main risk factors were investigated, each of which included some sub-factors. The students' risk levels were found to be low using the Entropy-FCE method. The result was validated using AHP-FCE approach. However, if adequate precautions, such as digital literacy, are not consistently implemented, the risk level may rise to medium. Therefore, youths should be taught cybersecurity. In current technological age, cybersecurity knowledge should be considered as important as the capacity to read, write, and calculate. Finally, assessing and preventing online hazards faced by children is critical to protecting their well-being, rights, and future possibilities in the digital era. Understanding the specific threats and vulnerabilities of young people in the online environment, and adopting proactive efforts to address them, allows us to create a safer, more inclusive digital society in which children may grow and reach their full potential.

Acknowledgment

Special thanks to the students of Elizade University who supported this study.

Conflict of Interest

Author declares that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

References

[1] OECD (2011-05-02), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD Publishing, Paris. http://dx.doi.org/10.1787/5kgcjf71pl28-en

[2] Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., & Sirivianos, M. (2016). Cyber Security Risks for Minors: A taxonomy and a software architecture. IEEE. https://doi.org/10.1109/smap.2016.7753391

[3] Chang, L. (2021). Application of fuzzy comprehensive evaluation based on genetic algorithm in psychological measurement. Scientific Programming, 2021, 1–11. https://doi.org/10.1155/2021/9607006

[4] El-Araby, A., Sabry, I., & El-Assal, A. (2022). A Comparative Study of Using MCDM Methods Integrated with Entropy Weight Method for Evaluating Facility Location Problem. Operational Research in Engineering Sciences: Theory and Applications/Operational Research in Engineering Sciences: Theory and Applications, 5(1), 121–138. https://doi.org/10.31181/oresta250322151a

[5] Dunwen, L., Lei, Y., & Li, B. (2012). Fuzzy-Entropy Theory Comprehensive Evaluation Method and its Application in Building Construction Safety. Procedia Engineering, 43, 137–142. https://doi.org/10.1016/j.proeng.2012.08.024

[6] Zhao, H., Yao, L., Mei, G., Liu, T., & Ning, Y. (2017). A fuzzy comprehensive evaluation method based on AHP and entropy for a landslide susceptibility map. Entropy, 19(8), 396. https://doi.org/10.3390/e19080396

[7] Ma, L., Liu, Y., & Zhou, X. (2011). Fuzzy comprehensive evaluation method of F statistics weighting in identifying mine water inrush source. International Journal of Engineering, Science and Technology &B. Lagos, 2(7). https://doi.org/10.4314/ijest.v2i7.63752

[8] Ml, Z., & Wp, Y. (2012). Fuzzy Comprehensive evaluation method applied in the Real Estate Investment Risks research. Physics Procedia, 24, 1815–1821. https://doi.org/10.1016/j.phpro.2012.02.267

[9] Xu, S., Cui, Y., Yang, C., Wei, S., Dong, W., Huang, L., Liu, C., Ren, Z., & Wei-Liang, W. (2020). The fuzzy comprehensive evaluation (FCE) and the principal component analysis (PCA) model simulation and its applications in water quality assessment of Nansi Lake Basin, China. Environmental Engineering Research/Enviromental Engineering Research, 26(2), 200022–0. https://doi.org/10.4491/eer.2020.022

[10] Deng, X., & Xiang, X. (2023). Fuzzy comprehensive evaluation method for evaluating stability of loess slopes. Advances in Civil Engineering, 2023, 1–15. https://doi.org/10.1155/2023/6692746

[11] Feng, C., Liu, Y., Yuan, Y., & Taghizadeh–Hesary, F. (2022). The application of an improved fuzzy comprehensive evaluation in coal quality rating: The Case Study of China. Frontiers in Energy Research, 9. https://doi.org/10.3389/fenrg.2021.752472

[12] Li, Y., Sun, Z., Han, L., & Mei, N. (2017). Fuzzy comprehensive evaluation method for energy management systems based on an internet of things. IEEE Access, 5, 21312–21322. https://doi.org/10.1109/access.2017.2728081

[13] Brodny, J. (2021). Assessing the level of digital maturity of enterprises in the Central and Eastern European countries using the MCDM and Shannon's entropy methods. PloS One, 16(7), e0253965. https://doi.org/10.1371/journal.pone.0253965

[14] Ma, H., Sun, Z., & Fang, C. (2020). Risk assessment of transnational oil investment in Central Asia using a fuzzy comprehensive evaluation method. Regional Sustainability, 1(1), 11–19. https://doi.org/10.1016/j.regsus.2020.06.002

[15] Yu, L., Cui, K., & Zhang, X. (2022). Research on Fuzzy Comprehensive Evaluation Method in Wireless Sensor Network Course Evaluation. Academic Journal of Science and Technology, 3(2), 174–177. https://doi.org/10.54097/ajst.v3i2.2165

[16] Zhang, P., & Guoqing, F. (2018). Application of fuzzy comprehensive evaluation to evaluate the effect of water flooding development. Journal of Petroleum Exploration and Production Technology, 8(4), 1455–1463. https://doi.org/10.1007/s13202-018-0430-y

[17] Azim, M. (2017). Security assessment model for a cloud-based e-Governance system based on Fuzzy Comprehensive Evaluation Method. International Journal of Computer Science and Information Security (IJCSIS), 15(4), 66–77. https://sites.google.com/site/ijcsis/

[18] Hussain, A. I., & Mandal, K. (2016). Entropy based MCDM approach for selection of material. National Level Conference on Engineering Problems and Application of mathematics.

[19] Hu, R. and Zhang, C.F. (2018) An Empirical Study on Fuzzy Comprehensive Evaluation of Red Tourism Resources Based on AHP. Applied Mathematics, 9, 171-177. https://doi.org/10.4236/am.2018.92012

[20] Mou, N., Wang, C., Yang, T., & Zhang, L. (2020). Evaluation of development potential of ports in the Yangtze River Delta using FAHP-Entropy Model. Sustainability, 12(2), 493. https://doi.org/10.3390/su12020493

[21] Ma, S., He, J., & Shuai, X. (2011). Application of fuzzy comprehensive evaluation method in trust quantification. ˜the œInternational Journal of Computational Intelligence Systems/International Journal of Computational Intelligence Systems, 4(5), 768. https://doi.org/10.2991/ijcis.2011.4.5.3

[22] Aliu, M., Ayeni, A., Thompson, F., & Alese, K. (2020). Information Security risk analysis using analytic hierarchy process and fuzzy comprehensive evaluation. International Journal of Computer Science and Information Security (IJCSIS), 18(6), 36–45. https://sites.google.com/site/ijcsis/ISSN 1947-5500

[23] Mustafa Elmontsri (2014). Review of the strengths and weaknesses of risk matrices. Atlantis Press

[24] Thomas, P., Bratvold, R. B., & Eric Bickel, J. (2014, March 27). The Risk of Using Risk Matrices. SPE Economics & Management, 6(02), 56–66. https://doi.org/10.2118/166269-pa

[25] Ball, D. J. and Watt, J. (2013), Further Thoughts on the Utility of Risk Matrices. Risk Analysis, 33: 2068–2078

[26] Zaky, M. (2018, October 2). Risk Analysis using Fuzzy System based Risk Matrix Methodology. Arab Journal of Nuclear Sciences and Applications, 51(4), 204–212. https://doi.org/10.21608/ajnsa.2018.2448.1047

[27] Saaty, T. L. (1980). The Analytical Hierarchy Process: Planning, Priority Setting. *Resource Allocation. McGraw-Hill, New York, NY, USA.*