Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

AI and Cybersecurity: Combating Deepfakes and Misinformation in Nepal

Anu Kumari
International Master in Business Administration, University of Wolverhampton, Wolverhampton, United Kingdom
Herald College Kathmandu, Nepal
theanukumari27@gmail.com

Type of Research: Original Research
Received: April 30, 2026; Revised & Accepted: June 29, 2026

Abstract

Background: The rapid expansion of artificial intelligence (AI) and digital communication platforms has intensified concerns regarding deepfakes and misinformation, particularly in developing contexts like Nepal. These challenges pose risks to information integrity, public trust, and digital security, necessitating effective mitigation strategies.

Methods: This study employs a quantitative research design using primary data collected through a structured online questionnaire. The questionnaire was shared with approximately 500 individuals across Nepal, of whom 400 respondents completed the survey and met the study requirements for final analysis, resulting in a response rate of 80%. A total of 400 responses were obtained using purposive sampling. All variables were measured using a five-point Likert scale. Data were analyzed using SPSS through descriptive statistics, cross-tabulation, Pearson correlation, and multiple linear regression analysis.

Results: The findings reveal that Public Awareness Campaigns and Digital Literacy significantly and positively influence the effectiveness of combating deepfakes and misinformation. Regression analysis indicates that Public Awareness Campaigns ($B = 0.476$, $p < 0.001$) and Digital Literacy ($B = 0.177$, $p = 0.008$) are significant predictors, while Cybersecurity Infrastructure, Government Policies, and Social Media Platform Measures show non-significant or weak effects. The model is statistically significant ($F = 42.983$, $p < 0.001$) and the model explains 35.3% of the variance ($R^2 = 0.353$, $F = 42.983$, $p < 0.001$).

Conclusion: The study concludes that human-centered factors, particularly awareness and education, are more influential than institutional or technological measures in combating deepfakes and misinformation in Nepal. Strengthening digital literacy and public awareness is essential for improving digital resilience.

Novelty: This study provides empirical evidence from Nepal highlighting the comparative dominance of human-centric factors over institutional mechanisms in addressing AI-driven misinformation challenges.

Keywords: Digital literacy, public awareness, Cyber resilience, Information integrity, Digital education

Introduction

Artificial Intelligence (AI) has rapidly transformed the digital information ecosystem by enabling machines to generate, analyze, and distribute content at an unprecedented scale. Recent studies highlight that generative AI systems have fundamentally altered how digital information is produced and consumed across online platforms (Westerlund, 2021). This transformation has increased both efficiency and risk within information systems, particularly in relation to authenticity and trust. As AI systems become more advanced, concerns regarding synthetic media and misinformation have intensified across global digital environments (Kietzmann et al., 2021).

Deepfake technology represents one of the most disruptive applications of AI, enabling the creation of highly realistic synthetic audio-visual content. These systems rely on deep learning models that can replicate human facial expressions, voice patterns, and behaviors with high accuracy (Mirsky & Lee, 2021). Such capabilities raise serious concerns regarding identity manipulation, fraud, and digital deception. Scholars emphasize that deepfakes significantly challenge traditional methods of verifying truth in digital communication systems (Vaccari & Chadwick, 2020).

The advancement of generative adversarial networks (GANs) has further accelerated the development of deepfake technologies. These models operate through adversarial training, where two neural networks compete to improve the realism of generated content (Tolosana et al., 2021). Misinformation has significant implications for political communication and public trust in digital systems. Studies show that exposure to manipulated or false content reduces confidence in online information sources and increases uncertainty among users (Lazer et al., 2020). Additionally, deepfakes can influence political discourse by fabricating speeches and events involving public figures (Bennett & Livingston, 2021).

The rapid proliferation of social media platforms has significantly reshaped the dynamics of information dissemination in the digital age. Algorithm-driven recommendation systems prioritize engagement-based metrics, often amplifying emotionally charged or sensational content regardless of its factual accuracy. This structural design enables misleading information to spread rapidly across interconnected user networks, often reaching large audiences before verification mechanisms can intervene (Cinelli et al., 2021; Zannettou et al., 2022). Consequently, the velocity and scale of misinformation diffusion have become critical challenges for digital governance and platform accountability.

Cybersecurity researchers have increasingly emphasized the importance of explainable artificial intelligence in combating misinformation and deepfake threats. Traditional black-box AI models often lack transparency, making it difficult for users and institutions to understand how detection decisions are made. Explainable AI frameworks aim to improve trust and accountability by providing interpretable outputs and decision pathways within detection systems (Adadi & Berrada, 2018; Vilone & Longo, 2021). This transparency is particularly important in high-risk environments where inaccurate classification of synthetic media can have serious social and political consequences.

The growing integration of artificial intelligence into communication platforms has also transformed the nature of online influence operations. Automated bots and AI-driven recommendation systems are increasingly capable of shaping online narratives, manipulating trending discussions, and amplifying divisive content at scale. Studies indicate that coordinated AI-supported disinformation campaigns can influence public sentiment and distort digital discourse across multiple platforms simultaneously (Ferrara et al., 2020; Cresci, 2021). Such developments highlight the strategic use of AI in information warfare and online manipulation.

Educational institutions and researchers have highlighted the growing importance of media literacy in strengthening societal resilience against misinformation. Digital literacy programs that focus on fact-checking, source verification, and critical thinking skills have shown positive effects in reducing susceptibility to manipulated content. Studies suggest that users with stronger media literacy competencies are more capable of identifying deceptive narratives and resisting misinformation exposure (Guess et al., 2021; Jones-Jang et al., 2021). Therefore, education-based interventions are increasingly recognized as essential components of long-term misinformation mitigation strategies.

The increasing dependence on AI-driven technologies has also exposed weaknesses in global digital governance structures. International organizations and policymakers continue to struggle with establishing unified standards for AI ethics, misinformation regulation, and platform accountability. Differences in national legal systems and technological capabilities create inconsistencies in how deepfake-related threats are addressed globally (UNESCO, 2021; European Commission, 2022). This fragmented governance landscape limits coordinated responses to transnational misinformation campaigns and AI-enabled cyber threats.

Based on the above discussion, the major objective of this study is to examine the effectiveness of strategies used to detect and reduce deepfakes and misinformation in Nepal. In line with this objective, the primary research question of the study is: "How can deepfakes and misinformation be effectively identified and controlled in Nepal?" In general, prior studies suggest that technological capabilities, institutional frameworks, and public awareness play a significant role in reducing the spread of AI-generated misinformation. Accordingly, it is hypothesized that there is a significant relationship between Cybersecurity Infrastructure (CI) and Combating Deepfakes and Misinformation (CDM), as advanced cybersecurity systems improve the detection and prevention of manipulated digital content. Moreover, there is a significant relationship between Digital Literacy (DL) and CDM, as digitally literate individuals are more capable of recognizing and verifying false information. Furthermore, there

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

is a significant relationship between Government Policies and Regulations (GPR) and CDM, as effective legal and regulatory mechanisms help control the misuse of deepfake technologies. In addition, there is a significant relationship between Social Media Platform Measures (SMPM) and CDM, as platform-level monitoring and content moderation reduce the dissemination of misinformation. Similarly, there is a significant relationship between Public Awareness Campaigns (PAC) and CDM, as awareness initiatives enhance users' ability to critically evaluate online content and resist misinformation. Consequently, this study seeks to empirically test these relationships using primary quantitative data in the Nepalese context.

Review of Literature

The rapid advancement of artificial intelligence (AI) has transformed the creation and dissemination of digital content, leading to the emergence of deepfake technologies capable of generating highly realistic synthetic audio, image, and video content. Recent studies indicate that deepfakes pose substantial challenges to information authenticity, public trust, and digital security because manipulated media can be difficult for ordinary users to distinguish from genuine content (Westerlund, 2021; Mirsky & Lee, 2021). As generative AI models continue to improve, the accessibility of deepfake creation tools has expanded beyond technical experts, increasing the likelihood of misuse in social, political, and commercial contexts (Matli, 2026). Consequently, researchers have identified deepfake technology as a growing threat to the integrity of digital information ecosystems and democratic communication processes.

The proliferation of deepfakes has intensified concerns regarding misinformation and disinformation across online platforms. Empirical evidence suggests that synthetic media can manipulate public opinion, distort political discourse, and reduce confidence in credible information sources (Vaccari & Chadwick, 2020; Cinelli et al., 2021; Pennycook & Rand, 2021). Social media algorithms often prioritize highly engaging content, enabling misleading information to spread rapidly among users before verification can occur (Cinelli et al., 2021). Furthermore, psychological research demonstrates that repeated exposure to false information can increase perceived credibility, making users more vulnerable to misinformation campaigns and digitally manipulated narratives (Pennycook & Rand, 2021). These findings highlight the need to understand both technological and behavioral dimensions of misinformation dissemination.

From a cybersecurity perspective, deepfakes have introduced sophisticated attack vectors involving impersonation, fraud, and identity manipulation. Research shows that AI-generated voice and video content can be exploited in phishing schemes, social engineering attacks, and biometric authentication bypass attempts. The increasing realism of synthetic media has created new challenges for organizations seeking to secure communication systems and verify digital identities. As a result, cybersecurity researchers emphasize the importance of developing advanced detection mechanisms capable of identifying manipulated content before it causes financial, reputational, or operational damage (Farid, 2022) .

The increasing sophistication of artificial intelligence has intensified concerns regarding society's ability to distinguish authentic information from manipulated digital content. Recent research suggests that deepfake technologies exploit cognitive limitations in information processing, making users more susceptible to deception when evaluating online media (Groh et al., 2022; Köbis et al., 2021). Studies further indicate that misinformation becomes particularly influential when individuals lack adequate digital competencies and source-verification skills, reducing their capacity to critically assess online content (Clayton et al., 2020; Guess et al., 2020).

In response to the growing threat of deepfakes, scholars have proposed a range of technological and governance-based solutions. Research demonstrates that forensic detection techniques based on physiological inconsistencies, facial artifacts, and multimodal analysis can improve the identification of manipulated media (Verdoliva, 2020; Pu et al., 2023). At the same time, regulatory scholars emphasize the importance of platform accountability, transparency requirements, and ethical AI governance frameworks to reduce the misuse of synthetic content in political and social contexts (Gorwa et al., 2020; de Gregorio, 2022).

In Context to Nepal, increasing dependence on digital technologies has transformed how information is created, shared, and consumed across society. Research examining social media manipulation in Nepal found that digital platforms can be strategically used to shape public opinion and influence information flows, creating challenges for information authenticity and trust (Bhandari, 2024). Similarly, studies of Nepal's digital economy indicate that rapid technological adoption has outpaced institutional preparedness, creating vulnerabilities in information governance and digital regulation (Pokharel, 2023). Furthermore, investigations into cybersecurity awareness among Nepalese students suggest that practical understanding of online threats remains limited, reducing users' capacity to identify and respond to misinformation and other digital risks (Adhikari et al., 2025). These findings collectively demonstrate that Nepal's digital transformation has created new challenges for maintaining information integrity and cybersecurity resilience.

From a socio-political perspective, misinformation and digital manipulation are increasingly linked to changing patterns of online communication and civic engagement in Nepal. Research on digital literacy and democratic participation highlights that citizens' ability to critically evaluate online content significantly influences their susceptibility to misinformation and political manipulation (Timalsina, 2025). In addition, studies exploring political communication on social media show that emotionally driven narratives and digitally mediated political identities can amplify misleading information and ideological polarization (Chapagain & Pulami, 2025). Together, these studies suggest that strengthening digital literacy, regulatory capacity, and public awareness is essential for mitigating misinformation and enhancing the security of Nepal's digital information ecosystem.

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Methods

This study follows a quantitative research approach using descriptive and causal-comparative research designs to analyze the factors affecting the control and prevention of deepfakes and misinformation in Nepal. The research is based on primary information gathered through a structured questionnaire prepared to understand respondents' opinions, experiences, and awareness regarding AI-generated misinformation and cybersecurity practices. In addition, the questionnaire is divided into two parts: demographic details (including gender, age, Marital Status, Qualification, Income, occupation, frequency of internet, familiarity with AI or Cybersecurity concepts and experience with misinformation/deepfakes online) and statements related to the study variables measured through a five-point Likert scale ranging from strongly disagree to strongly agree. The target respondents of the study are individuals aged below 20 years to 50 years and above. Who regularly use digital media and social networking platforms. Furthermore, purposive sampling is applied to collect responses from participants who have exposure to online communication and internet-based information systems.

Participation in the study was voluntary, and informed consent was obtained from all respondents before data collection. The responses were kept anonymous and used only for academic purposes. All collected data were stored securely and treated confidentially in accordance with ethical research guidelines.

The study is conducted within the Nepalese context, focusing on people who actively engage with digital platforms. Accordingly, data are collected from 400 respondents. For the purpose of analysis, both descriptive statistical tools (such as frequency and percentage) and inferential statistical methods (including correlation and regression analysis) are performed using SPSS software. Additionally, the consistency and dependability of the measurement scale are evaluated using statistical techniques such as Cronbach's alpha. Therefore, this research methodology helps ensure the credibility, consistency, and precision of the study findings.

Data for this study were collected between September 3, 2025, and January 21, 2026, through a structured questionnaire distributed using online platforms. The study covered respondents from across Nepal and employed purposive sampling to select participants who actively use digital media and social networking platforms. For the purpose of this study, regular digital media users were defined as individuals aged 20 years and above who access social media, online news portals, or other internet-based communication platforms multiple times per week. Prior to the main survey, a pilot study was conducted with 50 respondents to assess the clarity and reliability of the questionnaire. The pilot responses were analyzed using Cronbach's alpha to evaluate the internal consistency of the measurement items.

Table 1: Cronbach's Alpha Results for the Pilot Study

Variables	No. of items	Cronbach's Alpha
All Variables	30	0.950
Combating Deepfakes and Misinformation (CDM)	5	0.909
Cybersecurity Infrastructure (CI)	5	0.904
Digital Literacy (DL)	5	0.888

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Government Policies and Regulations (GPR)	5	0.930
Social Media Platform Measures (SMPM)	5	0.890
Public Awareness Campaigns (PAC)	5	0.938

The table presents the reliability results of the study variables using Cronbach's alpha. The overall scale shows excellent internal consistency ($\alpha = 0.950$), while all individual constructs report strong reliability with alpha values above 0.70. This indicates that the measurement items are reliable and appropriate for further analysis.

Similarly, this study applies a multiple linear regression model to evaluate the impact of different factors on combating deepfakes and misinformation. In this model, Combating Deepfakes and Misinformation (CDM) is considered the dependent variable, whereas Cybersecurity Infrastructure (CI), Digital Literacy (DL), Government Policies and Regulations (GPR), Social Media Platform Measures (SMPM), and Public Awareness Campaigns (PAC) are considered independent variables. The regression model is presented as:

$$CDM = \beta_0 + \beta_1 CI + \beta_2 DL + \beta_3 GPR + \beta_4 SMPM + \beta_5 PAC + \varepsilon$$

Here, β_0 indicates the constant value, β_1–β_5 represent the coefficients of the independent variables, and ε denotes the error term. The regression analysis is conducted using SPSS software to examine the significance, direction, and overall relationship between the dependent and independent variables.

Measurement of Variables

The study variables were measured using multiple-item scales based on a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. The questionnaire was developed based on existing literature related to deepfakes, misinformation, cybersecurity, digital literacy, public awareness, and platform governance, with modifications made to suit the Nepalese context. Each construct was measured using a set of statements designed to capture respondents' perceptions and experiences regarding the factors influencing the effectiveness of combating deepfakes and misinformation.

Table2: Measurement of Variables

(Table 2 presents the operational definition of each variable, the number of items used to measure the construct, and sample questionnaire statements.)

Variable	Definition	No. of Items	Sample Item
Combating Deepfakes and Misinformation (CDM)	Effectiveness of efforts to identify and control deepfakes and misinformation	5	Deepfakes and misinformation are a serious threat in Nepal.
Cybersecurity Infrastructure (CI)	Availability and effectiveness of technological systems to detect and prevent digital threats	5	Nepal has strong cybersecurity systems to monitor online content.
Digital Literacy (DL)	Ability to critically evaluate and verify online information	5	I can identify fake videos and news online.

Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Government Policies and Regulations (GPR)	Effectiveness of laws and regulations addressing misinformation	5	Government policies are enforced properly to combat misinformation.
Social Media Platform Measures (SMPM)	Actions taken by platforms to identify and remove misleading content	5	Social media platforms actively remove fake content from Nepal.
Public Awareness Campaigns (PAC)	Public education initiatives related to misinformation and deepfakes	5	Awareness campaigns improve understanding of deepfakes and misinformation.

Result and Discussion

The data and information collected from the respondents are presented, interpreted, and analyzed in this chapter. The questionnaire was administered using a purposive sampling approach to obtain relevant data. The collected data were entered into SPSS for further analysis. Techniques such as frequency table, correlation, regression, and reliability analysis are presented and interpreted to examine the relationships between the study variables.

Table 3: Reliability Analysis of Variables

(Table 3 presents the reliability statistics for the study variables, measured using Cronbach's Alpha. The table displays the number of items associated with each variable, including Combating Deepfakes and Misinformation (CDM), Cybersecurity Infrastructure (CI), Digital Literacy (DL), Government Policies and Regulations (GPR), Social Media Platform Measures (SMPM), and Public Awareness Campaigns (PAC). The Cronbach's Alpha values indicate the internal consistency of each variable, with higher values reflecting greater reliability in the measurement scale.)

Variables	No. of items	Cronbach's Alpha
All Variables	30	0.930
Combating Deepfakes and Misinformation (CDM)	5	0.928
Cybersecurity Infrastructure (CI)	5	0.918
Digital Literacy (DL)	5	0.868
Government Policies and Regulations (GPR)	5	0.934
Social Media Platform Measures (SMPM)	5	0.923
Public Awareness Campaigns (PAC)	5	0.939

Source: SPSS, (2026)

The overall Cronbach's Alpha value for all variables in the study was 0.930, indicating excellent internal consistency across the questionnaire. This suggests that the measurement items are highly reliable and appropriate for further statistical analysis. The dependent variable,

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Combating Deepfakes and Misinformation (CDM), recorded a Cronbach's Alpha value of 0.928, demonstrating strong reliability in measuring respondents' ability to identify and respond to manipulated digital content. Among the independent variables, Cybersecurity Infrastructure (CI) showed a value of 0.918, indicating reliable measurement of technological security systems. Digital Literacy (DL) recorded 0.868, reflecting consistent measurement of respondents' ability to evaluate online information and detect misinformation.

Similarly, Government Policies and Regulations (GPR) achieved a value of 0.934, indicating strong reliability in measuring regulatory and policy responses to misinformation. Social Media Platform Measures (SMPM) recorded 0.923, demonstrating reliable measurement of platform-level moderation and detection mechanisms. The variable Public Awareness Campaigns (PAC) showed the highest reliability with 0.939, indicating strong internal consistency in measuring awareness and educational initiatives. These results confirm that all variables exceed the acceptable reliability threshold, supporting the validity of the measurement instruments and ensuring that the data collected are suitable for further statistical analyses such as correlation and regression.

Descriptive Analysis

Table 4: Descriptive Analysis of the variables

Variables	Category	Percent
Gender	Male	50.2
	Female	49.8
Age	Below 20	14.0
	20-30	72.8
	30-40	11.0
	40-50	2.0
	50 & above	.3
Marital Status	Married	15.8
	Unmarried	84.3
Qualification	SLC/SEE or Below	2.3
	Intermediate/+2	17.0
	Bachelor's Degree	52.5
	Master's Degree	26.8
	MPhil/PHD or Higher	1.5
Occupation	Student	39.3
	Employed	47.5
	Unemployed	5.5
	Entrepreneur/Business Owner	7.8
Income	Under 20,000	39.0
	20,000-30000	18.8
	30,000-40,000	11.8

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

	40,000-50,000	10.0
	50,000 & Above	20.5
Frequency of Internet /Social media Use	Less than 1 hour per day	4.8
	1-3 hours per day	38.5
	4-6 hours per day	32.5
	More than 6 hours per day	24.3
Familiarity with AI or Cybersecurity concepts	Not familiar	6.5
	Somewhat familiar	31.0
	Familiar	42.8
	Very Familiar	19.8
Experience with misinformation/deepfakes online	Never encountered	8.8
	Rarely	28.0
	Occasionally	37.0
	Frequently	26.3

Source: SPSS, (2026)

The descriptive analysis presents the key characteristics of the respondents and provides an overview of their demographic profile. The study includes 400 respondents with a balanced gender distribution, where males account for 50.2% and females 49.8%, ensuring unbiased representation. The age distribution indicates that the majority of respondents (72.8%) fall within the 20–30 age group, followed by smaller proportions in other age categories. Additionally, most respondents are unmarried (84.3%), reflecting a young and digitally active population. This demographic structure is highly relevant, as younger individuals are more engaged with digital platforms and are more likely to encounter deepfakes and misinformation in their daily online activities.

In terms of educational and professional background, the findings show that a majority of respondents are well-educated, with 52.5% holding a bachelor's degree and 26.8% possessing a master's degree. This indicates that over three-quarters of the sample has higher education, enhancing the reliability of responses related to AI and cybersecurity. Occupationally, the respondents are diverse, with 47.5% employed and 39.3% students, while a smaller proportion includes entrepreneurs and unemployed individuals. The income distribution also reflects economic diversity, with the largest group earning below NPR 20,000, followed by respondents in higher income brackets. These factors collectively influence access to digital technologies and exposure to online information environments.

The analysis further highlights respondents' digital behavior and awareness related to AI and misinformation. A significant proportion of respondents spend considerable time on the internet, with most using social media between 1 to 6 hours daily, indicating high digital engagement. In terms of familiarity, the majority reported being either familiar or somewhat

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

familiar with AI and cybersecurity concepts, suggesting a knowledgeable sample. Moreover, exposure to misinformation is widespread, with most respondents encountering deepfakes and misleading content either occasionally or frequently. This high level of exposure emphasizes the importance of effective cybersecurity measures, digital literacy, and public awareness in addressing misinformation challenges in Nepal.

Inferential Analysis

Inferential analysis is used to examine the relationship between the dependent and independent variables of the study. Correlation and regression analysis are performed using SPSS to measure the significance and impact of the selected variables on combating deepfakes and misinformation in Nepal.

Correlation Analysis

Table 5: Correlation Analysis

(This table presents the Pearson correlation coefficients between the dependent variable, Combating Deepfakes and Misinformation (CDM), and the independent variables. The correlation analysis is based on the data from a sample size 400 from the year 2025/26. The independent variables are Cybersecurity Infrastructure (CI), Digital Literacy (DL), Government Policies and Regulations (GPR), Social Media Platform Measures (SMPM), Public Awareness Campaign (PAC).)

Correlations

		CDM	CI	DL	GPR	SMPM	PAC
CDM	Pearson Correlation	1	-.139**	.250**	-.151**	-.114*	.553**
	Sig. (2-tailed)		.005	<.001	.002	.023	<.001
	N	400	400	400	400	400	400
CI	Pearson Correlation	-.139**	1	.517**	.811**	.737**	.042
	Sig. (2-tailed)	.005		<.001	<.001	<.001	.404
	N	400	400	400	400	400	400
DL	Pearson Correlation	.250**	.517**	1	.510**	.502**	.488**
	Sig. (2-tailed)	<.001	<.001		<.001	<.001	<.001
	N	400	400	400	400	400	400
GPR	Pearson Correlation	-.151**	.811**	.510**	1	.730**	.033
	Sig. (2-tailed)	.002	<.001	<.001		<.001	.504
	N	400	400	400	400	400	400
SMPM	Pearson Correlation	-.114*	.737**	.502**	.730**	1	.119*
	Sig. (2-tailed)	.023	<.001	<.001	<.001		.018
	N	400	400	400	400	400	400
PAC	Pearson Correlation	.553**	.042	.488**	.033	.119*	1
	Sig. (2-tailed)	<.001	.404	<.001	.504	.018	
	N	400	400	400	400	400	400

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Source: SPSS, (2026)

The Pearson correlation analysis indicates the relationship between the independent variables (CI, DL, GPR, SMPM, PAC) and the dependent variable (CDM). The results show that Digital Literacy (DL) has a positive and statistically significant relationship with CDM ($r = 0.250$, $p <$

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

0.001), suggesting that higher levels of digital literacy are associated with better effectiveness in combating deepfakes and misinformation. Similarly, Public Awareness Campaigns (PAC) also exhibit a strong positive relationship with CDM (r = 0.553, p < 0.001), indicating that awareness initiatives play a crucial role in improving resilience against AI-generated misinformation. These findings highlight that awareness-based and skill-based factors significantly contribute to strengthening misinformation control mechanisms in Nepal.

In contrast, Cybersecurity Infrastructure (CI) (r = -0.139, p = 0.005), Government Policies and Regulations (GPR) (r = -0.151, p = 0.002), and Social Media Platform Measures (SMPM) (r = -0.114, p = 0.023) show weak but statistically significant negative relationships with CDM. This suggests that despite the existence of institutional and technological measures, their current implementation may not be sufficiently effective in reducing deepfakes and misinformation. The negative direction of these relationships may reflect gaps in enforcement, limited technological capacity, or inefficient policy execution in the Nepalese context.

Furthermore, the intercorrelation among independent variables indicates several moderate to strong relationships, such as CI with GPR (r = 0.811) and GPR with SMPM (r = 0.730), suggesting that these factors are closely interconnected. DL also shows moderate associations with CI (r = 0.517) and SMPM (r = 0.502), indicating overlapping influence among capacity-building and institutional factors. However, since most correlation values remain below the critical threshold of 0.80 (except CI–GPR), multicollinearity concerns are generally manageable, though the CI–GPR relationship may require attention in further regression analysis. Overall, the correlation results confirm that both individual awareness factors and systemic governance elements jointly influence the effectiveness of combating deepfakes and misinformation in Nepal.

Regression Analysis

Table 6: Regression Analysis

(Table shows how well the statistical model fits the survey data from 400 people. B coefficients, t-values, and significance (Sig.) values, indicating the strength and direction of each variable's impact. A p-value less than 0.05 suggests a statistically significant influence, whereas a higher value implies no significant effect on combating deepfakes and misinformation.) It lists four key numbers: R Square tells us how much of the change in people's ability to combat deepfakes is explained by the factors we studied; and the Durbin-Watson number checks that the model's errors are random and not connected to each other.)

Variables	B	T	Sig.	Collinearity Statistics		F	Sig.	R2	DW
				Tolerance	VIF				
(Constant)	2.378	13.717	<.001						
CI	-.057	-.779	.437	.287	3.486				
DL	.177	2.673	.008	.486	2.058				
GPR	-.099	-1.373	.171	.294	3.402	42.983	<.001	.353	1.663
SMPM	-.126	-2.048	.041	.393	2.543				
PAC	.476	10.206	<.001	.689	1.452				

Source: SPSS, (2026)

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Note: Dependent variable: Combating Deepfakes and Misinformation (CDM) and Independent Variables: Cybersecurity Infrastructure (CI), Digital Literacy (DL), Government Policies and Regulations (GPR), Social Media Platform Measures (SMPM), Public Awareness Campaigns (PAC), Unstandardized coefficients (B) reported.

The multiple regression findings demonstrate that the overall model is statistically significant, as shown by the F-value of 42.983 with a p-value below 0.001. This indicates that the independent variables together exert a meaningful influence on Combating Deepfakes and Misinformation (CDM). Furthermore, the R^2 value of 0.353 reveals that roughly 35.3% of the variance in combating deepfakes and misinformation can be accounted for by the selected predictors, reflecting a reasonable level of explanatory strength. This suggests that approximately 64.7% of the variation remains unexplained by the model. Therefore, other factors not examined in this study, such as trust in media, political orientation, social network influence, fact-checking behavior, technological experience, and demographic characteristics, may also contribute to individuals' ability to identify and resist misinformation. Future research should incorporate additional variables to improve the explanatory power of the model and provide a more comprehensive understanding of the determinants of combating deepfakes and misinformation.

Additionally, the Durbin–Watson (DW) statistic of 1.663 lies within the commonly accepted range of 1.5 to 2.5, suggesting that autocorrelation is not a significant concern in the dataset. Thus, the overall regression model is considered dependable and appropriate for further examination.

Looking at each predictor individually, the results show that Digital Literacy (DL) ($\beta = 0.177$, $p = 0.008$) and Public Awareness Campaigns (PAC) ($\beta = 0.476$, $p < 0.001$) have a positive and statistically meaningful effect on combating deepfakes and misinformation. This means that individuals with stronger digital skills and those reached by awareness initiatives are more likely to help identify and resist AI-generated false content. Among the significant predictors, PAC shows the largest coefficient, confirming it as the most dominant factor in this study. Therefore, the hypotheses concerning DL and PAC are supported by the evidence.

In contrast, Cybersecurity Infrastructure (CI) ($\beta = -0.057$, $p = 0.437$), Government Policies and Regulations (GPR) ($\beta = -0.099$, $p = 0.171$), and Social Media Platform Measures (SMPM) ($\beta = -0.126$, $p = 0.041$) are either statistically insignificant or show a negative relationship. Specifically, SMPM has a notable negative effect ($\beta = -0.126$, $p = 0.041$), implying that existing actions taken by social media platforms may be ineffective or even harmful in reducing misinformation within Nepal's context. The negative coefficient may not necessarily indicate that platform measures are objectively ineffective. Instead, it may reflect respondents' perceptions regarding the adequacy, transparency, consistency, or trustworthiness of current platform moderation practices. Users may perceive content moderation efforts as insufficient, delayed, inconsistent, or difficult to observe directly. Therefore, the finding may represent public dissatisfaction or limited confidence in existing platform interventions rather than the actual effectiveness of social media companies' misinformation control mechanisms. Meanwhile, CI and GPR lack statistical significance since their p-values exceed the 0.05 cutoff, suggesting that these structural and policy-oriented factors do not contribute meaningfully to combating deepfakes and misinformation at present.

Furthermore, the collinearity diagnostics indicate that all tolerance values are greater than 0.1 (ranging from 0.287 to 0.689) and all VIF values are below 5 (ranging from 1.452 to 3.486), confirming that multicollinearity does not pose a serious problem among the independent variables. In conclusion, the findings emphasize that human-focused elements particularly public awareness campaigns and digital literacy play a vital role in tackling misinformation, whereas institutional factors such as cybersecurity infrastructure, government regulations, and social media measures currently have limited or adverse effects in the Nepalese setting.

Discussion

The findings of this study demonstrate that Public Awareness Campaigns (PAC) have a significant positive influence on combating deepfakes and misinformation in Nepal. This finding suggests that awareness-based interventions improve individuals' ability to recognize manipulated content and critically evaluate online information. The result is consistent with previous studies that reported media literacy initiatives and public awareness programs enhance users' resistance to misinformation and improve information verification behavior (Guess et al., 2021; Jones-Jang et al., 2021). The finding indicates that increasing public knowledge about deepfakes and misinformation can strengthen societal resilience against digital deception.

Similarly, Digital Literacy (DL) was found to have a significant positive effect on combating deepfakes and misinformation. Individuals possessing stronger digital competencies and critical thinking skills are more capable of distinguishing authentic information from manipulated content. This finding supports previous research which concluded that digitally literate users are less susceptible to misinformation and more likely to verify information before sharing it online (Pennycook & Rand, 2021; Groh et al., 2022). In the Nepalese context, where internet usage continues to expand rapidly, strengthening digital literacy can play a crucial role in reducing vulnerability to AI-generated misinformation.

The study further revealed that Cybersecurity Infrastructure (CI) does not significantly influence the effectiveness of combating deepfakes and misinformation. Although previous studies have highlighted the importance of AI-based detection systems, digital forensic tools, and cybersecurity technologies for identifying manipulated media (Farid, 2022; Pu et al., 2023), the present findings suggest that users may not directly perceive these technological measures as effective at the individual level. A possible explanation is that advanced cybersecurity systems often operate in the background and remain inaccessible or unfamiliar to ordinary users. Therefore, technological capability alone may not be sufficient unless accompanied by public awareness and user engagement.

Government Policies and Regulations (GPR) also showed a statistically insignificant relationship with combating deepfakes and misinformation. This finding aligns with studies suggesting that regulatory frameworks frequently struggle to keep pace with rapidly evolving AI technologies and digital misinformation threats (de Gregorio, 2022). While legal

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

frameworks are necessary for establishing accountability and governance, their effectiveness depends on implementation, enforcement, and public awareness. The findings imply that policies alone may not directly improve citizens' ability to identify and resist misinformation without complementary educational and technological interventions.

An interesting finding of this study is the significant negative relationship between Social Media Platform Measures (SMPM) and combating deepfakes and misinformation. This suggests that respondents may perceive existing platform moderation systems as inadequate or ineffective in controlling the spread of manipulated content. Previous studies similarly reported that engagement-driven algorithms can unintentionally amplify misinformation despite moderation efforts (Cinelli et al., 2021; Ferrara et al.,2022). Furthermore, concerns regarding transparency, consistency, and trust in platform governance may reduce public confidence in platform-level interventions. Consequently, social media companies may need to improve content moderation mechanisms and increase transparency regarding misinformation management practices. A further limitation of this study is that the quantitative design does not allow for an in-depth exploration of respondent's perceptions regarding social media platform measures. Consequently, the significant negative relationship observed between SMPM and combating deepfakes and misinformation cannot be fully explained. Qualitative or mixed-methods research is recommended to investigate the reasons behind this finding and to better understand public attitudes toward platform governance and content moderation practices.

The findings also indicate strong interrelationships among Cybersecurity Infrastructure, Government Policies and Regulations, and Social Media Platform Measures. This suggests that respondents perceive these institutional mechanisms as interconnected components of a broader digital governance framework. However, their limited direct contribution to combating misinformation indicates potential gaps in implementation and public trust. Previous literature similarly emphasizes that effective responses to deepfakes require integrated strategies combining technological solutions, regulatory measures, platform accountability, and public education (Kietzmann et al., 2021; Tolosana et al., 2021). Therefore, combating misinformation requires a collaborative and multi-stakeholder approach rather than reliance on a single intervention.

The findings should also be interpreted within Nepal's unique digital and media environment. Nepal has experienced rapid growth in internet and social media usage over the past decade, while digital literacy levels, access to reliable information sources, and fact-checking capacities remain uneven across different regions and demographic groups. In addition, linguistic diversity and varying levels of media access between urban and rural communities create additional challenges for identifying and combating misinformation. These contextual factors may explain why public awareness campaigns and digital literacy emerged as the strongest predictors of combating deepfakes and misinformation in the present study. Unlike many developed countries where advanced technological solutions and institutional mechanisms play a more prominent role, Nepal's media landscape may place greater importance on human-centered interventions that enhance citizens' ability to critically evaluate online information.

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Therefore, strengthening public awareness, digital education, and community-based information verification initiatives may be particularly effective within the Nepalese context.

Overall, this study contributes to the growing body of knowledge on deepfakes and misinformation by providing empirical evidence from Nepal. Unlike many international studies that primarily focus on technological detection systems and regulatory responses, the present study demonstrates that human-centered factors, particularly public awareness and digital literacy, exert a stronger influence on combating deepfakes and misinformation. This finding contributes new evidence from a developing digital environment and highlights the importance of investing in educational initiatives, awareness programs, and digital literacy development to strengthen resilience against AI-driven misinformation in Nepal.

Conclusion and Recommendation

This study examined the determinants influencing the effectiveness of combating deepfakes and misinformation in Nepal by analyzing the roles of Cybersecurity Infrastructure (CI), Digital Literacy (DL), Government Policies and Regulations (GPR), Social Media Platform Measures (SMPM), and Public Awareness Campaigns (PAC). The findings reveal that human-centered factors, particularly public awareness campaigns and digital literacy, are the most significant positive contributors to combating deepfakes and misinformation. Respondents with stronger awareness and digital evaluation skills demonstrated greater ability to identify manipulated content and resist misinformation. In contrast, institutional and technological measures such as cybersecurity infrastructure, government regulations, and platform moderation mechanisms showed weak or statistically insignificant influence on perceived effectiveness.

The study contributes new empirical knowledge by demonstrating that technological systems and regulatory interventions alone are insufficient unless supported by strong public awareness and digital literacy capabilities. This research further highlights a gap between institutional cybersecurity measures and public trust or practical effectiveness within Nepal's digital environment. The findings therefore extend existing literature by emphasizing that combating AI-driven misinformation in developing digital ecosystems requires not only technological advancement but also behavioral, educational, and societal preparedness.

Based on these findings, the study recommends that policymakers, educational institutions, cybersecurity agencies, and social media platforms prioritize large-scale digital literacy and public awareness initiatives. Media literacy education should be integrated into academic curricula, while awareness campaigns should focus on content verification, critical thinking, and responsible online behavior. Additionally, the government should strengthen AI-related cybersecurity policies, encourage public-private collaboration for deepfake detection technologies, and improve transparency in platform-based moderation systems. These combined efforts would significantly enhance Nepal's resilience against the growing threat of AI-generated misinformation and deepfake technologies.

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

References

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6*, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

Adhikari, B. P., Acharya, A., Chhatkuli, A., Ghimire, A., & Poudel, L. (2025). *Assessing cybersecurity literacy proficiency among bachelor's degree students in Nepal*. *OCEM Journal of Management, Technology and Social Sciences, 5*(1). https://doi.org/10.3126/ocemjmtss.v5i1.89684

Bhandari, B. (2024). *Weaponizing information: The rise of social media manipulation in Nepal*. *Journal of Durgalaxmi, 3*(1). https://doi.org/10.3126/jdl.v3i1.73833

Birrer, A., & Just, N. (2024). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New Media & Society*. https://doi.org/10.1177/14614448241253138

Chapagain, S., & Pulami, M. J. (2025). *Fanaticism-as-performance: social media styled experts and politics of nostalgia in Nepal*. *Journal of Political Science, 26*(1). https://doi.org/10.3126/jps.v26i1.90792

Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences, 118*(9), e2023301118. https://doi.org/10.1073/pnas.2023301118

Cinelli, M., Quattrociocchi, W., Galeazzi, A., et al. (2021). The COVID-19 social media infodemic. *Scientific Reports, 10*, 16598. https://doi.org/10.1038/s41598-020-73510-5

Clayton, K., Blair, S., Busam, J. A., Forstner, S., Glance, J., Green, G., Kawata, A., Kovvuri, A., Martin, J., Morgan, E., Sandhu, M., Sang, R., Scholz-Bright, R., Welch, A., Wolff, A. G., Zhou, A., & Nyhan, B. (2020). Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories. *Political Behavior, 42*(4), 1073–1095. https://doi.org/10.1007/s11109-019-09533-0

Conti, M., Gangwal, A., & Ruj, S. (2018). On the economic significance of ransomware campaigns. *Computers & Security, 79*, 162–189. https://doi.org/10.1016/j.cose.2018.07.011

Cresci, S. (2021). A decade of social bot detection. *Communications of the ACM, 63*(10), 72–83. https://doi.org/10.1145/3409116

de Gregorio, G. (2022). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law, 19*(1), 41–70. https://doi.org/10.1093/icon/moab001

European Commission. (2022). Proposal for a regulation laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

Farid, H. (2020). Creating and detecting deepfakes. *arXiv*. https://doi.org/10.48550/arXiv.2202.07145

Ferrara, E., Chang, H., Chen, E., Muric, G., & Patel, J. (2022). Characterizing social media manipulation in the 2020 U.S. presidential election. *First Monday, 27*(1). https://doi.org/10.5210/fm.v25i11.11431

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society, 7*(1). https://doi.org/10.1177/2053951719897945

Groh, M., Epstein, Z., Firestone, C., & Picard, R. (2022). Deepfake detection by human crowds, machines, and machine-informed crowds. *Proceedings of the National Academy of Sciences, 119*(1), e2110013119. https://doi.org/10.1073/pnas.2110013119

Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2021). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences, 117*(27), 15536–15545. https://doi.org/10.1073/pnas.1920498117

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does media literacy help identification of fake news? Information literacy helps, but other literacies don't. *American Behavioral Scientist, 65*(2), 371–388. https://doi.org/10.1177/0002764219869406

Kietzmann, J., Lee, L., McCarthy, I. P., & Kietzmann, T. (2021). Deepfakes: Trick or treat? *Business Horizons, 64*(3), 317–329. https://doi.org/10.1016/j.bushor.2020.11.006

Köbis, N., Bonnefon, J. F., & Rahwan, I. (2021). Bad machines corrupt good morals. *Nature Human Behaviour, 5*(6), 679–685. https://doi.org/10.1038/s41562-021-01128-2

Lazer, D. M. J., Baum, M. A., Benkler, Y., et al. (2018). The science of fake news. *Science, 359*(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

Matli, W. (2026). Extending the Unified Theory of Acceptance and Use of Technology (UTAUT) to address deepfake health misinformation. *Universal Access in the Information Society, 25*, 80. https://doi.org/10.1007/s10209-026-01338-3

Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes. *ACM Computing Surveys, 54*(1), 1–41. https://doi.org/10.1145/3425780

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences, 25*(5), 388–402. https://doi.org/10.1016/j.tics.2021.02.007

Pokharel, S. (2023). *Development in digital capitalism: Challenges and prospects of Nepal*. *KMC Research Journal, 7*(1). https://doi.org/10.3126/kmcrj.v7i1.65080 processes.

Pu, J., Shen, X., & Zhao, G. (2023). Deepfake detection: A comprehensive survey. *Artificial Intelligence Review, 56*(7), 7015–7066. https://doi.org/10.1007/s10462-022-10357-y

Timalsina, D. P. (2025). *From screens to streets: Role of digital literacy and misinformation in shaping democratic participation in Nepal*. *Interdisciplinary Journal of Innovation in Nepalese Academia, 4*(1), 181–201. https://doi.org/10.32674/bvmx5818

Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2021). Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion, 64*, 131–148. https://doi.org/10.1016/j.inffus.2020.06.014

UNESCO. (2021). Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Vaccari, C., & Chadwick, A. (2021). Deepfakes and disinformation. *Social media + Society, 7*(1). https://doi.org/10.1177/2056305120903408

Verdoliva, L. (2020). Media forensics and deepfakes: An overview. *IEEE Journal of Selected Topics in Signal Processing, 14*(5), 910–932. https://doi.org/10.1109/JSTSP.2020.3002101

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Vilone, G., & Longo, L. (2021). Explainable artificial intelligence: A systematic review. *arXiv Preprint*. https://doi.org/10.48550/arXiv.2006.00093

Westerlund, M. (2021). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 11*(9), 39–52. https://doi.org/10.22215/timreview/1282

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

Appendix

Respected Participant,

Representing Herald College Kathmandu (University of Wolverhampton), I, Anu Kumari, am conducting research on the topic *"AI and Cybersecurity: Combating Deepfakes and Misinformation in Nepal."*

The purpose of this survey is to explore how artificial intelligence (AI) tools and cybersecurity measures can help detect, prevent, and reduce the spread of deepfakes and digital misinformation in the Nepalese context. Your valuable insights will contribute to a better understanding of the challenges and possible solutions in addressing this issue.

Please note that all responses will remain strictly confidential and will be used solely for academic purposes. Your honest and thoughtful input will be highly appreciated and will play a significant role in the success of this research.

Thank you very much for your time and valuable contribution.

SURVEY QUESTIONNAIRE

PARTICIPANT'S INFORMATION:

DEMOGRAPHIC INFORMATION

NAME:

GENDER:

1. Male
2. Female

AGE

1. Below 20
2. 20-30
3. 30-40
4. 40-50
5. 50 & above

MARITAL STATUS

1. Married
2. Unmarried

QUALIFICATION

1. SLC / SEE or Below
2. Intermediate / +2
3. Bachelor's Degree
4. Master's Degree
5. MPhil / PhD or Higher

OCCUPATION:

1. Student
2. Employed
3. Unemployed
4. Entrepreneur / Business Owner

MONTHLY INCOME (NPR)

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

1. Under 20,000
2. 20,000-30,000
3. 30,000-40,000
4. 40,000-50,000
5. 50000 & above

FREQUENCY OF INTERNET / SOCIAL MEDIA USE:

1. Less than 1 hour/day
2. 1–3 hours/day
3. 4–6 hours/day
4. More than 6 hours/day

FAMILIARITY WITH AI OR CYBERSECURITY CONCEPTS:

1. Not familiar
2. Somewhat familiar
3. Familiar
4. Very familiar

EXPERIENCE WITH MISINFORMATION / DEEPFAKES ONLINE:

1. Never encountered
2. Rarely
3. Occasionally
4. Frequently

2. LIKERT-TYPE QUESTIONS

To what extent do you consider the following AI and cybersecurity strategies effective in combating deepfakes and digital misinformation in Nepal?

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

A. Dependent Variables Likert Type Questions Table

Dependent Variables	Questions	1	2	3	4	5
Combating Deepfakes and Misinformation	1. Deepfakes and misinformation are a serious threat in Nepal.					
	2. AI and cybersecurity measures can reduce the spread of fake content.					
	3. Effective detection systems make me feel safer online.					
	4.The threat of misinformation has decreased due to existing digital security measures.					
	5. Reducing deepfakes contributes positively to public trust in online information.					

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

B. Independent Variables Likert Type Questions Table:

Independent Variables	Questions	1	2	3	4	5
Cybersecurity Infrastructure	1. Nepal has strong cybersecurity systems to monitor online content.					
	2. Cybersecurity measures reduce the risk of online misinformation.					
	3. Government agencies actively enforce cybersecurity policies.					
	4. I feel confident that my online activities are protected from fake content.					
	5. Cybersecurity infrastructure is adequately funded and maintained in Nepal.					
Digital Literacy	1. I can identify fake videos and news online.					
	2. Most people in Nepal are aware of deepfakes and misinformation.					
	3. Training programs improve the ability to detect fake content.					
	4. Schools and universities provide sufficient digital literacy education.					
	5. Public understanding of online misinformation helps reduce its spread.					
Government Policies and Regulations	1. Nepal has effective laws to prevent the spread of fake news and deepfakes.					
	2. Government policies are enforced properly to combat misinformation.					
	3. Legal consequences discourage individuals from creating or sharing fake content.					
	4. Policies keep up with the latest AI and cybersecurity developments.					
	5. Citizens are aware of government regulations regarding online misinformation.					
Social Media Platform Measures	1. Social media platforms actively remove fake content from Nepal.					
	2. Reporting tools on platforms help reduce misinformation.					
	3. AI moderation on social media is effective in detecting deepfakes.					

Nepal Journal of Multidisciplinary Research (NJMR)
Vol. 9, No. 2, June 2026. Pages: 325-347
ISSN: 2645-8470 (Print), ISSN: 2705-4691 (Online)
DOI: 10.3126/njmr.v9i2.95265

	4. Social media companies are responsible for content posted on their platforms.					
	5. Platforms provide enough guidance to users about recognizing fake content.					
Public Awareness Campaigns	1. Awareness campaigns improve understanding of deepfakes and misinformation.					
	2. Public campaigns encourage safe online practices.					
	3. Mass media programs educate citizens about detecting fake news.					
	4. Government and NGOs actively run anti-misinformation awareness programs.					
	5. Awareness campaigns have effectively reduced the spread of misinformation in Nepal.					

Thank you!