International Journal of Data and Network Science 7 (2023) 1471–1484

Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Evaluating the influence of security considerations on information dissemination via social networks

Issam AlHadid[a*], Evon M. Abu-Taieh[a], Mohammad Al Rawajbeh[b], Rami S. Alkhawaldeh[a], Sufian Khwaldeh[a,c], Suha Afaneh[d], Ala'Aldin Alrowwad[e] and Dima Farhan Alrwashdeh[a]

[a]*Faculty of Information Technology and Systems, University of Jordan, Aqaba 77110, Jordan*
[b]*Faculty of Science and Information Technology, Al Zaytoonah University of Jordan, Amman, 11733, Jordan*
[c]*College of Information Technology, University of Fujairah, Fujairah 2202, United Arab Emirates*
[d]*Faculty of Information Technology, Zarka University, Zarka 13110, Jordan*
[e]*School of Business, University of Jordan, Aqaba 77110, Jordan*

C H R O N I C L E

Article history:
Received: July 2, 2023
Received in revised format: July 26, 2023
Accepted: August 16, 2023
Available online: August 16, 2023

Keywords:
Trust
Privacy
Security
Awareness
Information Sharing
Social Networks

A B S T R A C T

This study investigates the factors that influence the sharing of information on social media platforms and examines the effects of perceived security, perceived privacy, and user awareness on users' trust in social media platforms, as well as the moderating effects of age, gender, educational attainment, and internet proficiency on information sharing. The study collected data from 837 social media users in Jordan and analyzed them using structural equation modeling (SEM), confirmatory factor analysis (CFA), and machine learning (ML) methods. The findings of the study indicate that perceived security, perceived privacy, and user awareness all have a significant impact on users' trust in social media platforms. Trust, in turn, has a significant impact on the amount of information shared on these platforms. Also, the findings of this study provide valuable insights into the dynamics of information sharing on social networks. This knowledge will be of interest to managers, policymakers, and developers of social media platforms. In addition, the findings of the study also have implications for the privacy and security of social media users. For example, social media users can be more careful about the information they share on social media platforms, and they can take steps to protect their privacy.

1. Introduction

Social media networks, as articulated by Koohang et al. (2021), are web-based platforms that both individuals and businesses utilize to generate, exchange, and circulate information in various formats for communication, acquiring, and spreading news. They encompass platforms like Facebook, Instagram, Twitter, Snapchat, Pinterest, LinkedIn, Tumblr, Reddit, Vine, Flickr, Snapchat, and TikTok, among others. Users share a wide spectrum of information on these platforms, from personal details to opinions on political, economic, social, cultural, and environmental matters, in several languages such as English, French, Russian, Chinese, and Arabic. While the inaugural purpose of social media platforms was to facilitate interaction among campus students, they have since evolved, and their political influence is increasingly palpable. With this evolution comes an abundance of information that can serve myriad purposes. Users often disclose substantial information that could be used for various prospects, which led to the instigation of this research to study the motives driving information sharing on these platforms (Koohang et al., 2021). This study brings several benefits, such as enlightening policymakers of social networks on the need for clear privacy options for users. Moreover, it will prove valuable to developers of social networks, researchers, and users. The uniqueness of this research lies in its comprehensive examination of all four factors (security, privacy, user awareness, and trust) and their moderating variables within the Arabic culture. This will be beneficial to users, researchers,

* Corresponding author.
E-mail address: i.alhadid@ju.edu.jo (I. AlHadid)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2023.8.015

policymakers, as well as legislators (Koohang et al., 2021; Gupta & Dhami, 2015; Maqableh et al., 2021). Security and privacy concerns have been serious issues in the realm of social media networks. Incidents like the Facebook data breach in 2018 (Ingram et al., 2018) highlight the risks associated with the extensive sharing of personal data on these platforms (Jeong & Kim, 2017). Therefore, these issues were given substantial consideration in this research.

The aim of this research is to examine the various factors that influence information sharing on social media networks, particularly security, privacy, user awareness, and trust. Despite previous research efforts, none have investigated all these four factors in one study (Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018; Paramarta et al., 2018; Gibson & Trnka, 2020; Shin, 2010; Lin & Liu, 2012; Majerczak & Strzelecki, 2022; Kim et al., 2023; Lin et al., 2019; Hou & Kankham, 2022). Consequently, the significance of this research is manifold; it covers all factors influencing information sharing on social media networks within the context of Arabic culture and uses moderators like age, gender, education level, and internet experience. The research poses two main questions:

Q1: What are the factors that influence users' trust in sharing personal information on social media networks?
Q2: What is the influence of security, privacy, awareness, and trust on sharing information on social media networks?

The significance of this research is shown in many aspects: first, this research covered all factors of privacy, security, trust user awareness influencing information sharing in social media networks which no other study did cover. Further, this study was conducted within Arabic culture and used moderators like age, gender, educational level, and internet experience.

2. Literature review

Different studies researched information sharing on social networks shown in Table 1. Information sharing included personal information that included name, location (Ruan et al., 2021), job, preferences, personal pictures, videos, ideas, and opinions. The studies research different factors that influence information sharing security (Koohang et al., 2021; Gupta & Dhami, 2015; Maqableh et al., 2021; Shin, 2010); trust (Koohang et al., 2021; Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018 ; Paramarta et al., 2018; Gibson & Trnka, 2020; Shin, 2010; Lin & Liu, 2012; Majerczak & Strzelecki, 2022; Hou & Kankham, 2022); user awareness (Hou & Kankham, 2022; Paramarta et al., 2018); and privacy concern (Koohang et al., 2021; Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018; Paramarta et al., 2018; Shin, 2010; Lin & Liu, 2012; Rawajbeh et al., 2023). One study took the psychological point of view like Self-connection, Self-efficacy, social connection, and Empathy. Other studies included Media Credibility, Social Ties (Majerczak & Strzelecki, 2022).

Table 1
Studies pertain to security, trust, privacy, user awareness, and information sharing in social media networks

Research	Focus on
Gupta & Dhami, (2015)	security, trust, and privacy in information sharing
Maqableh et al., (2021)	perceived privacy, perceived security, and trust in Facebook addiction
Kumar et al., (2018)	Trust and privacy in behavioral intention
Paramarta et al., (2018)	User Awareness, Trust, and Privacy in information sharing in Facebook, Twitter, and Instagram
Koohang et al., (2021)	privacy concerns, security concerns, trust, and awareness
Gibson & Trnka, (2020)	Trust
Shin, (2010)	trust, security, and Privacy on Adoption
Lin & Liu, (2012)	Trust and privacy concerns comparing Facebook with Myspace
Majerczak & Strzelecki, (2022)	Trust, Media Credibility, Social Ties, and the Intention to Share
Kim et al., (2023) and Lin et al., (2019)	Self-connection, Self-efficacy, social connection, Empathy on information sharing
Hou & Kankham, (2022)	Trust and status share Facebook icons

The proposed model introduces constructs such as Perceived security (PS), Perceived privacy (PPV), Users' awareness (AW), Perceived trust (TR), and Information Sharing (ISH). In addition, several moderators like age, gender, education level, and internet experience, as well as the social media networks utilized, are integrated into the model. Perceived privacy (PPV), referring to an individual's ability to govern how their personal information is collected and utilized, is explained in (Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018). Perceived security (PS) pertains to concerns regarding the protection of personal data with specific objectives, such as maintaining integrity, authentication, and confidentiality (Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018). Perceived trust (TR), a crucial requirement for self-disclosure, lowers perceived risks associated with disclosing private information (Gupta & Dhami, 2015; Maqableh et al., 2021; Kumar et al., 2018; Gibson & Trnka, 2020). It is defined in (Koohang et al., 2021) based on integrity, benevolence, and competence, and in (Kumar et al., 2018) as the willingness of an individual to be vulnerable to another's actions based on the expectation of positive action. Users' awareness (AW) is the knowledge of how to use social media sites and the understanding of the importance of protecting personal data (Koohang et al., 2021; Paramarta et al., 2018). Information sharing (ISH) is the act of disclosing personal data on a social network site (Gupta & Dhami, 2015). The information shared includes name, location (Ruan et al., 2021), employment, and education, as well as personal photos, videos, ideas, and opinions (Lin & Wang, 2020). The moderators incorporated in this study are derived from (Abu-Taieh et al., 2022a; Chawla & Joshi, 2020; Kwateng et al., 2018; Samsudeen et al., 2022), and they demonstrate the influence of age, gender, education level, and internet experience on information sharing in social media networks.

3. Theoretical Framework and Hypotheses Development

In the upcoming section, the content breaks down into subsections for easy navigation, this delivers a concise description of experimental results, their interpretation, and the experimental conclusions to be drawn. Through the analysis of several theoretical models, scholars have endeavored to comprehend the issues of security and privacy in the context of social networks. These models are drawn from social network theory, the Technology Acceptance Model (TAM), and earlier frameworks (Shin, 2010; Lin & Liu, 2012; Gross & Acquisti, 2005). Consequently, we have designed the model depicted in Fig. 1.

This model encompasses four categories: five independent constructs, mediating constructs, and dependent constructs. These have been adapted from (Shin, 2010; Lin & Liu, 2012; Gross & Acquisti, 2005) and cover Perceived Security (PS), Perceived Privacy (PPV), User Awareness (AW), Perceived Trust (TR), and Information Sharing (ISH). Moderating variables in this model include gender, age, education level, and Internet experience. The model stipulates those three independent variables (PS, PPV, and AW) are critical in examining the factors that impact users' perceived trust (TR) and information sharing in social networks. Additionally, the model's independent factors (PS, PPV, and AW), along with the mediating variable (TR), are employed to assess the impact of users' information sharing in social media networks.

Stallings (2017) articulated that security pertains to the safeguarding of information and systems from unauthorized access, damage, or disruption. Trust and security significantly impact user behavior and information disclosure, as stipulated by social exchange theory (Gupta & Dhami, 2015; Shin, 2010; Ajzen, 1991). Several studies have delved into the correlation between security and trust and their roles in information sharing. Singh and Gill (2015) explored users' security awareness levels and found that 50% of participants had secured their accounts by modifying privacy and security settings and refraining from responding to unfamiliar friend requests or fraudulent accounts. Several factors such as education influence the level of users' security awareness (Miyazaki & Fernandez, 2001). Furthermore, significant correlations between perceived security and perceived trust and between information sharing and perceived security have been identified (Gupta & Dhami, 2015; Kumar et al., 2018; Shin, 2010; Miyazaki & Fernandez, 2001; Dhami et al., 2013). Therefore, the following hypotheses were proposed:

H_1: *Perceived security positively influences information sharing on social media networks.*
H_2: *Perceived security positively influences perceived trust in social media networks.*

Chai et al. (2009) define information privacy as individuals, groups, or institutions' right to decide when, how, and to what extent their information is communicated to others. Alshare et al. (2019) indicated that privacy concerns could decrease the likelihood of individuals using social networks or sharing information. Several studies have found a significant association between perceived privacy and perceived trust and a positive correlation between perceived privacy and information sharing (Gupta & Dhami, 2015; Kumar et al., 2018; Shin, 2010; Miyazaki & Fernandez, 2001; Miyazaki & Fernandez, 2001; Dhami et al., 2013; Alshare et al., 2019a). The subsequent hypotheses were suggested:

H_3: *Perceived privacy positively influences perceived trust in social media networks.*
H_4: *Perceived privacy positively influences information sharing on social media networks.*

According to Paramarta et al. (2018), user awareness is defined as "an individual's knowledge or ability in using social media sites and understanding the importance of protecting personal data when using a social networking site". Increasing awareness amongst social network users will improve satisfaction and continuance intention, as stated by Maqableh et al. (2021). Hence, the following hypotheses were proposed:

H_5: *Users' awareness positively influences perceived trust in social media networks.*
H_6: *Users' awareness positively influences information sharing on social media networks.*
H_7: *Perceived trust positively influences information sharing on social media networks.*

Several studies have used moderators like age, gender, educational level, and internet experience to explain their work (Abu-Taieh et al., 2022a; Chawla & Joshi, 2020; Kwateng et al.,2018; Samsudeen et al., 2022). Accordingly, the following hypotheses were developed:

H_8: *Age positively influences information sharing on social media networks.*
H_9: *Internet experience positively influences information sharing on social media networks.*
H_{10}: *Gender positively influences information sharing on social media networks.*
H_{11}: *Education level positively influences information sharing on social media networks.*
H_{12}: *Social network usage positively influences information sharing on social media networks.*

The use of moderators such as age, gender, educational level, and internet experience is not a novel concept and has been employed in numerous studies (Abu-Taieh et al., 2022a; Chawla & Joshi, 2020; Kwateng et al., 2018; Samsudeen et al., 2022). For instance, Chawla and Joshi (2020) integrated age and gender as constructs in their model rather than using them as moderators. Abu-Taieh et al. (2022a, 2022b) also utilized similar moderators to explore the effects of social networks on anxiety and depression. Similarly, other studies, such as the works of Owusu Kwateng et al. (2018) and Samsudeen et al. (2022), employed these moderators to investigate the acceptance of mobile banking applications.

4. Survey Design & Methods

In the subsequent sections, an intricate design of the research study and the methodologies adopted therein are discussed. As illustrated in Fig. 1, the theoretical framework incorporates three independent constructs, an intermediate construct, and a single dependent construct. These independent constructs encompass PS, PPV, and AW, while the intermediate construct consists of perceived trust (TR). Information sharing (ISH) is delineated as the dependent construct. Age, gender, educational attainment, social network (SN), and Internet experience serve as the moderating variables in this model. The scarcity of previous research in this domain inspired the creation of this model, visually represented in Figure 1, leading to the subsequent development of the hypotheses. The study involved crafting a comprehensive questionnaire, subsequently scrutinized and validated. Data was amassed from a convenience sample. The forthcoming segments - research context, measurement items, participant demographic and procedure, and measurement instruments - elaborate on the nuances of the research design and methodologies. Each segment is crafted with meticulous attention to detail, providing an exhaustive understanding of the empirical study. This is expressed in an engaging academic tone to balance scholarly rigor and reader-friendly communication.

4.1 Research Context

A plethora of studies have been undertaken to scrutinize the nexus between security, privacy, user awareness, trust, and information sharing within the realm of social networks. This extensive body of research, encompassing more than 40 distinct investigations as displayed in Table 1, has explored these intricate relationships. However, no such inquiry has been carried out within the context of the Arab-speaking world. The question thus emerges: Do security, privacy, awareness, and trust indeed exert influence on information sharing in social networks? This compelling inquiry forms the foundation for the current study, setting the stage for the subsequent research procedure.

4.2 Measurement Items

In this study, a questionnaire was made to look at the suggested research model. The survey questions were made based on research that had already been done in the area. The model has nine factors, including ones that are independent, dependent, mediating, and moderating. Certain factors were used to judge each variable. There were five groups for each age, two groups for each gender, five groups for each level of education, and three groups for Internet knowledge. Five items from references (Alshare et al., 2019b; Hartono et al., 2014; Flavián & Guinalíu, 2006) were used to evaluate the PS (perceived security) construct. In the same way, five items from reference (Flavián & Guinalíu, 2006) were used to measure the PPV (perceived privacy breach) construct. Three questions from reference (Koohang et al., 2021) were used to measure AW (awareness). Five items from reference (Majerczak & Strzelecki, 2022) were used to measure trust (TR), and six items from reference (Lin & Wang, 2020) were used to measure information-sharing behavior (ISH). Alshare et al. (2019b), Hartono et al. (2014), and Flavián and Guinalíu (2006) helped choose the items used to measure PS. Flavián and Guinalu's (2006) work gave us the things we used to measure PPV. Research by Koohang, Floyd-Equivalent, Yerby, and Paliszkiewicz (2021) was used to make the things used to measure AW. Majerczak and Strzelecki (2022) did a study that was used to figure out how to measure TR. Lin and Wang (2020) did a study that was used to figure out how to measure ISH.

4.3 Participants and Procedure

Using Google Docs, an online poll questionnaire was made in both Arabic and English, with a five-point Likert scale that went from “strongly disagree” to “strongly agree”. A group of 12 academicians underwent a thorough review process with the form. Valuable feedback was gathered, and the form was improved by making the changes that were needed. After that, 35 Jordanian social network users took part in a pilot test to see if the questions were easy to understand. Based on the results of the pilot test, the poll instrument was changed again to make it better.

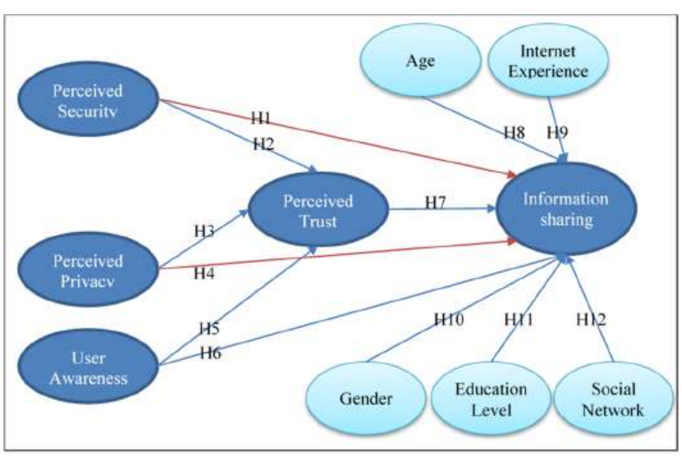

Fig. 1. Proposed research model

To make sure the survey link reached as many people as possible, it was sent out via email, school groups, researchers, and social media sites like Facebook, LinkedIn, Instagram, and WhatsApp groups that were made just for Jordanians. The study used a method called “convenience sampling”, in which people volunteered to take the poll without getting anything in return. The data from Morgan's table helped me figure out the right sample size. It showed that 384 respondents were needed to get the best statistical sample size for this study (Hair et al., 2010). The poll was done from December 15, 2022, to March 22, 2023. After taking out answers that were too short or did not make sense, the study could still include 837 users of social networking applications (SN applications). Table 2 shows that the same number of Males and females were among the people who answered the survey. Also, most of the people who took part were between 28 and 38 years old, had a diploma or bachelor's degree, had good to excellent internet experience, and mostly used Snapchat and Facebook as their favorite social media sites.

4.4 Measurement instruments

For measuring constructs, items have been adopted from previously validated instruments, subject to minimal alterations in wording for a better fit. The application of a five-point Likert scale, wherein "strongly disagree" corresponds to 1 and "strongly agree" corresponds to 5, has been judiciously incorporated. The careful adaptation and application of these methods underpin the originality and depth of this study.

Table 2
Respondents’ demography

		Female		Male		Total	
Age category	From 18 to less than 28	114	48%	126	53%	240	29%
	From 28 to less than 38	152	57%	115	43%	267	32%
	From 38 to less than 48	92	67%	45	33%	137	16%
	From 48 to less than 58	108	72%	41	28%	149	18%
	more than 58	25	57%	19	43%	44	5%
Education level	HS and less than HS	112	47%	125	53%	237	28%
	Diploma	117	54%	101	46%	218	26%
	BSC	123	63%	72	37%	195	23%
	Master	118	72%	45	28%	163	19%
	PhD	21	88%	3	13%	24	3%
Internet experience	Low	272	95%	14	5%	286	34%
	Good	139	48%	150	52%	289	35%
	Excellent	80	31%	182	69%	262	31%
Social network	Instagram	53	47%	59	53%	112	13%
	TikTok	15	56%	12	44%	27	3%
	Facebook	99	43%	132	57%	231	28%
	Snapchat	200	97%	7	3%	207	25%
	LinkedIn	14	18%	64	82%	78	9%
	WhatsApp	44	48%	48	52%	92	11%
	twitter	63	85%	11	15%	74	9%
	Others	3	19%	13	81%	16	2%
Total		491	59%	346	41%	837	100%

5. Data Analysis and Results

5.1 Descriptive Analysis

To characterize the responses and thus the attitudes of respondents toward each survey question, calculations of both the mean and standard deviation were carried out. The mean serves as a representation of the central tendency of the data, while the standard deviation measures its dispersion and offers an index of the data’s range or variability (Pallant, 2020; Sekaran & Bougie, 2016). A small standard deviation signifies that values are densely clustered around the mean, whereas a large standard deviation suggests a wider spread. The level of each item is determined as per the following specifications, furthering the authenticity and detailed exploration of this stud. The level of each item was determined by the following:

$$Level = \frac{highest\ point\ in\ Likert\ scale\ -\ lowest\ point\ in\ Likert\ scale}{the\ number\ of\ the\ levels\ used} = \frac{5-1}{5} = 0.80, \tag{1}$$

Hence, producing the following lookup Table 3 of values.

Table 3
Level lookup table of values and ranges

Range	Level	Range	Level
1–1.80	very low	3.41–4.20	High
1.81–2.60	Low	4.21–5	very high
2.61–3.40	moderate		

Displayed in Table 4, the constructs feature the mean, standard deviation (SD), level, and order. Each construct earns a rank of “High” to “Very High”, according to Table 2 based on the work of (Pallant, 2020; Sekaran & Bougie, 2016). While the construct AW ranked as the first among all. Mediating constructs are ranked “high” as well as the dependent construct, ISH.

Table 4
Overall mean and standard deviation of the study’s variables.

Type of variable	Variable	Mean	Std. Deviation	Level	Order
Independent	PS	3.65	0.96	High	5
	PPV	3.78	1.01	High	4
	AW	4.42	0.76	Very High	1
Mediating	TR	3.90	1.15	High	3
Dependent	ISH	3.98	0.89	High	2

In Table 5, one finds the mean, standard deviation, level, and order of the constructs in correlation with the items and the addition of Cronbach Alpha for each construct. This Alpha operates as a gauge of reliability and consistency in multiple-question Likert scale surveys. A range above 0.7 is desirable, anything below this threshold raises concern. Table 4 reveals satisfactory reliability with all constructs boasting a Cronbach Alpha exceeding 0.70.

Table 5
Mean and standard deviation of the study’s variables ITEMS.

Items	Mean		Std. Deviation	level	order	Cronbach alpha	internal consistency
	Statistic	Std. Error	Statistic				
			Perceived Security (PS)				
PS1	3.68	0.037	1.058	High	3	0.933	Excellent
PS2	3.73	0.032	0.925	High	2		
PS3	3.50	0.040	1.148	High	4		
PS4	3.87	0.041	1.182	High	1		
PS5	3.48	0.038	1.103	High	5		
			Perceived Privacy (PPV)				
PPV1	3.99	0.041	1.180	High	1	0.896	Good
PPV2	3.73	0.035	1.008	High	3		
PPV3	3.69	0.044	1.264	High	4		
PPV4	3.67	0.038	1.109	High	5		
PPV5	3.80	0.048	1.391	High	2		
			Awareness (AW)				
AW1	4.36	0.027	0.787	Very High	3	0.912	Excellent
AW2	4.43	0.029	0.847	Very High	2		
AW3	4.45	0.029	0.838	Very High	1		
			Trust (TR)				
TR1	3.80	0.039	1.141	High	5	0.971	Excellent
TR2	3.94	0.043	1.242	High	1		
TR3	3.90	0.043	1.245	High	4		
TR4	3.93	0.041	1.196	High	2		
TR5	3.91	0.043	1.258	High	3		
			Information Sharing (ISH)				
ISH1	4.31	0.029	0.839	Very High	1	0.912	Excellent
ISH2	3.77	0.031	0.889	High	5		
ISH3	3.97	0.042	1.217	High	4		
ISH4	4.12	0.036	1.053	High	2		
ISH5	3.99	0.038	1.090	High	3		
ISH6	3.70	0.044	1.282	High	6		

5.2 Structural Model Assessment and Analysis

Table 6 reflects the coefficients where two hypotheses, specifically H1 and H4, lack support due to a p-Value > 0.05. In contrast, this table confirms support for H2, H3, H5, H6, and H7 from the study's findings.

Table 6
Summary of the results for the research theoretical model

Research Proposed Paths	Std Regression weights	Regression weights				
	Estimate	Estimate	S.E.	C.R.	P	Label
H1: PS→ ISH	.063	.058	.043	1.345	.179	Not Supported
H2: PS→ TR	.369	.440	.030	14.448	***	Supported
H3: PP→ TR	.549	.628	.031	20.132	***	Supported
H4: PPV→ ISH	-.026	-.023	.048	-.483	.629	Not Supported
H5: AW→ TR	.081	.123	.023	5.439	***	Supported
H6: AW→ ISH	.219	.254	.029	8.763	***	Supported
H7: TR→ ISH	.630	.485	.044	11.117	***	Supported

***significantly different from zero at the 0.001 level

R-squared serves as an indicator of the variance proportion elucidated by the regression model. This study strongly recommends an R-square greater than 0.7 with independent variables (PS, PPV, AW) and the dependent variable TR. Adjusted R-square offers a comparative analysis of the explanatory power of regression models with varying numbers of predictors. While analyzing regression linear analysis the following was found summarized in the following table.

Table 7
Summary of the results for the research theoretical model of R-squared

Predictors	dependent	R	R2	Adjusted R2	Std. The error in the Estimate	Sig.
AW, PS, PPV	ISH	.758a	0.575	0.573	0.57852	<001
AW, PS, PPV	TR	.929a	0.862	0.862	0.42830	<001
TR	ISH	.771a	0.595	0.594	0.56399	<001
AW, PS, PPV, TR	ISH	.793a	0.630	0.628	0.54030	<001
PS	ISH	.677a	0.458	0.457	0.65241	<001
PPV	ISH	.711a	0.505	0.505	0.62316	<001
AW	ISH	.547a	0.299	0.298	0.74200	<001

5.3 Moderating effects

The study investigated the significance of the gender of respondents, and its effects on ISH and found that there is a significant difference between males and females in information sharing (ISH). Female ISH is more than male ISH As per the group statistic tables 8,9 and 10. Hence the results suggested that females are more in favor of information sharing than males.

Table 8
Group statistics of responders' gender. With ISH

Gender	N	Mean	Std. Deviation	Std. Error of Mean	Grouped Median
Male	346	3.6624	.83869	.04509	3.7630
Female	491	4.1839	.85443	.03856	4.7116
Total	837	3.9683	.88555	.03061	4.1304

Table 9
Independent sample test, Levene's Test and t-test for responders' gender and ISH

	Levene's Test for Equality of Variances		t-test for Equality of Means							
					Significance				95% Confidence Interval of the Difference	
	F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Equal variances assumed	0.398	0.528	-8.762	835	0	0	-0.52148	0.05952	-0.63831	-0.40466
Equal variances not assumed			-8.79	751.258	0	0	-0.52148	0.05933	-0.63795	-0.40501

As for other moderators age, educational level, and internet experience. Table 10 reflects the Means, Std Deviation, Std. Error Mean and Grouped Mean. The table shows that the mean of low internet experience is the highest, while educational levels Master and Ph.D. have the highest means, and age groups are all above mean 4.0 except the first age group which is the younger generation.

Table 10
Moderators Means, Std Deviation, Std. Error Mean and Grouped Mean

		Mean	N	Std. Deviation	Std. Error of Mean	Grouped Median
Internet Experience	Low	4.5895	286	0.63287	0.03742	4.7214
	Good	3.6291	289	0.77633	0.04567	3.8523
	Excellent	3.6645	262	0.87551	0.05409	3.7474
	Total	3.9683	837	0.88555	0.03061	4.1304
Educational Level	High school and less.	3.7629	237	0.86576	0.05624	3.8945
	Diploma	3.7289	218	0.85386	0.05783	3.8915
	Bachelor	3.8431	195	0.92010	0.06589	3.9083
	Master	4.6620	163	0.41799	0.03274	4.7642
	Ph.D.	4.4792	24	0.87724	0.17907	4.5136
	Total	3.9683	837	0.88555	0.03061	4.1304
Age	18 to less than 28.	3.5758	240	0.78474	0.05065	3.6667
	28 to less than 38 years old.	4.1659	267	0.81716	0.05001	4.5680
	38 to less than 48 years old.	4.0555	137	0.95878	0.08191	4.5171
	48 to less than 58 years old.	4.1315	149	0.85851	0.07033	4.3000
	58 and over.	4.0864	44	1.00778	0.15193	4.4800
	Total	3.9683	837	0.88555	0.03061	4.1304

The outcomes of the ANOVA test, presented in Table 11, indicate the following: there is a significant difference in the respondents' ISH, supportive of the respondent's age, internet experience, education, and use of SN.

Table 11
ANOVA analysis of respondents' ISH attributed to respondents' age, internet experience, education, and gender, and used SN

		Sum of Squares	df	Mean Square	F	Sig.
ISH * SN	Between Groups (Combined)	275.186	7	39.312	85.671	0.000
	Within Groups	380.405	829	0.459		
	Total	655.591	836			
ISH * INTERNET EXPERIENCE	Between Groups (Combined)	167.807	2	83.903	143.456	0.000
	Within Groups	487.784	834	0.585		
	Total	655.591	836			
ISH * Age	Between Groups (Combined)	53.019	4	13.255	18.302	0.000
	Within Groups	602.572	832	0.724		
	Total	655.591	836			
ISH * Education	Between Groups (Combined)	110.248	4	27.562	42.050	0.000
	Within Groups	545.343	832	0.655		
	Total	655.591	836			
ISH * GENDER	Between Groups (Combined)	55.197	1	55.197	76.765	0.000
	Within Groups	600.394	835	0.719		
	Total	655.591	836			

Tables 12 and 13 reflect Multiple comparisons analysis of the respondents' age, educational level, internet experience as well as types of SN on the ISH. Hence, there is a significant difference between respondents with low internet experience and good and excellent internet experience regarding ISH in favor of low experience as shown in Table 12. While there is no significant difference between respondents with good and excellent internet experience regarding ISH. There is a significant difference between respondents in the age group 18-28 and the other age groups regarding ISH. While there is no significant difference between the other age groups regarding ISH. There is a significant difference between respondents with education levels of master's and Ph.D. groups and the other age groups regarding ISH. While there is no significant difference between the other education level groups regarding ISH. Based on what is reflected in Tables 10, 11, and 12 one may conclude that the dependent factor information sharing in social media networks was impacted significantly by age, gender educational level, and internet experience. As such there was a significant difference among age groups in favor of all except the first age group.

Table 12
Multiple comparisons analysis of the ISH attributed to respondents' age, education, and internet experience using Tukey HSD

	(I) IntExp		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	Upper Bound
Internet Experience	Low	Good	.96044*	0.06379	0.000	0.8107	1.1102
		Excellent	.92501*	0.06540	0.000	0.7715	1.0786
	Good	Excellent	-0.03544	0.06524	0.850	-0.1886	0.1177
Age	18-28	28-38	-.59008*	0.07570	0.000	-0.7970	-0.3831
		38-48	-.47964*	0.09113	0.000	-0.7288	-0.2305
		48-58	-.55571*	0.08876	0.000	-0.7984	-0.3131
		Greater than 58	-.51053*	0.13956	0.003	-0.8921	-0.1290
	28-38	38-48	0.11044	0.08944	0.731	-0.1341	0.3549
		48-58	0.03437	0.08702	0.995	-0.2035	0.2723
		Greater than 58	0.07955	0.13847	0.979	-0.2990	0.4581
	38-48	48-58	-0.07607	0.10073	0.943	-0.3515	0.1993
		Greater Than 58	-0.03089	0.14747	1.000	-0.4340	0.3723
	48-58	Greater Than 58	0.04518	0.14602	0.998	-0.3540	0.4444
Education	less than HS	Diploma	0.03397	0.07598	0.992	-0.1737	0.2417
		BSC	-0.08021	0.07828	0.844	-0.2942	0.1338
		Master	-.89909*	0.08238	0.000	-1.1243	-0.6739
		PhD	-.71630*	0.17343	0.000	-1.1904	-0.2422
	Diploma	BSC	-0.11418	0.07980	0.608	-0.3323	0.1040
		Master	-.93306*	0.08383	0.000	-1.1622	-0.7039
		PhD	-.75027*	0.17412	0.000	-1.2263	-0.2743
	BSC	Master	-.81889*	0.08592	0.000	-1.0538	-0.5840
		PhD	-.63609*	0.17513	0.003	-1.1149	-0.1573
	Master	PhD	0.18280	0.17701	0.840	-0.3011	0.6667

*. The mean difference is significant at the 0.05 level.

Also, there was a significant difference between gender groups in favor of females rather than males. In addition, there was a significant difference among educational levels in favor of Masters and Ph.D. levels. Additionally, there was a significant difference among internet experience groups in favor of low internet experience. Further, Table 13 shows that there is a significant difference between respondents using Instagram with respondents using Facebook, Snapchat, LinkedIn, and Twitter regarding ISH. While there is no significant difference between respondents using Instagram with respondents using TikTok and WhatsApp regarding ISH. There is a significant difference between respondents using TikTok with respondents using Snapchat, LinkedIn, and Twitter regarding ISH. While there is no significant difference between respondents using TikTok with respondents using WhatsApp regarding ISH. There is a significant difference between respondents using Facebook with respondents using Snapchat, LinkedIn, and Twitter regarding ISH. While there is no significant difference between respondents using Facebook with respondents using WhatsApp regarding ISH. There is a significant difference between respondents using Snapchat with respondents using WhatsApp and LinkedIn regarding ISH. While there is not a significant difference between respondents using Snapchat with respondents using Twitter regarding ISH. There is a significant difference between respondents using WhatsApp with respondents using LinkedIn and Twitter regarding ISH.

Table 13
Multiple comparisons analysis of the ISH attributed to respondents' SN using Tukey HSD.

(I) SN		Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Instagram	TikTok	0.33142	0.14523	0.305	-0.1099	0.7727
	Facebook	.28057*	0.07800	0.008	0.0436	0.5176
	Snapchat	-1.04411*	0.07946	0.000	-1.2856	-0.8027
	WhatsApp	0.14092	0.09531	0.819	-0.1487	0.4305
	LinkedIn	-.57129*	0.09990	0.000	-0.8749	-0.2677
	Others	.77054*	0.18104	0.001	0.2204	1.3207
	twitter	-.83065*	0.10148	0.000	-1.1390	-0.5223
TikTok	Facebook	-0.05084	0.13777	1.000	-0.4695	0.3678
	Snapchat	-1.37552*	0.13861	0.000	-1.7967	-0.9543
	WhatsApp	-0.19050	0.14827	0.904	-0.6410	0.2600
	LinkedIn	-.90271*	0.15126	0.000	-1.3623	-0.4431
	Others	0.43912	0.21372	0.446	-0.2103	1.0885
	twitter	-1.16206*	0.15230	0.000	-1.6249	-0.6993
Facebook	Snapchat	-1.32468*	0.06483	0.000	-1.5217	-1.1277
	WhatsApp	-0.13966	0.08351	0.705	-0.3934	0.1141
	LinkedIn	-.85186*	0.08871	0.000	-1.1214	-0.5823
	Others	0.48996	0.17512	0.097	-0.0422	1.0221
	twitter	-1.11122*	0.09048	0.000	-1.3862	-0.8363
Snapchat	WhatsApp	1.18502*	0.08488	0.000	0.9271	1.4429
	LinkedIn	.47282*	0.09000	0.000	0.1993	0.7463
	Others	1.81464*	0.17577	0.000	1.2805	2.3488
	twitter	0.21346	0.09175	0.280	-0.0653	0.4923
WhatsApp	LinkedIn	-.71221*	0.10426	0.000	-1.0290	-0.3954
	Others	.62962*	0.18349	0.015	0.0721	1.1872
	twitter	-.97156*	0.10578	0.000	-1.2930	-0.6501
LinkedIn	Others	1.34183*	0.18591	0.000	0.7769	1.9067
	twitter	-0.25936	0.10993	0.263	-0.5934	0.0747
Others	Twitter	-1.60118*	0.18676	0.000	-2.1687	-1.0337

*. The mean difference is significant at the 0.05 level.

5.4 Machine Learning Techniques Validation and Prediction

The utilization of modern technologies, such as machine learning, has become prevalent across various applications (Abu-Taieh et al., 2022b; Abu-Taieh et al., 2022c; AlHadid et al., 2022; Masa'deh et al., 2022; Alkhawaldeh et al., 2022; Alkhawaldeh , 2021; Alkhawaldeh , 2019; Abualkishik, 2023; Rawajbeh et al., 2010; Al Rawajbeh et al., 2016; Khan et al., 2023). This research focuses on exploring five classification techniques within machine learning (ML) that transform input data from a dataset into the desired output pattern (Witten et al., 2016). Specifically, the study employs a dataset to investigate the influence of perceived security, perceived privacy, and user awareness on information sharing in social media networks, incorporating five machine learning models: Artificial Neural Network (ANN) (Da Silva et al., 2017), Linear Regression (Yao & Li, 2014), Sequential Minimal Optimization algorithm for Support Vector Machine (SMO) (Platt, 1998), Bagging using the REFTree model (Breiman, 1996), and Random Forest (Tasin & Habib, 2022), for development and evaluation purposes.

The ANN model employs the back-propagation method to calculate the errors between predicted and actual output values, aiming to minimize these errors by adjusting the weights and bias parameters. Linear Regression establishes a dependent output based on target labels, representing a polynomial function with weighted coefficients for independent variables. The model's coefficients are updated during the training phase using the training dataset. The SMO method utilizes the Sequential Minimal Optimization algorithm to update the weighted vectors of the Support Vector Machine (SVM) model. By iteratively identifying minimal values in a sequence, the SMO algorithm achieves optimal values for the SVM model. The bagging technique involves creating multiple REFTree models by randomly sampling instances and features from the training set. The final prediction is made by averaging the values obtained from these trees. Random Forest is a collection of interconnected decision tree (DT) models. Each sub-tree model is constructed using random attribute subsets and a random sample of training data instances. The model's final output is determined by averaging the predictions from the individual DT trees. These machine learning models, integrated into the dataset application, serve various purposes, including predicting hidden patterns and analyzing user behavior concerning perceived security, perceived privacy, and user awareness in information sharing on social media networks. To evaluate the effectiveness of the models in predicting target values, the study employs the 10-fold cross-validation technique. This technique involves dividing the dataset into 10 parts, sequentially using one part as the testing set while the remaining nine parts serve as the training set. The classifier model's performance is assessed in each iteration, and the overall average performance indicates its effectiveness. This methodology ensures the utilization of the entire dataset for both training and testing, reducing the risk of overfitting. If the model accurately classifies all the training data but struggles with the test sets, it suggests the presence of a problem.

5.4.1 ML Results and Discussion

This research focuses on the act of sharing information on social networks, with an emphasis on examining factors such as trust, user awareness, security, and privacy that impact individuals' decisions to share information. To analyze the relationship between these factors and the associated challenges, intelligent ML techniques are employed to extract meaningful information from datasets. To evaluate the performance of ML models, two datasets are utilized.

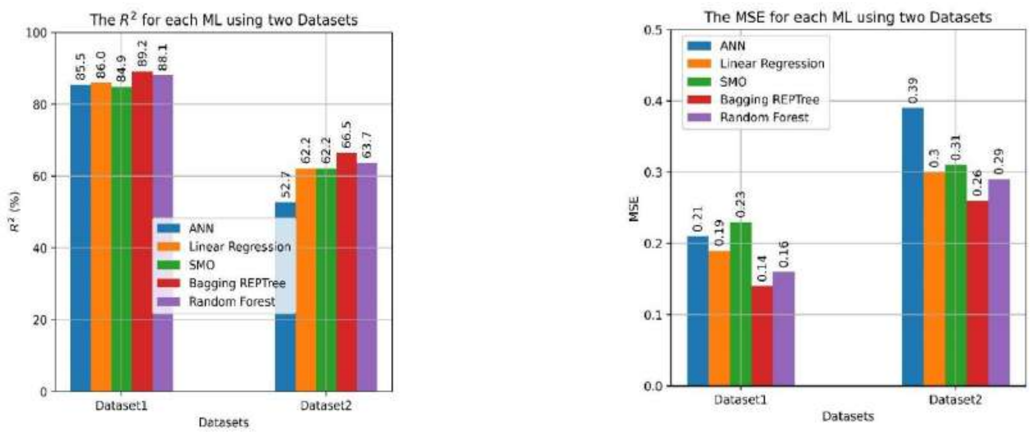

Fig. 2. The results of using ML techniques on YouTube dataset (a) R2; (b) MSE.

The first dataset belongs to Model 1, where the dependent outcome is PT, and the independent inputs consist of three parameters: PS, PP, and UA. The second dataset pertains to Model 2, which investigates the influence of four inputs (PS, PP, AU, and PT) on the dependent variable IS. The experimental findings are presented in Figure (2), where the evaluation metrics of R2 and Mean Square Error (MSE) are utilized. The x-axis represents the different models used, while the y-axis represents the values of R2 and MSE. R2 provides insight into the expected influence of the independent variables on the dependent variable (target), while MSE calculates the average difference between the predicted and actual output values of a model. Among the two database models, the Bagging REFTree and random forest models demonstrate satisfactory outcomes, achieving R2 values of 89.2% and 8.1% respectively. The remaining machine learning techniques also yield consistent results, with R2 values exceeding 85%. However, the results indicate a weaker relationship between the factors in Model 2 and the target factor IS, with R2 values ranging from 52.7% to 66.5% for the employed ML techniques. The corresponding MSE values fall between 0.26 and 0.39. To summarize, the research findings indicate that security, privacy, and user awareness have significant impacts on the intermediary factor of trust. Moreover, both trust as an intermediary factor and user awareness as an independent factor demonstrate a reasonable level of influence on information sharing in social media networks.

6. Findings and discussion

In contrast to the research hypothesis that suggests a positive relationship between perceived privacy and information sharing (H1), this study did not find support for that hypothesis. However, previous studies (references (Gupta & Dhami, 2015; Dhami et al., 2013; Flavián & Guinalíu, 2006) have supported this hypothesis. On the other hand, the study did find support for H2, which suggests a positive relationship between perceived privacy and perceived trust. This finding aligns with previous studies (Maqableh et al., 2021; Gupta & Dhami, 2015; Chawla & Joshi, 2020; Dhami et al., 2013) and contradicts the findings of a different research study (Carlos Roca et al., 2009). Similarly, H3, which proposes a positive relationship between perceived privacy and perceived trust, was supported by this research and is consistent with the findings of (Paramarta et al., 2018; Lin & Wang, 2020; Lin et al., 2019), but contradicts the findings of (Gupta & Dhami, 2015; Dhami et al., 2013).

Regarding H4, which suggests a positive relationship between perceived privacy and information sharing, this research did not find support for this hypothesis, like the findings of (Gupta & Dhami, 2015; Dhami et al., 2013). However, this contradicts the findings of (Paramarta et al., 2018; Lin & Wang, 2020; Lin et al., 2019). While H4 was not supported in this research, it aligns with the studies (Maqableh et al., 2021; Miyazaki & Fernandez, 2001) and contradicts (Gupta & Dhami, 2015; Paramarta et al., 2018; Dhami et al., 2013). Hence, the influence of both perceived security (PS) and perceived privacy (PPV) on information sharing (ISH) was not supported.

The fifth hypothesis, H5, which examines the relationship between users' awareness and perceived trust, was supported in this research and is consistent with previous studies (Gupta & Dhami, 2015; Paramarta et al., 2018; Dhami et al., 2013), but opposed by (Carlos Roca et al., 2009). H6, which states that users' awareness has a positive relationship with information sharing on social media networks, was also supported in this research, in agreement with the findings of (Paramarta et al., 2018).

The seventh hypothesis, H7, proposes a positive relationship between perceived trust and information sharing on social media networks. This hypothesis was supported in this research, aligning with the findings of (Gupta & Dhami, 2015; Paramarta et al., 2018; Dhami et al., 2013; Alkhawaldeh et al., 2022; Alkhawaldeh , 2021), but opposing the finding of (Kumar et al., 2018).

This critical analysis of the research findings reveals mixed support for the hypotheses. The relationship between perceived privacy and information sharing showed inconsistent results, with some studies supporting the hypothesis while others did not. However, perceived privacy was consistently found to have a positive relationship with perceived trust. Users' awareness was also found to positively influence both perceived trust and information sharing on social media networks. Finally, perceived trust was consistently found to have a positive relationship with information sharing. These findings provide valuable insights into the factors influencing information sharing on social media networks and highlight the importance of privacy, trust, and awareness in shaping users' behaviors.

6.1 Practical Implications

This research delves into the central inquiry of information sharing on social networks, aiming to investigate and shed light on the underlying factors at play. Trust, user knowledge, security, and privacy are identified as crucial elements that influence individuals' inclination to share information. By conducting a comprehensive study of these aspects and gaining a deeper understanding of them, researchers, social network developers, marketers, and academicians can glean valuable insights into the behaviors and preferences of social networking site users. Privacy concerns are pervasive, prompting the attention of politicians in the United States and Europe, as exemplified by interviews conducted with key stakeholders from major online platforms such as Facebook, Twitter, and TikTok. The political and economic ramifications of privacy issues for both users and governments underscore the significance of this research topic. Moreover, it is imperative to grasp the diverse cultural norms and expectations surrounding privacy matters, emphasizing the need for a nuanced understanding of privacy-related concerns across different societies. Security considerations about social networks hold significant importance for both citizens and governments, particularly regarding security threats such as espionage. The control and utilization of individuals' data raise concerns about who has access to such data and how it is utilized by various parties. Consequently, governments express legitimate apprehensions about data access and usage, necessitating the establishment of effective safeguards. Trust emerges as a critical factor influencing users' willingness to disclose personally identifiable information in public settings. As individuals place varying levels of trust in different social networks, it becomes essential to investigate the underlying reasons for these trust disparities. Therefore, understanding the determinants of user trust in specific networks assumes utmost significance. Considering these findings, social media networks should prioritize the development of transparent and easily comprehensible privacy policy statements. This approach is crucial for safeguarding and advocating for user interests, while concurrently implementing measures to protect and guide inexperienced users. By critically examining the interplay between trust, user knowledge, security, and privacy in social networks, this research provides valuable insights for stakeholders involved in the development, regulation, and utilization of these platforms.

6.2 Theoretical Implications

This research makes a valuable contribution to the existing literature by addressing the four critical factors—security, privacy, user awareness, and trust—that shape information sharing on social media networks. It fills a gap in the current research landscape, as no previous studies have comprehensively examined all four factors in conjunction. The findings of this research have implications for researchers, users, developers, and academicians, serving as a foundational piece of knowledge in this domain. It is important to note that this research specifically focused on Arabic-speaking countries, recognizing the potential cultural variations that may impact the results. This cultural context adds depth and nuance to our understanding of how these factors operate within specific cultural settings and highlights the need for future investigations to consider such cultural differences in their analyses. One significant outcome of this research is the potential application of the findings for developers as part of their social responsibility when designing or improving social networks. Trust emerges as a multifaceted and evolving process, influenced by the presence of robust security and privacy features, as well as users' awareness. Recognizing the importance of these factors, developers and researchers should incorporate them into their design strategies, fostering greater trust among users and encouraging them to engage in information sharing. The study highlights the multifaceted nature of security, privacy, and users' awareness, which can be influenced by various factors such as social network procedures, policies, practice changes, user experiences, and emerging technologies. Users' trust in social networks is contingent upon their knowledge and awareness of potential security and privacy threats. Greater awareness of the security and privacy features offered by social networks positively impacts users' trust, whereas a lack of awareness can have a detrimental effect on trust levels. Additionally, users' ability to manage how their information is shared and their profiles' protection significantly influences their trust in social networks.

These findings hold practical implications, particularly in terms of educating individuals about the importance of security and privacy features. The study underscores the need to enhance users' awareness regarding the means to protect their data and information within the social network environment. By raising awareness about different online activities on social networks and their implications for trust and the sharing of private information, individuals can make more informed decisions and actively contribute to protecting their data. Consequently, these research findings have the potential to empower users, improve their understanding of security and privacy measures, and foster a safer online environment.

This research presents a comprehensive examination of the factors shaping information sharing on social media networks. It expands our knowledge base, specifically in the context of Arabic-speaking countries, and provides insights that can inform future research and development endeavors. The study emphasizes the importance of trust as a dynamic process influenced by security and privacy features, as well as users' awareness, and advocates for the integration of these factors into the design and implementation of social networks.

6.3 Limitations and Future Research

This research encountered several challenges during its execution. One notable challenge was the reluctance of respondents to engage in discussions and respond to questionnaires, despite the assurance of anonymity. This hesitancy can be attributed to the sensitivity of the topics explored, including privacy, security, trust, user awareness, and information sharing. These themes elicit apprehension among respondents, leading to potential difficulties in data collection and analysis. Moreover, it is recommended that future research delve deeper into the gender issue, as the findings indicated that female respondents exhibited a higher willingness to share information on social networks (SN) compared to their male counterparts. Therefore, it is crucial to conduct further investigations to understand the significant difference in information sharing (ISH) between genders and to explore the underlying factors driving this discrepancy. Additionally, the study identified the significance of age and education about information sharing on social networks. The age group of 18-28 years old displayed notable differences compared to other categories, emphasizing the need for further exploration. Furthermore, there were significant variations observed in educational levels, particularly among individuals with master’s and Ph.D. degrees in comparison to other categories. Consequently, future research should investigate the underlying factors contributing to these differences and their implications for information-sharing behavior. Moreover, social network users originate from diverse nations, each with its own unique cultures, perspectives, and opinions on privacy and trust issues. These varying factors may significantly influence how individuals utilize social network services. Therefore, it is imperative to conduct further investigations that consider the cross-cultural aspects and their impact on users' engagement in online activities. Exploring additional factors such as reliability, credibility, and safety can also provide valuable insights into the factors influencing trust in social networks and users' online behaviors.

7. Conclusions

This study was conducted with the primary objective of comprehensively investigating the factors that influence the dissemination of information within social media networks. The research specifically focused on four key aspects: trust, user knowledge, security concerns, and privacy issues. Trust emerged as a crucial mediator in the relationship between these factors and the dependent variable of information exchange. The findings of the study shed light on the significant impact that security concerns, user knowledge, and privacy issues have on the mediating role of trust. Additionally, the study revealed that information sharing on social media networks is not solely influenced by user knowledge, but also by the mediating factor of trust between users. Furthermore, the study uncovered noteworthy associations between information sharing and various demographic variables, including age, gender, educational level, and internet experience. Notably, distinct differences in information-sharing patterns were observed across different age groups, with the first age group displaying significantly lower levels of engagement compared to the other groups. Moreover, a notable gender disparity emerged, with females exhibiting a higher inclination for information sharing in comparison to males, a trend supported by empirical evidence. Additionally, variations were identified among participants with different educational backgrounds, as individuals with master's degrees or higher demonstrated a clear advantage in terms of their propensity for information sharing. Furthermore, disparities were observed among groups with different levels of internet experience, where individuals with limited experience demonstrated a higher propensity for information sharing compared to those with greater internet proficiency.

These findings contribute to our understanding of the complex dynamics surrounding information sharing in social media networks. The study highlights the multifaceted nature of trust and its crucial role as a mediating factor. Moreover, the identification of demographic variables that influence information-sharing behavior provides valuable insights for researchers and practitioners seeking to understand user engagement within social media platforms. By recognizing the disparities and nuances in information-sharing patterns among different demographic groups, targeted strategies, and interventions can be developed to enhance user experiences and optimize information dissemination within social media networks.

References

Abualkishik, A., Alzyadat, W., Al Share, M., Al-Khaifi, S., & Nazari, M. (2023). Intelligent Gesture Recognition System for Deaf People by using CNN and IoT. *International Journal of Advances in Soft Computing & Its Applications, 15*(1).

Abu-Taieh, E. M., AlHadid, I., Abu-Tayeh, S., Masa'deh, R. E., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. A. (2022c). Continued Intention to Use of M-Banking in Jordan by integrating UTAUT, TPB, TAM and Service Quality with ML. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(3), 120.

Abu-Taieh, E. M., AlHadid, I., Masa'deh, R. E., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. A. (2022a). Factors affecting the use of social networks and its effect on anxiety and depression among parents and their children: Predictors using ML, SEM and extended TAM. *International Journal of Environmental Research and Public Health, 19*(21), 13764.

Abu-Taieh, E., AlHadid, I., Masa'deh, R. E., Alkhawaldeh, R. S., Khwaldeh, S., & Alrowwad, A. A. (2022b). Factors influencing YouTube as a learning tool and its influence on academic achievement in a bilingual environment using extended information adoption model (IAM) with ML prediction—Jordan case study. *Applied Sciences, 12*(12), 5856.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al Rawajbeh, M., Sayenko, V., & Muhairat, M. I. (2016). Simplified CBA concept and express choice method for integrated network management system. *International Journal of Computer Networks & Communications (IJCNC), 8*(3).

AlHadid, I., Abu-Taieh, E., Alkhawaldeh, R. S., Khwaldeh, S., Masa'deh, R. E., Kaabneh, K., & Alrowwad, A. A. (2022). Predictors for E-government adoption of SANAD App services integrating UTAUT, TPB, TAM, Trust, and perceived risk. *International Journal of Environmental Research and Public Health, 19*(14), 8281.

Alkhawaldeh, R. S. (2019). DGR: gender recognition of human speech using one-dimensional conventional neural network. *Scientific Programming,* 2019.

Alkhawaldeh, R. S. (2021). Arabic (Indian) digit handwritten recognition using recurrent transfer deep architecture. *Soft Computing, 25*(4), 3131-3141.

Alkhawaldeh, R. S., Alawida, M., Alshdaifat, N. F. F., Alma'aitah, W. Z. A., & Almasri, A. (2022). Ensemble deep transfer learning model for Arabic (Indian) handwritten digit recognition. *Neural Computing and Applications, 34*(1), 705-719.

Alshare, K. A., Moqbel, M., & Al-Garni, M. A. (2019a). The impact of trust, security, and privacy on individual's use of the internet for online shopping and social media: a multi-cultural study. *International Journal of Mobile Communications, 17*(5), 513-536.

Alshare, K. A., Moqbel, M., & Al-Garni, M. A. (2019b). The impact of trust, security, and privacy on individual's use of the internet for online shopping and social media: a multi-cultural study. *International Journal of Mobile Communications, 17*(5), 513-536.

Breiman, L. (1996). Bagging predictors. *Machine learning, 24*, 123-140.

Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182.

Chawla, D., & Joshi, H. (2020). The moderating role of gender and age in the adoption of mobile wallet. *Foresight, 22*(4), 483-504.

Da Silva, I. N., Hernane Spatti, D., Andrade Flauzino, R., Liboni, L. H. B., dos Reis Alves, S. F., da Silva, I. N., ... & dos Reis Alves, S. F. (2017). Artificial neural network architectures and training processes (pp. 21-28). Springer International Publishing.

Dhami, A., Agarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013, February). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. *In 2013 3rd IEEE International Advance Computing Conference (IACC)* (pp. 465-469). IEEE.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial management & data Systems, 106*(5), 601-620.

Gibson, K., & Trnka, S. (2020). Young people's priorities for support on social media: "It takes trust to talk about these issues". *Computers in human behavior, 102,* 238-247.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in online social networks. *In Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80).

Gupta, A., & Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice, 17*, 43-53.

Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis: A global perspective* (Vol. 7).

Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision support systems, 62*, 11-21.

Hou, J. R., & Kankham, S. (2022). More than feelings? How Facebook reaction icons affect online users' behavioral intentions toward online health rumor posts. *Internet Research, 32*(6), 1978-2002.

Ingram, D., Panchadar, A., & Auchard, E. (2018). Facebook Privacy Scandal Widens as Data Leak Hits 87 Million Users. CIO. Available online at: https://www. cio. com. au/article/635768/facebook-privacy-scandal-widensdata-leak-hits-87-million-users/(accessed September 5, 2019).

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior, 69,* 302-310.

Khan, F., Al Rawajbeh, M., Ramasamy, L. K., & Lim, S. (2023). Context-aware and Click Session-based Graph Pattern Mining with Recommendations for Smart EMS through AI. IEEE Access.

Kim, M., Jun, M., & Han, J. (2023). The relationship between needs, motivations and information sharing behaviors on social media: Focus on the self-connection and social connection. *Asia Pacific Journal of Marketing and Logistics, 35*(1), 1-16.

Koohang, A., Floyd, K., Yerby, J., & Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. *Issues in Information Systems, 22*(2), 133-145.

Kumar, S., Kumar, P., & Bhasker, B. (2018). Interplay between trust, information privacy concerns and behavioural intention of users on online social networks. *Behaviour & Information Technology, 37*(6), 622-633.

Kwateng, K. O., Atiemo, K. A. O., & Appiah, C. (2018). Acceptance and use of mobile banking: an application of UTAUT2. *Journal of enterprise information management, 32*(1), 118-151.

Lin, S. W., & Liu, Y. C. (2012). The effects of motivations, trust, and privacy concern in social networking. *Service Business, 6*, 411-424.

Lin, X., & Wang, X. (2020). Examining gender differences in people's information-sharing decisions on social networking sites. *International Journal of Information Management, 50*, 45-56.

Lin, X., Sarker, S., & Featherman, M. (2019). Users' psychological perceptions of information sharing in the context of social media: A comprehensive model. *International Journal of Electronic Commerce, 23*(4), 453-491.

Majerczak, P., & Strzelecki, A. (2022). Trust, media credibility, social ties, and the intention to share towards information verification in an age of fake news. *Behavioral Sciences, 12*(2), 51.

Maqableh, M., Hmoud, H. Y., & Jaradat, M. (2021). Integrating an information systems success model with perceived privacy, perceived security, and trust: the moderating role of Facebook addiction. *Heliyon, 7*(9).

Masa'deh, R. E., AlHadid, I., Abu-Taieh, E., Khwaldeh, S., Alrowwad, A. A., & Alkhawaldeh, R. S. (2022). Factors influencing students' intention to use E-textbooks and their impact on academic achievement in Bilingual environment: An empirical study Jordan. *Information, 13*(5), 233.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs, 35*(1), 27-44.

Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS. McGraw-hill education (UK).

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I. C., Sandhyaduhita, P. I., & Hidayanto, A. N. (2018, October). Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, Twitter, and Instagram. *In 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)* (pp. 271-276).

Platt, J. (1998). Sequential minimal optimization: A fast algorithm for training support vector machines.

Rawajbeh, M. A., Mansi, I., & Hussien, M. (2010). Algorithm development for measurement and prediction the traffic in broad band integrated service networks. *Journal of Computer Science, 6*(10), 1164.

Rawajbeh, M., Alzyadat, W., Kaabneh, K., Afaneh, S., Alrwashdeh, D., Albayaydah, H., & AlHadid, I. (2023). A new model for security analysis of network anomalies for IoT devices. *International Journal of Data and Network Science*, *7*(3), 1241-1248.

Ruan, O., Zhang, L., & Zhang, Y. (2021). Location-sharing protocol for privacy protection in mobile online social networks. *EURASIP Journal on Wireless Communications and Networking, 2021*(1), 1-14.

Samsudeen, S. N., Selvaratnam, G., & Hayathu Mohamed, A. H. (2022). Intention to use mobile banking services: An Islamic banking customers' perspective from Sri Lanka. *Journal of Islamic Marketing, 13*(2), 410-433.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. john Wiley & Sons.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.

Singh, K. P., & Gill, M. S. (2015). Role and users' approach to social networking sites (SNSs): a study of universities of North India. *The Electronic Library, 33*(1), 19-34.

Stallings, W. (2017). The principles and practice of cryptography and network security 7th edition, isbn-10: 0134444280. *Pearson Education, 20*(1), 7.

Tasin, T., & Habib, M. A. (2022). Computer-Aided Cataract Detection Using Random Forest Classifier. In Proceedings of the International Conference on Big Data, IoT, and Machine Learning: BIM 2021 (pp. 27-38). Springer Singapore.

Witten, I. H., Frank, E., Hall, M. A., & Pal, C. J. (2016). Data mining fourth edition: Practical machine learning tools and techniques. San Francisco: Morgan Kaufmann Publishers Inc.

Yao, W., & Li, L. (2014). A new regression model: modal linear regression. *Scandinavian Journal of Statistics, 41*(3), 656-671.