International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

IMPACT OF TRUST, PRIVACY AND SECURITY IN FACEBOOK INFORMATION SHARING

[1]JithiKrishna P P, [2]Suresh Kumar R,[3]Sreejesh V K

[1]Mtech Computer Science and Information Security LBS College of Engineering Kasaragod, Kerala

[2]Assistant Professor Department of Statistics GPM Govt College Manjeswaram,Kerala

[3]Assistant Professor Department of Computer Science LBS College of Engineering Kasaragod, Kerala

ABSTRACT
In recent years, online social networks have become an important part of daily life for many. Users built explicit networks to represent their social relationships, either existing or new. Most social networking sites like Facebook, Orkut, Twitter, LinkedIn etc provide many features like online interaction, sharing of information and developing new relationships, but also raise privacy, security and trust concerns. So it requires an exploratory insight into user's behavioural intention to share information. This study aimed to identify the effect of security, privacy and trust in social networks. From the survey of 40 participants the findings suggested that the perceived privacy and perceived trust of members in social networking sites significantly related with information sharing whereas the perceived security has no direct effect upon information sharing. But it has an indirect effect through perceived trust.

Key Words:- Social Networks, Perceived Privacy, Perceived Trust, Perceived Security, Information Sharing

1. INTRODUCTION
In recent years social networking sites are the effective medium of communication between family members and friends. The rapid growth of social networking sites such as Facebook, Orkut etc helps millions of individuals to build a public or semi public profile within a bounded system. We can't imagine the life of today's youth without Facebook. Latest Facebook statistics show that in every 20 minutes, 1,00,000 link sharing, 14,84,000 new uploadings, 13,23,000 photo tagging, 18,51,000 status updating, 1972 million friend request accepting, 27,16,000 photo updating and 27,16,000 message sending take place.

Social networking sites have changed the way people build their online personal network for computer mediated communication. The primary objective of social networking user's is to make connections, communication and maintain relationships. But latest trend shows that social networking sites like Facebook is reshaping the way people communicate.

For social networking site users, there are many privacy and trust considerations that needs to be addressed. For example the information revealed in a user's profile can lead to risks like identity theft, online stalking, and cyber harassment. However social networking sites have provided many security features for preserving the privacy of users. Despite all such features, the impact of security, privacy and trust on sharing of information needs to be answered. This paper focuses on the impact of privacy, security and trust on users willingness to share information in social networking sites. The primary research questions of study are:

RQ1: What are the antecedents of trust in the social networking sites?

RQ2: What is the impact of privacy, security and trust on the willingness of sharing information?

2. LITERATURE REVIEW
2.1) Previous Research on Privacy Concerns in Social Networking Sites
Online social network is emerging as the web's top application [4]. Social networking sites, which are primarily used for social interaction, have received significant research attention in recent years.

Some prior studies have examined the user's acceptance of social networking sites, with behavioural intention to use. In related social networking sites research, some prior studies examined the impact of privacy concerns in usage behaviour and information revelation. In [11] author has defined information privacy as the claim of individuals, groups, or institutions to determine of themselves when, how, and to what extent information about them is communicated to others.

In [5] author has proposed trust, security leads the direct effect on usage behaviour and information revelation with trust as central component of social exchange theory. As trust and privacy plays a crucial role in face to face communication and development of new relationship; the similar approach is used by the users in social networking sites as proposed by authors in [2],[3]. Other studies have further established the privacy paradox on social networking sites. Furthermore, several risks to users of online social network and group have been highlighted [4], like embracement, stalking and identity theft. Online social networking has been criticized because users lack trust in site security [2]. In [2], [6] authors have attempted to determine implication of privacy concerns and awareness to user's online practices and behaviour.

2.2) Concept of Privacy and Trust in Social Networking Sites

Privacy concern is the primary focus of this study. Trust is defined as "willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster irrespective of the ability to monitor or control that other party." Whereas privacy can be defined as, "control over the flow of one's personal information including the transfer and exchange of that information." Security is defined as "the extent to which a user believes that using a social networking application will be risk free." The major categories of trust and privacy in social networking site can be defined by the following measures:

- Security
- Control over the flow of information in user's profile
- Notification

3. OBJECTIVES AND HYPOTHESES

3.1) Objectives

1) To assess the perceived trust, security, privacy and information sharing in social networks.

2) To test the relationship between information sharing in social network sites and perceived trust, security and privacy.

3) To estimate the nature of relationship between information sharing and the combined effect of privacy, security and trust.

3.2) Research Hypotheses

The following research hypotheses will be considered in this study and all tested at five percentage level of significance.

H11: Perceived security is positively related to perceived trust with in social networking sites.

H12: Perceived privacy is negatively related to perceived trust with in social networking sites.

H13: Perceived security is positively related to information sharing in social networking sites.

H15: Perceived trust is positively related to information sharing in social networking sites.

4. RESEARCH METHODOLOGY

4.1 Research Framework

Path analysis is used for the model fit of proposed framework. It involves various multiple regression models or equations that are estimated simultaneously. This provides a more effective and direct way of modeling mediation, indirect effects and other complex relationship among variables [7]. Structural relations are hypothesis about directional influences or causal relations of multiple variances.

The proposed framework for finding the willingness of sharing information in social networking sites are represented in figure 4.1. The proposed hypotheses in figure 4.1 was empirically tested.

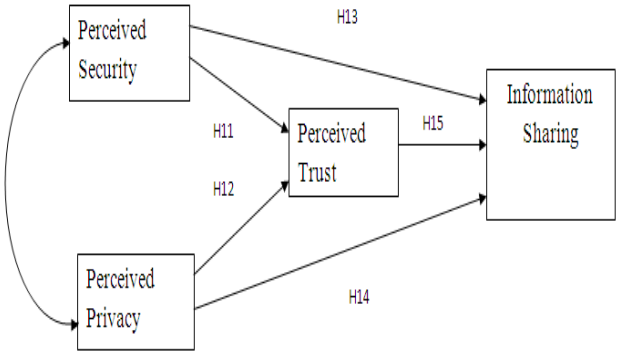


Fig 4-1. Research framework

4.1.1Construct definition

Perceived privacy: - Extent to which an individual has control over his information flow and protection of his profile privacy.

Perceived trust: - An individual's belief in the ability of social networking site that revealing information and performing any task is risk free.

Perceived security: - An individual's belief that using social networking site over Internet is risk free.

Information sharing: - An individual's belief that he will continue to share information over social networking site with regard to privacy concerns.

4.2 Research Design

4.2.1 Data Collection

The study was conducted at LBS College of Engineering , Povval, Kasaragod during the last week of January 2014. The data was collected from 40 students doiing both Btech and Mtech. The samples were selected by purposive sampling method.

A descriptive survey approach was used to conduct the study. The main objective of the study is to identify the factors related to information sharing and also to study the relationship between those factors. We also studied the relationship between information sharing and the demographic characteristics of the subject.

4.2.2 Tools and Techniques Used for the Study

Data was collected by using five point Likertscale. The tool was administered in 8 subjects and obtained the reliability r=0.78 by Cronbach's alpha method. It indicates the tool is reliable to measure the perceived trust, privacy and security.

4.2.3 Validity of the Tool

The tool is given to 5 experts in different areas. Three from computer science and engineering, a statistician and a social researcher. All of them thoroughly examined the questions and suggested their recommendations and finally prepared this tool.

5 DATA ANALYSIS

Data was analysed using descriptive statistics like frequency table, percentage, mean, standard deviation. The hypotheses was tested using inferential statistics- SEM, path analysis, correlation analysis.

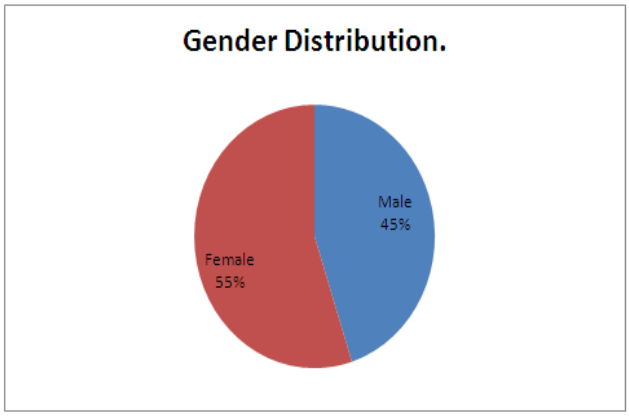
5.1 Profile of Respondents

Table shows the sample demographics of collected data.

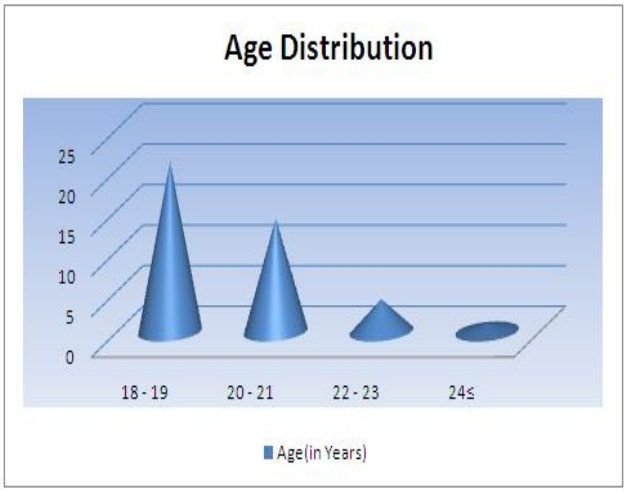
Table 5- 1: Demographics of respondents

Sl no.	Variable	Frequencies	Percentage
1	Gender		
	Male	18	45%
	Female	22	55%
2	Age (in years)		
	18-19	21	52.5%
	20-21	14	35%
	22-23	4	10%
	24&above	1	2.5%
3	Visit in Facebook		
	Don't visit	20	50%
	One	6	15%
	Two	4	10%
	More than twice	10	25%
4	Duration of Facebook visit per day		
	Don't visit every day	14	35%
	< 30 minutes	10	25%
	1 hr	7	17.5%
	<2hr	2	5%
	2hr &more	7	17.5%

Pie chart for Gender Distribution of the sample



Bar chart for Age Distribution

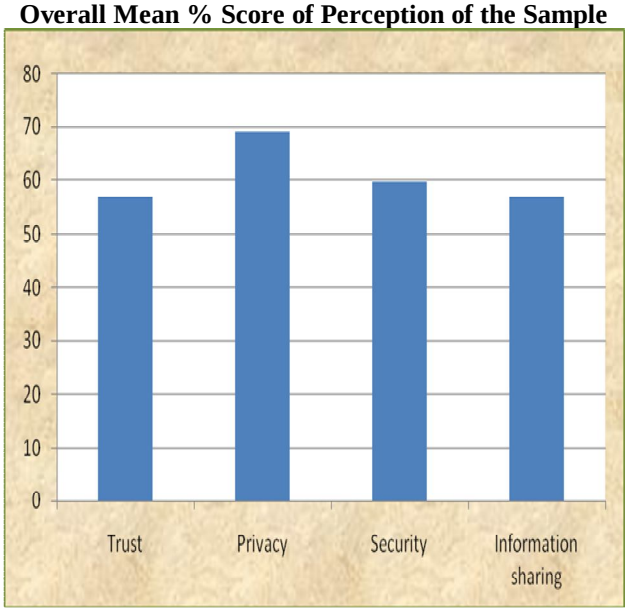


There are 40 students (55% males and 45% females) who participated in this study. 52.5% of them are in the age group 18-19 years. While 2.5% of them are above 23 years. 20(50%) of them do not visit Facebook every day.Only 25% of them visit Facebook more than 3 times a day. Out of 40 respondents 9(22.5%) of them visit Facebook more than one hour in a day and only 50% of them use Facebook less than 1/2hr a day.

Table5- 2: Variables

	Trust	Privacy	Security	Information Sharing
Mean	11.375	6.93	5.98	2.55
Median	12	8	6	2
SD	3.13	2.74	2.21	1.7
Minimum	5	2	2	1
Maximum	20	10	10	5
Mean %	56.875	69.3	59.8	57.0
Overall Level	Average	Good	Average	Average

Overall Mean % Score of Perception of the Sample



The above table shows that the students have a good perception about the control over their information flow and protection of their profile privacy in social networking sites.

5.2 Model Fit Summary

Multiple regression analysis is used for the model fit of the proposed framework. Various fit indices (like R (square)) and ANOVA are used to test the goodness of fit of the regression model.

6. RESULTS

6.1 Structural Paths and Hypotheses Test

The hypothesized casual paths (β) were estimated for hypotheses testing. The table given below represents the results of hypothesis testing.

Table 6-1: Hypotheses Testing

Hypothesis	Path coefficient	P-value	Support
H11:Perceived Security → Perceived Trust	0.443	0.008	Yes
H12:Perceived Privacy → Perceived Trust	-0.324	0.048	Yes

H13:Perceived Security → Information Sharing	0.144	0.246	No
H14:Perceived Privacy → Information Sharing	0.722	0.000	Yes
H15:Perceived Trust Information Sharing	0.119 →	0.309	No

Hypotheses H11 proposes that there is a positive relationship between perceived security and perceived trust (β=0.443, p=0.008), thus supporting H11.This suggests that if users are provided with perceived security while accessing their profile, then it increases their trust level.

There is a negative relationship between perceived privacy and perceived trust (β= -0.324, p=0.048). This supports Hypothesis H12.This suggests that if users have more control over their information flow and protection of their profile privacy, then it decreases their trust level in Facebook.

Hypotheses H13 proposes that there is significant positive relationship between perceived security and information sharing (β=0.144, p=0.246) directly, thus rejects Hypothesis H13.

Hypotheses H14 proposes that there is a positive relationship between perceived privacy and information sharing (β=0.722, p=0.000), thus support H14.This suggests that if users have the control over their information flow and protection of their profile privacy, then it increases the users interest to share information in Facebook.

Hypotheses H15 proposes that there is a positive relationship between perceived trust and information sharing (β=0.119, p=0.309), thus reject hypothesis H15. This suggests that if users trust in the ability of Facebook, it will lead user's willingness to share information, which is not statistically significant.

Thus we can conclude that the perceived security has a positive relation with perceived trust in Facebook. But perceived privacy has a negative relationship with perceived trust in Facebook, are antecedents of perceived trust. Figure 6.1 and Table 6.1 summarizes the result of hypotheses test portrain the full path model.

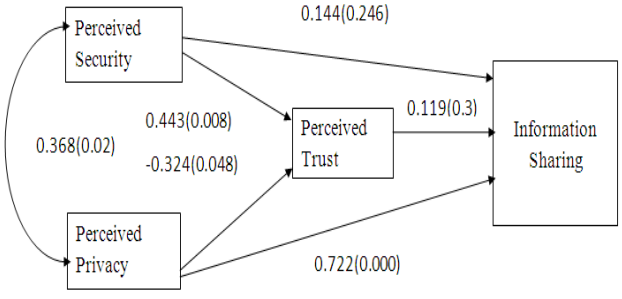


Fig 6-1. Result of Hypotheses Testing

The above model posits that there is no direct effect of perceived security on information sharing (that its only effect is an indirect one channeled through perceived trust) and perceived privacy has only direct effect (with negative relation indirect effect channeled through perceived trust).

6.2 Structural Equation Model

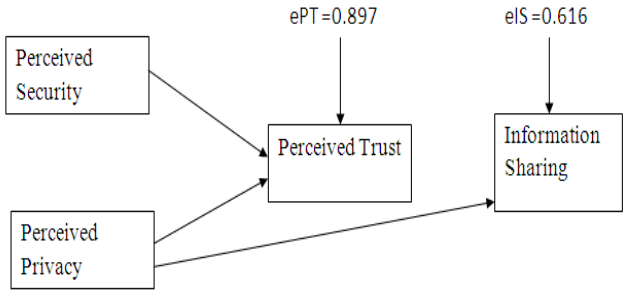


Fig 6-2. Hypothesized Structural Equation Model

7. DISCUSSION AND CONCLUSION

In this study, we assessed the effect of user's privacy concern on usage behavior as well as information sharing on social networking sites with special reference to Facebook. Structural Equation Model is used to analyze the relationship between perceived security, privacy and trust on information sharing. The empirical results indicate that there is a positive correlation between perceived security and perceived privacy. This may be because the extent to which an individual have control over his information flow and protection of his profile privacy will increase the belief that using social networking sites over Internet is risk free.

This research finding suggests that users having control over their information sharing and protection of their profile is more likely trust in Facebook. Further results suggests that perceived privacy and perceived security are antecedents of perceived trust where as there is strong correlation between perceived privacy and perceived trust.

In terms of information sharing, when trust is exerted through privacy and trust it leads to users willingness to share information. Whereas security has no direct effect on sharing of information, which is an interesting result of the study. It shows that trust in the ability of Facebook will lead a user's tendency to share more information.

The result obtained in this study has significant practical implications. The findings may provide social network operators a better understanding of how privacy concern may affect user's trust and information sharing. It leads the operators to develop and promote corresponding application to the users.

This study was conducted on a small group of college students which may not cover the general populations of social networking sites users.

BIBILIOGRAPHY

[1]. A.Dhami, Neha Agarwal, T.K.Chakraborty, B.P.Singh and Jasmine Minj "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook", 3rd IEEE

International Advance Computing Conference, 2013, PP 465-469.

[2]. C.Dwyer, S.R.Hiltz, and K.Passerini, "Trust and privacy concern with in social networking sites: A comparison of Facebook and Myspace", proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado, August 2007, P 339.

[3]. R.Gross, A.Aquisti and H.John Heinz III, "Information revelation and privacy in online social networks", workshop on privacy in the electronic society, November 2005, PP 71-80.

[4]. C.M.K.Cheung, Pui-Yee Chiu and M.K.O.Lee, "Online social networks: why do students use Facebook", computers in human behavior, July 2010, vol 27, no. 4, PP 1337-1343.

[5]. I.Ajzen, "The theory of planned behavior", Organizational behavior and human decision processes, 1991, vol.50, no.2, PP 179-211.

[6]. T.Govani and H.Pashley, "Student awareness of the privacy implications when using Facebook", unpublished paper presented at the aAIJPrivacy Poster FairaAI at the Carnegie Mellon University School of Library and Information Science, 2005, vol. 9

[7]. Pui-Wa Lei and Qiong Wu, "Introduction to Structural Equation Modeling: Issues and practical considerations", Instructional Topics in Educational Measurement, 2007, PP 33-43.

[8]. Abdulla Al Hasib, "Threats of online social networks", Seminar on Internetworking, April 2008, PP 71-75.

[9]. T.Correa, A.W.Hinsley and H.G. de Zuniga, "Who interacts on the web?: The intersection of users personality and social media use", computers in human behavior, October 2010, vol.26, no.2, PP 247-253.

[10]. Danah Boyd, "Facebook's privacy trainwreck exposure, invasion and social convergence", The International Journal of Research into New Me Technologies, 2008, vol.14, no.1, PP 13-20.

[11]. S. Chai, S. Bagchi-Sen, C. Morrell, H. Rao and S. Upadhyaya, "Internet and online information privacy: An exploratory study of preteens and early teens", Professional Communication, IEEE transactions, 2009, vol. 52, no.2, PP. 167-182.