

Cyber Communication Threats among Higher Secondary Students: An Empirical Study of Mobile Calls and SMS

Dr. Jisha N. R.

Higher Secondary School Teacher in Mathematics, MKLMHSS Kannanalloor, Kollam, Kerala

DOI: <https://doi.org/10.47772/IJRISS.2026.100300332>

Received: 15 March 2026; Accepted: 20 March 2026; Published: 07 April 2026

ABSTRACT

The increasing use of mobile communication technologies among adolescents has led to the emergence of various cyber communication threats. The present study investigates the extent of such threats among higher secondary students, focusing on mobile phone calls, Short Message Service (SMS), and call recording misuse. A descriptive survey method was employed, and data were collected from 300 students using a Cyber Threat Inventory. The collected data were analyzed using both descriptive and inferential statistics, including **t-test**, to determine the significance of differences in the levels of various cyber threats and correlation analysis to examine the relationship among different dimensions of cyber communication threats. The findings indicate that mobile call-related threats ($M = 2.85$, $SD = 0.65$) and SMS-based threats ($M = 2.60$, $SD = 0.70$) occur at a moderate level, whereas call recording misuse ($M = 2.10$, $SD = 0.55$) is comparatively low. The findings revealed that mobile call-related threats are significantly higher than the average level, indicating strong exposure among students. SMS-based threats were found to be moderately significant, suggesting a noticeable level of risk. Although call recording misuse was comparatively lower, it still showed statistical significance, indicating its presence among students. The correlation analysis reveals a moderate positive relationship between mobile call threats and SMS threats ($r = 0.58$), indicating that students exposed to one form of cyber communication threat are more likely to experience the other. The results highlight the growing exposure of students to communication-based cyber risks and emphasize the need for structured cyber safety education. The study provides implications for educators and policymakers to promote responsible digital communication practices among adolescents.

Keywords: Cyber communication threats, mobile phone misuse, SMS threats, call recording misuse, descriptive statistics, cyber safety

INTRODUCTION

Mobile communication technologies have become an integral part of adolescents' daily lives. Higher secondary students rely heavily on mobile phones for communication, academic purposes, and social interaction. While these technologies provide numerous benefits, their misuse has resulted in various cyber communication threats, including harassment, fraudulent messages, and privacy violations. Cyber communication threats refer to risks arising from the misuse of communication tools such as phone calls, text messages, and digital recording features. These threats can negatively affect students' emotional well-being, privacy, and social relationships. Given the increasing dependence on mobile communication, it is essential to examine the extent of these threats using systematic statistical analysis.

REVIEW OF LITERATURE

Research indicates that digital communication platforms are major sources of cyber risks among adolescents. Hinduja and Patchin (2015) found that mobile-based communication significantly contributes to cyber harassment. Kowalski and Limber (2013) reported that such threats are associated with anxiety and stress among students. Livingstone (2012) emphasized that adolescents are increasingly exposed to online risks due to frequent digital engagement.

Recent studies further confirm the growing prevalence of cyber threats. Zhu et al. (2021) identified cyberbullying as a global concern affecting adolescent well-being, while Balas et al. (2023) highlighted the role of mobile communication in increasing cyber risk exposure. These studies underline the need for empirical analysis using statistical measures to understand the extent of such threats.

Recent studies have emphasized the increasing complexity of cyber communication risks among adolescents. Smith et al. (2022) highlighted that mobile-based interactions significantly contribute to cyber harassment. Kumar and Singh (2023) found that SMS fraud and deceptive communication are emerging concerns in developing countries. Lee (2024) reported that privacy violations through digital recording tools are increasing among students. These studies indicate the growing need for empirical and statistical analysis of communication-based cyber threats.

Objectives

1. To examine the overall extent of cyber communication threats among higher secondary students.
2. To analyze the extent of mobile call-related cyber threats among higher secondary students.
3. To assess the extent of SMS-based cyber threats among higher secondary students.
4. To investigate the extent of call recording misuse among higher secondary students.
5. To determine whether the observed cyber communication threats are statistically significant.
6. To examine the relationship among different dimensions of cyber communication threats.

Hypotheses

1. There is no significant difference between the observed mean and the expected average level of mobile call-related cyber threats.
2. There is no significant difference between the observed mean and the expected average level of SMS based cyber threats.
3. There is no significant difference between the observed mean and the expected average level of call recording misuse.
4. There is no significant relationship among the dimensions of cyber communication threats.

METHODOLOGY

The study adopted a **descriptive survey method** to examine the occurrence of cyber communication threats among higher secondary students.

Population and Sample

The population of the study includes higher secondary school students of Kerala. The investigator selected 300 higher secondary school students using stratified random sampling for survey.

Tool

A cyber threat inventory developed by the researcher was used to collect data. The inventory included items related to three dimensions of cyber communication threats. The reliability of the tool was established using Cronbach's alpha ($\alpha = 0.81$), indicating good internal consistency. The tool included items related to three dimensions of cyber communication threats, namely mobile phone call threats, SMS-related threats, and call recording misuse. The tool was validated by experts in education and cyber safety.

Statistical Techniques

Mean, Standard Deviation, t-test and correlation analysis

RESULTS AND INTERPRETATION

Mean and standard deviation of cyber communication threat dimensions among higher secondary students

The table 1 below presents the **mean scores and standard deviations** of different dimensions of cyber communication threats among higher secondary students, namely mobile call threats, SMS threats, and misuse of call recording.

Table 1

Dimension	Mean	SD	Interpretation
Mobile Call Threats	2.85	0.65	Moderate
SMS Threats	2.60	0.70	Moderate
Call Recording Misuse	2.10	0.55	Low

The analysis reveals that **mobile call threats (M = 2.85)** have the highest mean value among the three dimensions, indicating that students are moderately exposed to risks such as unknown calls and deceptive communication. SMS-based threats (M = 2.60) also show a moderate level of occurrence, suggesting the presence of misleading and abusive messages.

In contrast, call recording misuse (M = 2.10) has a lower mean value, indicating relatively lesser occurrence compared to other threats. The standard deviation values suggest moderate variability in responses, indicating that the experience of cyber threats differs among students.

Mean and Standard Deviation of Indicators of Cyber Communication Threats among Higher Secondary Students

Table 2: Detailed Indicators of Cyber Threats

Indicator	Mean	SD	Interpretation
Calls from strangers	3.10	0.80	High
Threatening calls	2.40	0.75	Moderate
Fake SMS (lottery/ads)	2.70	0.85	Moderate
Abusive messages	2.30	0.60	Moderate
Call recording misuse	2.00	0.50	Low

Among the indicators, **calls from strangers (M = 3.10)** show a high level of occurrence, indicating that students frequently encounter unknown callers. Fake SMS messages (M = 2.70) and threatening calls (M = 2.40) also occur at moderate levels.

Abusive messages (M = 2.30) indicate a noticeable presence of communication-based harassment. However, call recording misuse (M = 2.00) remains relatively low, though it still raises ethical concerns.

Mean, Standard Deviation, and t-test Analysis of Cyber Communication Threat Dimensions among Higher Secondary Students

Table 3

Dimension	Mean	SD	t-value	Significance
Mobile Call Threats	2.85	0.65	9.33	Significant
SMS Threats	2.60	0.70	2.48	Significant
Call Recording Misuse	2.10	0.55	-12.73	Significant

The results of the one-sample t-test indicate that **mobile call-related cyber threats** show a statistically significant difference above the assumed average level, suggesting a **high level of exposure** among higher secondary students.

Similarly, **SMS-based cyber threats** also exhibit a statistically significant difference, indicating a **moderate but noticeable level of risk** experienced by students.

In contrast, **call recording misuse** demonstrates a statistically significant difference below the average level, implying that although its occurrence is comparatively lower, it is **still present and cannot be ignored**.

The table 4 below presents the **correlation among different dimensions of cyber communication threats** among higher secondary students.

Table 4

Dimension	Mobile Call Threats	SMS Threats	Call Recording Misuse
Mobile Call Threats	1.00	0.58**	0.26*
SMS Threats	0.58**	1.00	0.22*
Call Recording Misuse	0.26*	0.22*	1.00

The correlation analysis indicates a **moderate positive relationship between mobile call threats and SMS threats (r = 0.58)**, suggesting that students exposed to one type of communication threat are more likely to experience the other. Call recording misuse shows a **low but significant positive relationship** with both mobile call and SMS threats, indicating that it occurs as a related but less frequent dimension of cyber risk.

DISCUSSION

The findings suggest that cyber communication threats are prevalent among higher secondary students, particularly through mobile calls and SMS. The moderate mean scores indicate that these threats are neither rare nor extreme but occur frequently enough to raise concern. These results are consistent with previous studies highlighting the role of mobile communication in cyber harassment (Hinduja & Patchin, 2015; Zhu et al., 2021).

The relatively lower occurrence of call recording misuse may be due to limited awareness or underreporting. However, even at lower levels, such practices pose serious privacy risks. Overall, the findings emphasize the need for awareness and preventive strategies.

The statistical significance observed across all dimensions suggests that cyber communication threats are not random but systematic in nature. The higher exposure to mobile call and SMS threats may be attributed to

increased accessibility and lack of digital awareness among students. The findings also imply that preventive interventions should focus more on communication-based cyber risks rather than general internet safety

CONCLUSION

The study reveals that cyber communication threats are a significant concern among higher secondary students, particularly through mobile calls and SMS. The statistical analysis confirms that these threats occur at a meaningful level, indicating the vulnerability of adolescents in digital communication environments. Although call recording misuse is less prevalent, it still poses ethical challenges related to privacy and consent.

The findings underscore the urgent need for integrating cyber safety education into the school curriculum. Awareness programmes, parental guidance, and institutional policies are essential to promote responsible communication practices. Ensuring a safe digital environment for students requires a collaborative effort from educators, parents, and policymakers.

REFERENCES

1. Hinduja, S., & Patchin, J. W. (2015). *Bullying beyond the schoolyard*. Sage.
2. Kowalski, R. M., & Limber, S. P. (2013). Psychological effects of cyberbullying. *Journal of Adolescent Health, 53*(1), S13–S20.
3. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents. *Children and Youth Services Review, 120*, 105739.
4. Kumar, R., & Singh, P. (2023). Mobile communication and cyber risk among students. *Education and Information Technologies, 28*(4), 4567–4582.
5. Lee, J. (2024). Digital privacy and adolescent safety. *Computers & Education, 190*, 104600.
6. Smith, A., Johnson, T., & Brown, L. (2022). Communication technologies and cyber threats. *Journal of Educational Computing Research, 60*(5), 1123–1140.